



DAILY SECURITY AWARENESS TIPS

 inspired eLearning®
education for your enterprise

JAN

2018



SUN	MON	TUE	WED	THU	FRI	SAT
	Don't let anyone, 1 including family, friends, or coworkers, use your work computer or your user account.	Computer worms replicate themselves and can quickly spread. Use antivirus software to stop worms in their tracks. 2	Whenever you give your password out, you become vulnerable. Don't share your password with anyone under any circumstance! 3	Hackers target end users because they are considered the weakest link. Keep security strong by remaining vigilant. 4	Thieves looking for data may go through the garbage to get information. Always dispose of sensitive or confidential documents properly. 5	Fake URLs may seem very convincing. Learn to identify the building blocks of a URL to protect yourself from phishing attacks. 6
Your child may 7 not want to tell you if they are being bullied online. Talk to your child about bullying to make them feel more at ease.	Personally identifiable information is typically protected through privacy laws. 8	Never leave sensitive information in conference rooms or other shared meeting areas. 9	Short, simple passwords can be guessed in minutes by a password cracker program. Always use long, complicated passwords to defend against this threat. 10	Be suspicious of people you don't know who ask for sensitive information. 11	Take special precautions to protect private, confidential, and any other type of sensitive information. 12	Help ensure 13 our security by monitoring the work environment and reporting any breaches of policy or security.
Choose 14 passwords that cannot be found in a dictionary and that cannot be easily guessed.	Don't access 15 workplace data on mobile devices unless absolutely necessary.	Social media 16 apps may broadcast your location. Don't give apps permission to post this sensitive information.	Old browser 17 plugins may have security vulnerabilities. Update them regularly to protect your computer.	Friends may 18 be unwitting participants in scams. Let your friends know of any suspicious activity on their email accounts.	Identity thieves 19 may test out your accounts with small charges. Go through your credit card statements line by line.	Keep yourself 20 safe when you are traveling. Never transport items for others and keep your important possessions secure.
Classify, label 21 and protect all documents and files to safeguard them from malicious insiders.	Phishing emails 22 sometimes pose as queries from legitimate businesses. Always check with the company direct before clicking.	Securely delete 23 all files before disposing of old computers, printers, and fax machines.	Verify the 24 sender's identity before responding to a request to provide personal information over the internet.	Protect 25 personal identifiable information to counter ID theft.	Back up your 26 laptop's data to secure, removable media devices.	Always get 27 authorization from management before accessing your organization's information when working remotely to avoid data theft.
Protect your 28 home computer by using strong security measures.	Your children 29 may put themselves at risk by sharing personal information online. Always use parental controls.	Public cloud 30 storage is not always secure. Never store confidential data on a public cloud storage server without approval.	Protect your 31 home computer and personal devices by automatically installing operating system, browser, and plugin updates.			

JANUARY 1

Don't let anyone, including family, friends, or coworkers, use your computer or user account.

This could easily lead to a breach of security and is almost certainly a breach of policy. Notify your manager or the IT department if coworkers might legitimately need to access your computer or a user account.

JANUARY 2

Computer worms replicate themselves and can quickly spread. Use antivirus software to stop them.

A computer worm is a malware program that can self-replicate. It creates copies of itself on other computers and can thus spread through a network quite quickly. Use antivirus software and update it often to ensure that worms cannot spread to or from your computer. A worm may not always have an obvious effect on your computer, so without an antivirus solution you might not know that you are infected.

JANUARY 3

Whenever you give your password out, you become vulnerable. Don't share your password with anyone!

Even if you trust someone, you should never give out your password. Your communications could be intercepted, the other person may write your password down or save it somewhere, or the other person's computer may be infected with malware. You cannot control what happens to your password after you give it out. The only solution is to never share your password with anyone else, regardless of how much you trust them. No one should ever need your password.

JANUARY 4

Hackers target end users because they are considered the weakest link. Be vigilant and keep security strong.

Hackers often target end users and their devices as a way to gain access to an organization's network. End users are the actual users of software and they are considered vulnerable to social engineering tactics, viruses and malware. Protect yourself by understanding the risks involved and by knowing that you may be targeted as a means to get into your workplace's network and confidential data.

JANUARY 5

Thieves looking for data may go through the garbage to get info. Always dispose of documents properly.

Identity and information thieves will often go through the trash to find confidential or sensitive information. Always dispose of these documents by shredding them or otherwise destroying them. Keep in mind that copies of sensitive documents will also need to be shredded or destroyed to protect workplace data. Thieves may also look for discarded USB drives, cds and other physical media, which should also be properly destroyed before being discarded.

JANUARY 6

Fake urls may seem very convincing. Learn to identify the building blocks of a URL to protect yourself.

Phishing attacks often use fake urls to make you think that you are on a different site than the one you are one. URLs, such as "http://subdomain.domain.com/folder/page.html", are comprised of specific parts: the protocol ("http://"), the domain ("subdomain.domain.com"), directories ("/folder/") and finally a page ("page.html"). The domain is the part of the URL that you must pay attention to and it is only the part after the "http://" and before the first forward slash ("/"). "http://www.bank.com" is a domain on "bank.com," but "http://wwwbank.com" and "http://www.bank.co/m" are both entirely different domains.

JANUARY 7

Your child may not tell you if they are being bullied online. Talk to your child about cyberbullying.

Children who are being bullied online may not want to talk about it. They may feel ashamed or embarrassed, or simply be afraid of getting into trouble. Talk to your children about bullying and make sure that they know that they can come to you with any of their problems. Watch for any signs that someone may be bullying them through social media accounts or other online venues, such as a change in personality.

JANUARY 8

Personally identifiable information is typically protected through privacy laws.

PII, or Personally Identifiable Information, is a protected subset of information that is considered sensitive and confidential. This data is almost always required to be secured by local privacy laws. If you are not clear about the requirements for compliance regarding PII, or if you're not sure whether you deal with PII, you should contact your supervisor immediately. Proper protocols and technology must be in place to protect PII.

JANUARY 9

Never leave sensitive information in conference rooms or other shared meeting areas.

When you leave a shared meeting area or conference room, be sure to erase any whiteboards before you leave and never throw sensitive information in the garbage in shared meeting areas. Dispose of it per your organization's security policy.

JANUARY 10

Simple passwords are guessed in minutes by a password cracker program. Always use complicated passwords.

A password cracker program is used to guess your password by trying many thousands of combinations of numbers, letters, and special characters per second. To guard against these programs, use strong passwords that contain upper and lowercase letters, numbers, and special characters like "&" and "%". The longer the password, the harder it is to crack.

JANUARY 11

Be suspicious of people you don't know who ask for sensitive information.

"Social engineers" use lies and manipulation to trick people into giving away sensitive information, such as usernames, passwords, and credit card numbers. Don't fall for it! Follow these best practices: always maintain a healthy sense of skepticism when dealing with unknown individuals, especially if they ask for any internal or sensitive information; verify the identity of those who ask for information in person or over the phone, before you release any information.

JANUARY 12

Take special precautions to protect private, confidential, and any other type of sensitive info.

Each document and email should be clearly classified based on its value and sensitivity level, such as public, private, or confidential. Appropriate protections should be defined for each classification level for the document when it is in storage, in transit, who it may be shared with, and its secure disposal, like whether the document can be sent to a service provider, or if it must be encrypted. Recognize, understand, and implement the defined protection requirements.

JANUARY 13

Help ensure our security by monitoring the work environment and reporting any security breaches.

If you notice an unescorted visitor, escort them to the security guard. If you find sensitive documents, protect them and turn them into the IT department. Close and lock the emergency door that has been propped open, and report the incident to security.

JANUARY 14

Choose passwords that cannot be found in a dictionary and that cannot be easily guessed.

Passwords are supposed to be kept secret and choosing a strong password will help to keep it that way. If yours can be easily guessed, it weakens the security and might lead to a costly breach. Don't choose passwords that use names or special dates, like birthdays and anniversaries. Attackers search social networking websites for personal details and try them as passwords.

JANUARY 15

Don't access workplace data on mobile devices unless absolutely necessary.

Mobile devices, such as smartphones and tablets, are not always secure ways to connect to our organization's network. For the purposes of mobile device security, you should only access workplace data on your mobile device when absolutely necessary and you should always connect from a secured and encrypted connection. Additionally, any device that you use to access the business network or workplace data should be approved for business use and meet minimum security requirements defined by IT.

JANUARY 16

Social media apps may broadcast your location. Don't give apps permission to post sensitive info.

There are many social media apps that may broadcast your location. On a smartphone, these apps will usually request access to your GPS coordinates. On the web, however, these apps may simply pick up your location from your IP address and never ask for permission. Be very cautious about this. Someone could use your location to stalk you. They could also use this information to determine when you are not home so they can rob you. Avoid the temptation to "check in" on social media.

JANUARY 17

Old browser plugins may have security vulnerabilities. Update regularly to protect your computer.

Browser plugins, such as Flash, Java, and Acrobat, may become out of date and represent a security risk. Update them on a regular basis or set them to update themselves automatically to ensure your computer is protected. Make sure to restart after updating.

JANUARY 18

Friends may be unwitting participants in scams. Let them know of any suspicious activity with their email.

Occasionally, social engineers may use a friend's email address to send out viruses, malware, or phishing attempts. If you receive a suspicious email from a friend, you should avoid clicking or downloading anything within it. Immediately alert your friend through phone or text regarding the message to make them aware of it. This will help stop malicious emails going out to others.

JANUARY 19

Identity thieves may test out your accounts with small charges. Go through your statements line by line.

Suspicious activity on your credit card or bank account statements may not be large or noticeable. Often, identity thieves will try to steal a small amount of money from many accounts or may test out an account with a small charge before stealing more. Look through your credit card statements carefully and contact your bank immediately if you notice any unauthorized charges.

JANUARY 20

Keep yourself safe when you are traveling. Never transport items for others and keep your possessions secure.

It's important that you remember not to transport items for others when you travel. However, this doesn't just include bags and other physical items. Keeping copies of important documents will make it more difficult for problems to arise.

JANUARY 21

Classify, label and protect all documents and files to safeguard them from malicious insiders.

Often, a security system may not be effective when keeping data safe because the threat may come from within the organization. To avoid security threats from malicious insiders, ensure that all documents and files are properly classified to minimize risk.

JANUARY 22

Phishing emails sometimes pose as queries from legitimate businesses. Always check with the company directly and never click on links.

Many fake emails, known as phishing emails, pretend that they are from legitimate companies and ask you to click a link to log in or ask you directly for personal information. Rather than trusting these emails, contact the company directly using contact information that you already had previously and ask them if the email is legitimate. Don't click the link. Go directly to the official website first.

JANUARY 23

Securely delete all files before disposing of old computers, printers, and fax machines.

If you have ever accidentally deleted a file and tried to get it back, you should know that specialized software tools can help you recover missing data. This is possible because when you move a file into your computer's trash and then delete it, the data still exists until you write a new file to the hard drive. Data recovery software can also help criminals capture information that has been deleted but not physically wiped out. Always securely delete sensitive files from old computers and devices such as printers and fax machines to protect your organization from criminals once the equipment is no longer under your control.

JANUARY 24

Verify the sender's identity before responding to a request to provide personal information over the internet.

Phishing is a method of fraudulently obtaining information about a computer user by posing as a trusted entity, like a bank. The most common form of phishing involves contacting users by email and asking to verify an account by providing information to a false website that looks legitimate. Avoid schemes by contacting the purported sender to confirm the organization actually sent the message. It's also good practice to manually enter the genuine URL into your browser's address bar, rather than clicking on the link.

JANUARY 25

Protect personal identifiable information to counter ID theft.

If your organization maintains files on people, such as account information and contact details for customers and clients, you need to make sure you are protecting their Personal Identifiable Information or PII. The government defines PII as information that will directly identify a person, such as a mailing address, email address, phone number, or an ID code issued by your organization. A criminal can use PII to impersonate someone and commit identity theft.

JANUARY 26

Back up your laptop's data to secure, removable media devices.

Laptops can be lost, damaged or stolen. To avoid losing valuable information, back up your laptop's data regularly to an authorized network drive or a secured, removable device such as an encrypted and password-protected USB flash drive. Check with the IT department for authorized devices and locations for backing up your data.

JANUARY 27

Always get prior authorization from management before accessing your organization's information when working remotely to avoid data theft.

When you are working remotely from home or while on the road, it's important to take precautions before you access proprietary and sensitive data from your organization. Your Internet connection may not be as secure at home or while you are traveling, giving hackers an opportunity to steal data. When working remotely, always ask your manager for permission before you log in.

JANUARY 28

Protect your home computer by using strong security measures.

A home computer often has significant amounts of personal information on it. You can protect your home computer using the same security techniques that you use for your work technology. Use a strong password, run your anti-virus software regularly, avoid phishing techniques, backup your data, and never use unsecured wireless connections.

JANUARY 29

Your children may put themselves at risk by sharing personal information online. Always use parental controls.

Children could potentially compromise their identities by sharing personal information with strangers, such as their name, age or even their address. Even something as small as a name and town could potentially be used to identify your child. Always turn on parental controls on any device your children use that can connect to the Internet.

JANUARY 30

Public cloud storage is not always secure. Never store sensitive data on a public cloud server without approval.

Cloud storage has some innate security risks. A public cloud storage solution could potentially be compromised by other users and will only be as secure as your account password. Public cloud servers are also easily accessible from anywhere, and thus malicious individuals can target them. Sensitive or confidential information shouldn't be stored on these servers without pre-approval. Public cloud servers include solutions such as iCloud and Dropbox.

JANUARY 31

Protect your personal devices by automatically installing operating system, browser, and plugin updates.

New threats to devices and personal computers are discovered all the time. Once a new threat has been discovered, it may quickly propagate. To protect your computer and mobile devices from these potential threats, you should always install the latest operating system, browser, and plugin updates.

FEB

2018



SUN	MON	TUE	WED	THU	FRI	SAT
				Use as many characters as possible in your password. 1	Avoid WEP Wi-Fi security connections because intruders can easily hack WEP. 2	Keep copies of important documents when traveling. 3
Use caution when opening email attachments, especially password-protected ZIP files. 4	Be careful about what you post on social media. Attackers can use your information to impersonate you or steal your identity. 5	Protect your home computer with anti-spyware. 6	Always cover the keypad when entering your PIN at an ATM to counter ATM skimmers. 7	Back up key data on your mobile devices on a regular basis. 8	Check the identify of your driver before getting in the car when you are traveling. 9	Delete all sensitive data from desktops, laptops, mobile devices and removable media before disposing of them. 10
Never respond to unsolicited email messages that request your personal information. 11	When your computer is logged in, it is vulnerable to physical intrusion. Always log off or lock your computer when away from your desk. 12	Properly dispose of all sensitive hardcopy files. 13	Use only trusted app stores like Google Play and the Apple App Store. 14	For a safer web browsing experience, look for HTTPS in the web address before submitting sensitive data to a website. 15	Phishing emails can be detected. Learn about the obvious signs. 16	Tag your luggage with your name, address, and phone number when traveling and ensure you don't leave it unattended. 17
Don't fall for hacker tricks: email and instant messaging attachments may contain malware. 18	Children may be at risk online. Educate them about the dangers early to protect them online. 19	If you think you're being followed, you may be in danger. Find help immediately or drive to the nearest police station. 20	Your voicemail could contain sensitive data. Always protect your voicemail with a password. 21	Identity thieves often use phishing techniques. Protect yourself by keeping personal information to yourself. 22	Any child can become a bully. Speak to your child if you suspect they are bullying others. 23	Guests could cause security breaches. Guests should have their own accounts. 24
Fake online romances may lead to phishing attempts. Be skeptical of trading personal information. 25	Never use personal information within your passwords. 26	Exercise caution when using ATMs. 27	Be on guard against unknown people who ask you for sensitive information. Social engineers are criminals who want to steal crucial data. 28			

FEBRUARY 1

Use as many characters as possible in your password.

As a password gets longer, it gets exponentially harder for a hacker or a password guessing program to crack. Passwords should be at least eight characters long and passwords with administrative rights should be twelve characters long. And of course all passwords should use special characters in your password such as “!”, “\$”, and “&” to make your password even more secure.

FEBRUARY 2

Avoid WEP Wi-Fi security connections because intruders can easily hack WEP.

If you need to wirelessly access a network to obtain data from your organization or to get on the Internet, it's important to make a secure connection. Otherwise, criminals may eavesdrop on your communications and steal passwords and other vital data. Avoid WEP (Wired Equivalent Privacy), which is an older and less secure protocol. Instead, use the latest WPA2 (Wi-Fi Protected Access) protocol, which includes high-grade encryption to safeguard your information. When connecting over a public Wi-Fi hotspot, use a Virtual Private Network to keep your data encrypted and secure.

FEBRUARY 3

Keep copies of important documents when traveling.

Losing important documents while traveling, such as your ID and passport, can be extremely inconvenient and costly. Always leave a copy of your itinerary and your important documents with someone else while you're traveling, and call in regularly to update them on your trip. You can also keep digital copies of your important documents while you travel; these copies may be able to help you should your originals be misplaced or stolen.

FEBRUARY 4

Use caution when opening email attachments, especially password-protected ZIP files.

Malicious software or malware can be found in email attachments. This especially true of password-protected ZIP files, since a virus scanner won't be able to automatically scan the contents of the ZIP file. To protect yourself, make sure that you know and trust the sender of an email message before opening any of its attachments.

FEBRUARY 5

Be careful about what you post on social media. Attackers can use your information to impersonate you or steal your identity.

The information that you innocently post on social media such as Facebook and Twitter can help criminals commit identity theft and give unauthorized users access to your organization's private information. Don't post a birth date or age when posting images from your birthday party, for example, and don't give out private details such as your mother's maiden name or digits from a state-issued ID number.

FEBRUARY 6

Protect your home computer with antispyware.

Spyware transmits information about your computer activities to another person without your knowledge, especially Internet surfing behavior. Be sure the antivirus application you use at home also protects your computer from spyware and ensure that the software is updated daily.

FEBRUARY 7

Always cover the keypad when entering the PIN at an ATM to counter ATM skimmers.

It's prudent to remain aware of your surroundings when using an ATM machine to get money from your account, to avoid getting mugged by a criminal. However, criminals don't have to be physically present at your ATM to steal from you. Always cover the keypad when entering your personal identification number or PIN at the ATM. Thieves bent on fraud sometimes place counterfeit bank card readers or ATM skimmers over the real card reader slot to copy your information. Then they use a camera to capture your PIN number and match it with your account so they can clone your card and steal from you.

FEBRUARY 8

Back up key data on your mobile devices on a regular basis.

Just as you must back up the data on your desktop or laptop computer in case of hard drive failure, loss, or theft, it's equally important to back up the crucial data that you store on your mobile device. Otherwise, this data could be lost forever if your mobile device is lost, stolen, or suffers a hardware failure.

FEBRUARY 9

Check the identify of your driver before getting in the car when you are traveling.

When you are traveling for work and need to be picked up by someone whom you've never met before, exercise appropriate caution. This is particularly important when you are traveling in an unfamiliar region or an area known to be plagued by kidnapers and other dangerous criminals. To be safe, verify the identity of your driver before getting into his or her car. Check a photo ID; do not be lulled into a false sense of security by someone holding up a sign with your name on it.

FEBRUARY 10

Delete all sensitive data from desktops, laptops, mobile devices & removable media before disposing of them.

If you are updating your computer or mobile device, it's important to digitally wipe it clean before you dispose of it or give it to someone else in your organization to use. Otherwise, unscrupulous individuals or outright criminals may use data recovery software to access your organization's sensitive and confidential data. Use a secure data deletion program and reformat hard drives and removable media to erase all traces of your information. Contact the Help Desk for assistance if necessary.

FEBRUARY 11

Never respond to unsolicited email messages that request your personal information.

Cybercriminals looking to commit fraud or identity theft or who want to steal your organization's confidential data will send out unsolicited messages to unsuspecting people asking for their account login information or other sensitive details. Be very skeptical of such requests and do not provide your personal data in response to these "phishing" messages. No reputable firm, such as a bank or online service, will ever request your personal data via email. Delete these types of messages without clicking on them.

FEBRUARY 12

When your computer is logged in, it is vulnerable to physical intrusion. Always log off or lock your computer when away from your desk.

Anyone can get onto your computer and review sensitive or confidential data while it is logged in. Simply stepping away for five minutes could be enough time for someone to copy a file. If you want to protect the data on your computer, you should always log off or lock your computer when you are away. For additional protection, go into your computer's settings and set your computer to lock automatically if idle.

FEBRUARY 13

Properly dispose of all sensitive hardcopy files.

Sensitive hardcopy files, if not properly disposed, can represent a significant security issue. A hardcopy file can be copied without any indication that the data has been breached, and hard copies are often much easier to steal than digital copies. To prevent these files from being abused by malicious insiders or otherwise exploited, these documents should all be shredded or incinerated properly when they are no longer of use. Sensitive documents should always be kept properly secured before disposal.

FEBRUARY 14

Use only trusted app stores like Google Play and the Apple App Store.

Malicious programs, or malware, often infect a mobile device when you download applications from an untrusted source. It's therefore essential that you obtain applications for your mobile device from a trusted source such as Google Play and the Apple App Store. The applications from these sources have a lower chance of being infected with malware because these companies regularly review the applications in their stores. You should also refrain from jailbreaking an iPhone or rooting an Android phone, as that could make it easier for malware to infect your device.

FEBRUARY 15

For a safer web browsing experience, look for HTTPS in the web address before submitting sensitive information to a site.

Some people set up websites without providing security to protect your data. Before submitting sensitive information, such as a password or credit card information, make sure to look for "HTTPS" in a Web address, which indicates that the site is secure and encrypted to protect your private information. You should also see a padlock icon in the address bar of your Web browser. A secure website uses Secure Sockets Layer (SSL) to encrypt your data and is suitable for online banking transactions or making purchases.

FEBRUARY 16

Phishing emails can be detected. Learn about the obvious signs.

Phishing emails are emails that are designed to gather information about you for a malicious purpose. While these emails can be quite deceptive, there are usually some major warning signs. Phishing emails often contain some form of warning, such as an account suspension. This warning will request that you click on a link and fill out a form with either personal information or account login information. When in doubt, contact the company directly rather than responding to the email in any fashion.

FEBRUARY 17

Tag your luggage with your name, address, and phone number when traveling and ensure you don't leave it unattended.

The loss of your luggage during travel can occur accidentally or through theft. Protect yourself from the accidental loss of luggage by tagging it on the inside and outside with your name, address, and phone number. Use brightly-colored tags made from strong plastic that will resist rough handling. Avoid theft of your luggage by attending to it at all times, and don't allow someone to distract you by asking directions or spilling a drink on you.

FEBRUARY 18

Don't fall for hacker tricks: email and instant messaging attachments may contain malware.

If someone you don't know sends you an attachment via email or through instant messaging, do not click on it. Hackers are notorious for trying to trick people by attaching malware to unsolicited messages. Only consider selecting or downloading an attachment from someone you already know or whose identity and intentions you can verify. Otherwise, malware from the attachment could wind up infecting not just your computer, but also all computers on your organization's network.

FEBRUARY 19

Children may be at risk online. Educate them about the dangers early to protect them.

Children will face many dangers online: cyberbullying, predators, and even oversharing. Teach your children about the risks they face online once they begin using the Internet, and encourage them to always follow their instincts and talk to an adult if something does not seem right. Monitoring their Internet usage and social media accounts will reduce risks further.

FEBRUARY 20

If you think you're being followed, you may be in danger. Find help immediately.

Criminals may follow a prospective victim for quite some time before they strike. If you feel as though you're being followed, you should enter into the first open public establishment that you pass. If it is dark, stay as close to the light as possible until you enter. Tell an employee, manager or owner within the establishment that you are being followed and ask them to call the local authorities. The police can then determine whether the person following you was a threat. Do not leave until you are certain that you are safe.

FEBRUARY 21

Your voicemail could contain sensitive data. Always protect your voicemail with a password.

Personal and work voicemail accounts may contain sensitive or confidential information. Someone trying to gather information about you or about your workplace may know enough to attempt to log into your voicemail account. Secure your voicemail with a password and delete old voicemails that you no longer need to reduce risk.

FEBRUARY 22

Identity thieves often use phishing techniques. Protect yourself by keeping your personal data to yourself.

Phishers will often attempt to gain information from you under false pretenses so that they can steal your identity. As an example, they might claim to be from your ISP and ask you for your PIN or your mother's maiden name to verify your account. If you respond, they will then have some of the information they need to get into your accounts. Protect yourself by never giving out personally identifiable information over the phone, through email or through instant messenger.

FEBRUARY 23

Any child can become a bully. Speak to your child if you suspect they are bullying others.

Children don't always understand the consequences of their actions or how they may affect others. If you suspect that your child is bullying another child you should speak with them immediately. Explain to them how bullying can affect other people and the consequences bullying may ultimately have for both them and the others involved. Make sure that your child understands how serious bullying is and that it needs to stop.

FEBRUARY 24

Guests could cause security breaches. Guests should have their own accounts.

If you do need to share your computer with someone, you should make sure that the guest logs in with their own username and password. Otherwise, the guest will be able to connect to any of the information that you can connect to. Further, you could become responsible for anything the guest does as it may appear to have been done by you. When at all possible, computer sharing should be avoided.

FEBRUARY 25

Fake online romances may lead to phishing attempts. Be skeptical of trading personal information.

Regardless of how real someone seems, you should never give them personal information. Many phishing attempts occur through fake online dating sites. The person in question may ask you casual questions such as questions about your children, your hometown or your high school. The answers to these questions could potentially be used to steal your identity.

FEBRUARY 26

Never use personal information within your passwords.

Passwords that contain personal information can be guessed easily. Your birthday, children's names, anniversary, pet's names, hometown, or favorite sports team could all be easily gleaned from social media accounts or other sources. Instead, use a completely random password and change it often. Strong passwords are lengthy and include numbers and special characters.

FEBRUARY 27

Exercise caution when using ATMs

ATM skimming is a type of fraud that involves the thief obtaining, or "skimming," the data on your ATM card. The most common form of skimming occurs when a thief installs a card reader and a small hidden camera on an ATM machine, allowing the thief to record the data on your ATM card's magnetic strip and your PIN code. Avoid ATMs that seem suspicious and cover the keypad with one hand while you type in your PIN code with your other hand to prevent a camera from secretly recording your PIN.

FEBRUARY 28

Be on guard against unknown people who ask you for sensitive information. Social engineers are criminals who want to steal crucial data.

Social engineers may try to trick you into giving away sensitive information, such as user login names and passwords or credit card numbers. They may pose as authorized users or members of a security firm, for example. Remain on guard and verify the identity of any person making an unsolicited request before you give away information by phone, email, or in person.

MAR

2018



SUN	MON	TUE	WED	THU	FRI	SAT
				To avoid becoming the victim of a phishing expedition, call your friend or colleague if an email seems suspicious. 1	Ask your tech-savvy children to teach you about using computers to help you learn what they are doing online. 2	Encrypt sensitive data when it is stored on a mobile device. 3
Set your home computer to receive automatic operating system and application updates since they contain security patches. 4	Do not give out data about coworkers, remote network access, organizational practices/strategies to people you do not know. 5	Phishers may call asking for private data. Do not give private data over the phone to someone who calls in. 6	Kids need extra protection online. Use a kid-friendly browser to ensure their safety. 7	You should only have access to the information you need. Report any irregularities to the help desk. 8	Ensure that your data is protected at home. Encrypt hard drives and password protect devices. 9	Business cards aren't always real. Do not trust someone on the basis of a business card. 10
Identity thieves may use public forums. Watch what you say. 11	Your email password could be compromised if you use the same password elsewhere. Always change your password often. 12	Luggage can be lost or stolen. Never leave your luggage unattended and clearly label it with your name, address and phone number. 13	Fake identity theft recovery services will target victims of identity theft. Don't get robbed twice: hang up on these scammers. 14	Your laptop is fragile. Place your laptop somewhere safe before falling asleep at night. 15	Even Snapchat is not safe. Photos you send to others never go away and they can be saved. 16	Viruses and malware can be anywhere. Always use antivirus protection and set it to automatically update. 17
Accidents are a leading cause of information leaks and loss. Always be careful about your actions. 18	Stay safe with mobile devices and data: always follow acceptable use policies and get approval from your IT department. 19	Protect your data when on Wi-Fi by only using secured connections. 20	Avoid donation scams by verifying the sender's identity. 21	Safety tips for travelers: leave copies of your ID and passport along with your complete itinerary with someone back home. 22	Social media can be dangerous. Use strong privacy settings to reduce the risk. 23	Scan your email messages with antivirus software. 24
Secure your work area from physical security threats. Malicious criminals use clever techniques to compromise organizations. 25	Secure your data when browsing the web by using encrypted sites. 26	Protect your data by identifying sensitive data, restricting its access, and encrypting it. 27	Avoid getting caught in a phishing expedition: hover over URLs to make sure they're legitimate. 28	"Tailgating" is a common method used to gain access to restricted areas. Don't let others in when you use your badge or key card. 29	Scam artists use your social media to make their emails more convincing. Remain skeptical about any unsolicited emails. 30	

MARCH 1

To avoid becoming a victim of a phishing expedition, call your friend or colleague if an email seems suspicious.

If you ever receive a suspicious email or text message from a work associate, friend, or relative, remain on guard. Cybercriminals can send out emails that appear to be coming from someone you trust. For optimum security, pick up the phone if a message appears to come from someone you trust but is asking for sensitive information. Do not reply until you verify its authenticity.

MARCH 2

Ask your tech-savvy children to teach you about using computers to help you learn what they are doing online.

Many adults who are not very computer-savvy have children who know much more about technology than they do. This presents a perfect opportunity to protect your kids when they go online. Have your children instruct you on how they use the computer and demonstrate what they are typically doing on the Internet, from spending time on social media, to downloading files and visiting favorite websites. This will help you learn how to best protect them while they are online.

MARCH 3

Encrypt sensitive data when it is stored on a mobile device.

Some smartphones and tablets can be fully encrypted for maximum security. If you believe the information you are authorized to store on a mobile device requires extra security, contact the Help Desk.

MARCH 4

Set your home computer to receive automatic operating system and application updates since they contain security patches.

Software developers frequently need to apply patches to fix security holes and other problems that could impact the integrity of computer operating systems and applications. For optimum security, verify that your computer's operating system and applications are set to automatically download each update and patch as soon as they become available. Otherwise, cybercriminals may take advantage of a known security hole and use it to attack your computer via the Internet. Follow the same updating procedure with your mobile devices to keep them safe.

MARCH 5

Do not give out information about fellow employees, remote network access, organizational practices, or strategies to people you do not know.

Avoid being the victim of a social engineer. If a person you don't know calls, sends an email or text, or visits you in person and asks for confidential information about your organization, do not supply any data until the person's identity has been verified.

MARCH 6

Phishers may call asking for private data. Do not give your information over the phone to anyone who calls in.

If someone calls you asking for sensitive or confidential information, do not give it to them. Instead, ask them to give you a case number or an extension number and then call back through the main number of the company that they claim to work for. If the company cannot find this case number or the extension number does not exist, it is likely that the request was a phishing attempt.

MARCH 7

Kids need extra protection online. Use a kid-friendly browser to ensure their safety.

It is important to control the content that your kids can view online. Even children who are not looking for material that is unsuitable for them could still happen upon it. To ensure your child's safety, use kid-friendly software and a kid-friendly browser. These software solutions operate like kid-friendly cable by only allowing them to access sites that are suitable for their age.

MARCH 8

You should only have access to the information you need. Report any irregularities to the help desk.

For security reasons, all employees should only have access to information on a need to know basis. This reduces the possibility of security risks. If you find that you have access to files, documents, or other data that you should not have access to, you should report it to the Help Desk. This will also ensure that you are not responsible for any issues that arise regarding the data.

MARCH 9

Ensure that your data is protected at home. Encrypt hard drives and password protect devices.

Your home computer may have sensitive personal information on it as well as confidential organization information. To ensure that your data is protected, you should encrypt your hard drives; this will keep data safe even if the hard drives are lost or stolen. Use a password to protect all of your computers and devices and make sure that all the passwords you use are completely unique.

MARCH 10

Business cards aren't always real. Do not trust someone on the basis of a business card.

Fake business cards may be used by social engineers to gain access to certain areas. If someone gives you a business card, you should still verify the information on the card. Do not take a business card as proof that someone should be allowed to access any confidential information or private areas. If you don't feel right about something, report it.

MARCH 11

Identity thieves may use public forums. Watch what you say.

Don't let your guard down on public forums. Anything you say may be used by identity thieves. Thieves can look through your public posts, profiles and social accounts to create a picture of your identity. They can find your full name, your age, your location, and your profession and they can use all of these items to compromise your identity. Remaining anonymous on the Internet is ideal.

MARCH 12

Your email password could be compromised if you use the same password elsewhere. Always use a unique password and change it often.

Your email account could be compromised if you use the same password for multiple sites and one of these other sites has a security breach. You should always set a completely unique password for your email account and you should change it often. In the event that an unknown intruder does access your account, changing your password often will limit the duration that they have access. Make sure that you don't reuse your passwords when changing them.

MARCH 13

Luggage can be lost or stolen. Never leave your luggage unattended and clearly label contact information.

Luggage can easily get misplaced or stolen while you travel. Make sure that you never leave your luggage unattended. When possible, carry your luggage with you rather than checking it in. If you have to check in luggage, pick it up as quickly as possible following your arrival. Always mark your luggage clearly with your contact information so that it can be sent to you if it is recovered.

MARCH 14

Fake identity theft recovery services will target victims of identity theft. Don't get robbed twice: hang up on these scammers.

After an incident of identity theft, you may get a call from a telemarketer offering to help you recover your stolen money or offering a service that will help secure you from future identity theft. These telemarketers are con artists who specifically target victims of identity theft. They will not recover your money; they will simply ask you to pay them for their services and will take additional money from you. Hang up immediately. Don't become a victim twice!

MARCH 15

Your laptop is fragile. Place your laptop somewhere safe before falling asleep at night.

Many people use their laptop in bed. If you leave your laptop in bed, you could risk dropping it, having it overheat or even rolling onto it and breaking it. If you use your laptop in bed at night, you should always place it somewhere safe before falling asleep. Make sure there is nothing that could spill on it, such as a glass of water on a nightstand, and that it is completely stable.

MARCH 16

Even Snapchat is not safe. Photos you send to others never go away and they can be saved.

You should never assume that anything you send to another person, whether it be text or photo, is safe from being copied. Do not send anything to another person that you would not want to see posted online. Snapchat photos can be copied with a multitude of apps that do not tell you that the photo has been saved.

MARCH 17

Viruses and malware can be anywhere. Always use antivirus protection and set it to automatically update.

Anything you do on the Internet could potentially expose you to viruses or malware. Always have antivirus protection running; never turn your antivirus protection off, even if a software program recommends that you do so. Set your antivirus protection to automatically update itself as new security risks are discovered; otherwise you may become vulnerable to newer exploits.

MARCH 18

Accidents are a leading cause of information leaks and loss. Always be careful about your actions.

Accidents happen, but they can also be disastrous. Accidents, such as accidentally leaving data in an unsecured place, are a leading cause of information leaks. Always be conscientious about your actions when you are dealing with confidential and sensitive information. If you have accidentally caused a data breach or data loss, you should immediately notify your workplace so that the issue can be dealt with in a timely fashion. Don't try to resolve the problem on your own.

MARCH 19

Stay safe with your mobile devices and data: always follow acceptable use policies and get IT approval.

Criminals and hackers are always on the lookout for unsuspecting people using improperly configured mobile devices to access valuable information. This is why you should always abide by your organization's Acceptable Use policies for mobile data and device security to make sure you aren't compromising the network. For example, use a strong password that includes numbers and upper and lower case characters. Enable the "remote wipe" feature of your smartphone so you can delete files if it is lost or stolen.

MARCH 20

Protect your data when on Wi-Fi by only using secured connections.

Wireless Internet connections work by broadcasting the data that you are sending and receiving between your device and the Internet. To ensure that your data is safe, only connect to secured wireless signals. When transmitting important personal information such as credit card information, make sure that the website you are on is using SSL and has a current and verified security certificate. A website that is using SSL should have a URL containing "https" rather than "http." On most systems, secured internet connections will have a lock icon on the left of the name of the connection.

MARCH 21

Avoid donation scams by verifying the sender's identity.

Donation scams often attempt to obtain money or personal information by relying on your sympathy for victims of illness or natural disasters. If you receive an email from someone claiming to represent a charity, use resources on the Internet to confirm that the charity is legitimate. Go to the charity's actual website to make a donation, rather than clicking on a link in the email message. Make donations directly to the charity instead of relying on an intermediary party to make the donation on your behalf.

MARCH 22

Safety tips for travelers: leave copies of your ID and passport along with your itinerary with someone at home.

When traveling, especially to an unfamiliar location on behalf of your organization, it's important to follow some basic safety tips. Make copies of important documents such as your ID, passport and the complete itinerary of your trip. Give this information to someone back at home and check in with this person periodically. This way, if you lose your ID, the person can send you a copy. If you don't check in on a regular basis, your safety person can alert the authorities that you may have gone missing.

MARCH 23

Social media can be dangerous. Use strong privacy settings to reduce the risk.

Social media accounts can give any individual enough information to be dangerous. Use strong privacy settings to reduce your exposure. You can use privacy settings to ensure only those you know can see your posts, and this can greatly reduce the amount of information a stranger can gather from you. Many social media platforms also have increased security options, requiring you to verify your identity with your phone or email address before logging in. When in doubt, refrain from sharing too much online.

MARCH 24

Scan your email messages with antivirus software.

Viruses often infect your computer via instant messages and email attachments, especially when the attachment is an executable file. Enable your antivirus software's auto-protect feature to automatically scan email attachments for viruses when the messages are downloaded. Hackers routinely create new viruses, so it's essential to keep the signature files for your antivirus software updated. Ensure your antivirus software also uses heuristic algorithms that allow the software to detect viruses based on their behavior, rather than a specific signature.

MARCH 25

Secure your work area from physical security threats. Criminals use clever techniques to attack organizations.

Be on guard against the various physical security techniques that criminals use from the inside when attacking organizations. For example, a criminal might use an expired ID card to fool the security guard or access a locked room. At large organizations, a brazen criminal might try to blend in with the crowd coming back from lunch and gain unauthorized access to the building. Put away documents containing sensitive information when you leave your work area, and log out of your computer when you take breaks or leave for the day.

MARCH 26

Secure your data when browsing the web by using encrypted sites.

When you send and receive data to and from a website, such as credit card data, you may be exposed. To ensure safer web browsing, make sure that every site that you give information to uses encryption. You may want to make sure they have an active security certificate or that they are using "https" rather than "http."

MARCH 27

Protect your data by identifying sensitive information, restricting its access, and encrypting it.

Business theft often involves the theft of data rather than physical assets. Identify sensitive information and the computers on which it's stored. Sensitive data includes data that pertains to an individual, such as credit card data, and information that applies to an entire organization, such as proprietary data. Minimize the number of computers that store sensitive data as well as the number of people with access to those computers. Store sensitive data in an encrypted format, especially when using portable storage media.

MARCH 28

Be on guard against unknown people who ask you for sensitive data.

Social engineers may try to trick you into giving away sensitive information, such as user login names and passwords or credit card numbers. They may pose as authorized users or members of a security firm, for example. Remain on guard and verify the identity of any person making an unsolicited request before you give away information by phone, email, or in person.

MARCH 29

"Tailgating" is a common method used to gain access to restricted areas. Don't let others follow you in.

Tailgating is when one person follows another person in after the first person has used their badge or key card. You should never let another person follow you into a restricted area, even if you have seen this person use their own badge or key card before; their credentials may have been revoked and you may not know.

MARCH 30

Scam artists use social media to make their emails more convincing. Remain skeptical of unsolicited emails.

Scam artists may use the information you post on social media accounts to make their phishing emails seem more legitimate. Always be skeptical of unsolicited emails. Keep as much of your personal information off of social media as possible.

APR

2018



SUN	MON	TUE	WED	THU	FRI	SAT
Create, distribute, 1 retain, and access only the minimum amount of data that you need to perform your duties.	Only deal with 2 people that you trust when participating in online auctions.	Sensitive data 3 stored on mobile devices may be easily accessed. Encrypt data on mobile devices for additional security.	When traveling, 4 only use registered taxi services, and get dropped off at a safe location.	Data breaches 5 from within do occur. Limit access to sensitive information on a need to know basis.	Spear phishers 6 target individuals with manipulative emails to trick them into giving sensitive data or infecting devices with malware.	Emails may not 7 be from who they seem to be. Don't automatically trust emails from friends and colleagues.
Everyone is 8 responsible for confidential data. Contact the help desk if you know of lost or stolen information.	Sensitive data 9 can be retrieved from old devices. Always erase devices before disposing of them.	Lost or stolen 10 laptops and mobile devices may represent a security breach. Report them immediately.	Hardcopy and 11 electronic data must be disposed properly. Wipe electronic data from devices completely and shred all hard copies.	Not all 12 websites are secure. Don't buy from websites that have no physical address.	Use encryption 13 to securely store and transmit sensitive information.	Protect the 14 data on your home computer with antivirus and antispyware software.
Verify the 15 identity of anyone who asks you for your confidential information over the phone or in person.	Only give out 16 your social security number if it is absolutely necessary and you have verified the identity of the requester.	An unsecured 17 Wi-Fi network may compromise your data security. When choosing between Wi-Fi networks, find the encrypted and trusted one.	Social media 18 apps could contain malware or Trojan Horses. Avoid installing unnecessary 3rd party apps, and restrict data sharing.	Keep in mind 19 that all of your emails and documents are official records and could be involved in litigation.	Protect yourself 20 from online fraud by working with reputable and verifiable companies.	Excessive use 21 of email and IM for personal communications is not allowed at work.
Simple 22 passwords are often easily guessed. Use capitalized letters, numbers and special characters.	All operating 23 systems can be affected by viruses and malware. Take steps to protect your system.	Social engineers 24 may use your personal data against you. Never trust anyone without the appropriate credentials.	Identity 25 thieves may use unsolicited credit offers to gather information. Consider opting out.	An improperly 26 configured Wi-Fi router can represent a huge security risk. Never install your own Wi-Fi router in the workplace.	Home wireless 27 networks are vulnerable when not properly secured with a password and an encrypted connection.	Identity theft 28 can occur anywhere. Pay with cash when your suspicions are aroused.
Revealing 29 any personal information can be dangerous. Don't include sensitive information in your usernames.	The web can 30 be a dangerous place. Turn your security settings up on your browser for additional protection.					

APRIL 1

Create, distribute, retain, and access only the minimum amount of data that you need to perform your duties.

In keeping with the records retention and destruction policy of the organization, you should only have access to the least amount of data possible to carry out the functions of your job. As a general rule, the less data that you work with, the fewer opportunities there will be for you to misplace it, accidentally expose it to unauthorized users, or have it stolen from you.

APRIL 2

Only deal with people that you trust when participating in online auctions.

When buying items via an Internet auction, it's prudent to always make sure that you are dealing with a trusted seller. Check the feedback given by other buyers to get a good idea of how reputable the seller is and avoid sellers with little or no history. If you get involved with an unscrupulous seller, you might wind up having to pay for an item that you never receive. If something doesn't feel right about an auction, trust your instincts and move along to the next seller.

APRIL 3

Sensitive data stored on mobile devices may be easily accessed. Encrypt data for additional security.

Keeping sensitive data on mobile devices can be dangerous. Data that is not encrypted on a mobile device could be easily accessed if the device is lost or stolen. If you need to keep sensitive data on your mobile device and have authorization to do so, password protect the device and consider encrypting the data.

APRIL 4

When traveling, only use registered taxi services, and get dropped off at a safe location.

Traveling can be dangerous if you aren't conscientious about your travel plans. Only use registered taxi services and don't get into an unmarked taxi or a taxi that you did not request. Know your route well enough to know whether you have deviated from it, and make sure that your taxi driver drops you off in a safe, well-lit location.

APRIL 5

Data breaches from within do occur. Limit access to sensitive information on a need to know basis.

To combat the malicious insider threats, limit the access of sensitive data on a need to know basis. Don't send any data to someone who does not need to work with this data and is not authorized by management to access the data. If in doubt, consult with your supervisor regarding who has access to what information.

APRIL 6

Spear phishers target specific individuals with manipulative emails, hoping to trick them into giving away sensitive information or infecting their computers with malware.

Spear phishing is a special type of fraud, usually conducted through email, which appears as though it comes from a legitimate source. Spear Phishers often request personal or confidential information from you, or they will attempt to trick you into installing malicious software by clicking on a link or opening an attachment. Always be suspicious of emails, even if they appear to come from a trusted source. When in doubt, call the sender and ask if they did in fact send the email.

APRIL 7

Emails may not be from who they seem to be. Don't automatically trust emails from friends and colleagues.

Malicious users can send emails that appear to have come from anyone. An email from a friend or colleague may have come from a hacked account. Contact your friend or colleague directly if you have concerns about an email they have sent to you and do not transmit personal or sensitive data through email. Do not respond directly to the email until certain it came from a valid source.

APRIL 8

Everyone is responsible for confidential data. Contact the help desk if you know of lost or stolen information.

If you believe that sensitive or confidential data has been lost, stolen, or otherwise compromised, you should immediately contact the help desk. They can identify whether a breach has occurred. This includes both electronic data and hard copies of information.

APRIL 9

Sensitive data can be retrieved from old devices. Always erase devices before disposing of them.

Desktop computers, laptop computers and mobile devices may have confidential or sensitive data on them. If disposed of improperly, this data may be accessed by anyone. Always erase devices thoroughly before disposal or use a service specifically designed for the recycling and removal of unwanted devices.

APRIL 10

Lost or stolen laptops and mobile devices may represent a security breach. Report them immediately.

Lost or stolen laptops or mobile devices can potentially be used to access sensitive and confidential data, even if the data is not stored directly on the device. If the device is ever used to connect to the organization's network or accounts, it may still pose a risk. If a device that you use to access the organization's data is either lost or stolen, you should report it immediately to IT security.

APRIL 11

Hardcopy and electronic data must be disposed properly. Wipe electronic data from devices and shred copies.

Data that is not disposed of properly could be recovered or accessed by a malicious user. For electronic devices, special data wiping procedures must be used to ensure that data is completely removed from the device. For hard copies, documents must be shredded to ensure that they are properly destroyed.

APRIL 12

Not all websites are secure. Don't buy from websites without a physical address.

Anyone can start an online shop. Before buying from an online store, look up the store's physical address. Do not buy an item from a website that lists only a P.O. Box address. A reputable store should have a physical address even if it does not have a physical location. Otherwise your payment information, such as credit cards and debit cards, may be at risk.

APRIL 13

Use encryption to securely store and transmit sensitive information.

Electronic sensitive data should always be password protected and encrypted when it is stored or transmitted. Encryption is a way of scrambling data so that only someone with an appropriate key can read it. Hardcopy sensitive data should always be stored under lock and key.

APRIL 14

Protect the data on your home computer with antivirus and antispyware software.

Workplace computers and devices are not the only ones that should be secured with antivirus and antispyware software. Your home computer should have the same level of protection, especially if you are authorized to use it to access workplace information.

APRIL 15

Verify the identity of anyone who asks you for your confidential information over the phone or in person.

Social engineering is the art of tricking people into revealing data to those who are not authorized to access it. Social engineers may pose as security technicians or officials at your bank or data center and then ask you for your login information. Always verify their identity before giving out your information. Call the person back at a number you have determined to be legitimate, or check an individual's government-issued photo ID when meeting in person before you release your personal details.

APRIL 16

Only give out your social security number if it is absolutely necessary and you have verified the identity of the person requesting it.

Your Social Security Number is often requested and used by organizations to help identify you and to access your confidential records. If someone asks for your Social Security Number, ask if there is some other way to verify your identity. Only give your information out if you have verified the requester's identity, for example, by calling a known and publicly posted phone number. Never give out your Social Security Number to an unknown person who calls you.

APRIL 17

An unsecured Wi-Fi network may compromise your data security. When choosing between Wi-Fi networks, find the encrypted and trusted one.

When choosing a Wi-Fi network, you may find that you have multiple choices. A Wi-Fi network that is not secure could compromise your data by allowing another person to intercept it. Think about which network you join. A trustworthy network will be encrypted. You should see a "lock" icon next to the network, and there should be a security method listed when you view connection details.

APRIL 18

Social media applications could contain malware or Trojan horses. Avoid installing unnecessary 3rd party apps, and restrict your sharing settings.

Social media applications can sometimes represent a risk; they may be embedded with malware or Trojan Horses. 3rd party social media applications often request access to your personal data. Avoid unnecessary risk by only installing 3rd party applications that you need and are popular. Limit the amount of data you share with applications through your social media account settings.

APRIL 19

Keep in mind that all of your emails and documents are official records and could be involved in litigation.

Anything you commit to writing, including anything printed, created electronically, or recorded, becomes an official record of that information and can be accessed later and referenced in litigation. It's important to follow regulations regarding the amount of time records need to be retained and destroyed and to be aware that all documents may become involved in legal situations.

APRIL 20

Protect yourself from online fraud by working with reputable and verifiable companies.

Never work with companies online that cannot be verified and that aren't reputable and known to be trustworthy. Larger companies such as eBay and Amazon provide assurances for consumers and are well-known enough to be considered trustworthy. When using a new company, verify they are trustworthy by using resources such as online reviews and the Better Business Bureau.

APRIL 21

Excessive use of email and IM for personal communications is not allowed at work.

Messaging and communication systems such as email and instant messaging can quickly become a time sink or even a security risk if they are used heavily throughout business hours. Ensure that email and IM are not used for excessive personal communications while you are at work; restrict these modes of communication to business purposes and ensure that no confidential information is shared with those that are not privileged to it.

APRIL 22

Simple passwords are often easily guessed. Use a mix of upper & lower case, numbers, and special characters.

When choosing a password, you should avoid simple passwords because they could be easily guessed. Instead, create a password that includes a mix of upper and lower case characters. Including at least two numbers and at least one special character will greatly increase the complexity of your password and ensure that they cannot be guessed.

APRIL 23

All operating systems can be affected by viruses and malware. Take steps to protect your system.

Many believe that Mac computers are immune to viruses and malware, but this is not true. Any operating system, and even mobile devices such as smartphones and tablets, can acquire viruses and malware. To protect your system, ensure that you have an updated security system running at all times, scan anything you add to your computer, and avoid opening programs and links that seem suspicious or aren't from someone you trust.

APRIL 24

Social engineers may use your personal data against you. Never trust anyone without proper credentials.

Social engineers are individuals who will call you and pretend to be either within your organization or with a service that is attempting to work with your organization. They will often pretend to need confidential information from you and will claim to have the clearance to access this information. A social engineer might call and say that they are troubleshooting your web service and need an administrative password; they may use your social media to determine your position within the organization. Never give out any information to anyone without verification of their credentials from management.

APRIL 25

Identity thieves may use unsolicited credit offers to gather information. Consider opting out.

Everyone gets unsolicited credit offers in the mail, but not all of these credit offers are legitimate. Identity thieves may send out these offers in an attempt to gather personal information from you. Consider opting out of all unsolicited credit card offers. If you are interested in a credit card, apply directly with the credit card service rather than responding back to unsolicited mail and only work with reputable credit card companies.

APRIL 26

An improperly configured Wi-Fi router could be a huge security risk. Never install your own Wi-Fi router at work.

Though a personal Wi-Fi router may seem convenient, it can be a substantial security risk within a business environment. Rather than attempting to install your own personal Wi-Fi router, ask the help desk if you need Wi-Fi access.

APRIL 27

Home wireless networks are vulnerable when not properly secured, password protected, or encrypted.

Intruders who break into your wireless network could potentially gain access to your personal and confidential documents or to work documents that you have accessed from home. To reduce the possibility of risk, you should require a login and password to connect to your network and you should ensure that it is encrypted. Use WPA rather than WEP; WEP is an old type of security that is not very effective. If your wireless router only offers WEP security, it may be time to upgrade.

APRIL 28

Identity theft can occur anywhere. Pay with cash when your suspicions are aroused.

When you travel, simply using your credit card could potentially expose you to the risk of identity theft. If you begin to feel wary about using your credit card, you should trust your instincts. Pay cash rather than handing over your credit card. Your gut knows best. If you distrust the situation, make sure that you do not reveal how much cash you have, as this could make you a target.

APRIL 29

Revealing any personal information can be dangerous. Don't include sensitive information in your usernames.

Including sensitive information in your social media and other online account usernames could inadvertently lead to identity theft. Do not put information such as your age in your username; an identity thief could use this information to derive your date of birth. Similarly, don't reveal to the public maiden names, locations of birth, or current addresses.

APRIL 30

The web can be a dangerous place. Turn your security settings up on your browser for additional protection.

There are many malicious applications and security vulnerabilities you could be exposed to online through your web browser. Most browsers, such as Internet Explorer or Chrome, have a selection of security settings ranging from lowest to highest. To give yourself additional protection against malicious attacks, choose higher levels of security settings. These security settings will block certain types of scripts from running and reduce the permissions settings of the websites.

MAY

2018



SUN	MON	TUE	WED	THU	FRI	SAT
		Only store personally identifiable information (PII) on authorized systems. 1	When staying at a hotel, store your computers, devices, and other valuable items in a safe or keep them locked in your luggage. 2	Do not comment on investigations or pending litigation via email or any other method, unless necessary. 3	Do not use debit cards for online purchases. Criminals may intercept your data and use it to commit fraud. 4	Do not use email or instant messaging for personal business or solicitation while at work. 5
Use unique and memorable phrases to create secure passwords that are easy for you to remember. 6	Protect your computer from Trojan Horse programs that look innocent but are not. 7	Do not fall for scams where criminals impersonate people you know via social media. 8	Configure your home computer to use a firewall and AntiSpyware software to provide a safer web browsing experience. 9	Never open unsolicited bulk advertising that you receive via email. 10	Never leave printouts of sensitive documents at your desk when you step away. Lock and protect your data. 11	Shred all hardcopy files containing personally identifying information (PII) before you dispose of them. 12
If you must leave a laptop or mobile devices in a locked car, store them in the trunk where criminals cannot see them. 13	Certain types of attachment are more dangerous than others. Never open .Exe files from your email. 14	Posting your email on websites could open you up to risks. 15	Printed items can be compromised. Never leave sensitive or confidential documents on a printer or fax machine. 16	Personally identifiable information (PII) must be protected. Never transmit PII through unsecured emails. 17	Lost or stolen devices could lead to a data breach. Always secure with a password, screensaver, and encryption. 18	Electronic and physical files must be retained during a litigation hold. Never delete or throw away these items. 19
Data sent via email may be accessible to others. Using a password-protected, encrypted zip file will protect data. 20	Data not properly backed up could be lost forever. Protect the data on your home computer with a cloud backup system. 21	Your mother's maiden name can be used by identity thieves. Make sure you keep it safe. 22	Twitter is a completely public social media platform. Never post any PII data on twitter. 23	Your email software can learn to identify spam. Flag unwanted emails as spam to ensure they are sorted correctly. 24	Public computers may be infected with malware or have other security issues. Never enter personal data on untrusted devices. 25	Fighting back doesn't work with bullies, especially on the web. Educate your child on the proper response to cyberbullying. 26
The internet can be a dangerous place. Educating your kids is the vital first step towards protecting them. 27	Cybercriminals can listen to your internet activity. Always use encryption when transmitting sensitive data. 28	Your data may be vulnerable to permanent loss. Use an external hard drive to backup your home computer. 29	Cyberbullying isn't just a matter for school officials. It's also a crime. Report any instances of cyberbullying to your local authorities. 30	Malicious insiders are a serious threat. Always use a password protected screen saver at work. 31		

MAY 1

Only store personally identifiable information (PII) on authorized systems.

The PII that your organization collects and stores must be safeguarded against unauthorized access. Otherwise, criminals could use the information to commit fraud and perpetrate identity theft against the people whose information you are charged with keeping secure. For best practices, only store PII on systems that have been authorized by the IT department. They are built and configured with security in mind to protect PII according to legal requirements.

MAY 2

When staying at a hotel, store your computers, devices, and other valuables in a safe, locked location.

Criminals prey on people who are traveling, and if they get a hold of your laptop, tablet, or smartphone in your hotel room, they may access your organization's sensitive data. Any time that you need to work remotely and are staying in a hotel, protect your organization's information by storing all devices as securely as possible. If there is no safe in your room, ask the front desk if they have a general-purpose hotel safe that you can use. Secure your items by locking them up in luggage when they are not in use.

MAY 3

Do not comment on investigations or pending litigation via email or any other method, unless it is necessary.

Remember that all emails or any other form of digital communications are admissible in a court of law, so if you are not directly involved with an issue, internal investigation, or pending litigation avoid discussing it with others or commenting on the situation.

MAY 4

Don't use debit cards for online purchases. Criminals may intercept your data and use it to commit fraud.

While it may be convenient for you to enter your debit card information online to make a purchase, this is a dangerous practice that could allow criminals to steal your banking data. They can then use it to commit fraud and drain your bank account. Instead, use a credit card that is designated just for online use to ensure maximum protection against cyber thieves. For added safety, check your bank statement for unusual activity on a regular basis.

MAY 5

Do not use email or instant messaging for personal business or solicitation while at work.

Although there may be some exceptions, most organization's acceptable use and auditing policies prohibit using a work email account to send out messages for non-work related issues.

MAY 6

Use unique and memorable phrases to create secure passwords that are easy for you to remember.

Robust password management takes only a modest amount of time and effort, and the reward is improved security, which is essential when it comes to protecting your organization's sensitive data. Come up with a phrase that has meaning to you, such as "My 2 favorite pizza toppings are mushrooms and sausage." Then, simply take the first letter of each word in the phrase to create your password, which in this case would be "M2ftamas." This ensures that you are not using a password that is easily guessable. Including numbers, special characters, and a mix of upper and lowercase letters helps ensure the strongest possible password.

MAY 7

Protect your computer from Trojan horses – programs that look innocent but are not.

Cybercriminals seeking to break into people's computers will use a type of malware known as a "Trojan Horse." In the ancient Greek myth, a Trojan Horse was a gift of an enormous hollow horse, inside of which soldiers hid until they were let inside the city gates. Once inside, they commenced with their attack. Modern Trojan Horses are malware disguised as something innocent, such as a video player application or an emailed file attachment. Once you click on them, they can infect your computer with malware or spyware. Protect your computer against Trojan Horses with a firewall and antivirus software.

MAY 8

Do not fall for scams where criminals impersonate people you know via social media.

cyber thieves will try to make you think they are a known friend via social networks. If you receive a suspicious email or post via sites such as Facebook or Twitter, be on guard. A hacker may have taken over your friend's account, and be using it to send out messages to every contact to scam them out of money. For example, you may get a message that a friend who is traveling abroad, has lost his luggage and wallet and needs you to transfer funds immediately to help him get home. Verify that the message is real before taking action.

MAY 9

Configure your home computer to use a firewall and antispyware software to provide a safer web browsing.

Always keep your home computer's operating system up to date, as well as applications such as your web browser and any add-ons, such as Adobe Acrobat. Configure the latest version of your computer's firewall and antispyware software to make sure you are protected against the latest threats from hackers and cybercriminals. If you don't take these basic precautions, you run the risk of an attacker putting malware on your computer that can capture your login data, letting thieves access your confidential data.

MAY 10

Never open unsolicited bulk advertising that you receive via email.

When you get what is obviously an example of unsolicited bulk advertising in your inbox (Spam), do not click on the message or open it. Just clicking on the message can signal to the sender that your email address is valid and will encourage him or her to send you more. The message might also contain an attachment with malware that will infect your computer or mobile device. Mark the message as "Spam" to train your email program to ignore similar messages in the future.

MAY 11

Never leave printouts of confidential or sensitive documents at your desk when you step away. Lock & protect.

When you leave your work area unsecured and unsupervised, a criminal trespasser or a malicious insider could access your desk and see sensitive documents that you've left lying about. It only takes a few seconds to snap a photo of a document, photocopy it or outright steal it, which can compromise the security of the organization. Lock up your confidential documents in a filing cabinet or a safe whenever you leave the area.

MAY 12

Shred all hardcopy files containing personally identifying information (PII) before you dispose of them.

Criminals often go through unguarded garbage cans and recycling bins in an attempt to find documents that contain personally identifying information (PII). They can use PII to steal people's identities, such as of your fellow employees or the clients and customers the organization serves. By shredding all hard copy files with PII before you put them in the trash or send them for recycling, you will prevent criminals from accessing confidential data.

MAY 13

If you must leave a laptop or mobile devices in a locked car, store them in the trunk out of view from criminals.

Your laptop or mobile device sitting on the passenger seat of your vehicle is a tempting target for potential thieves. If you must store a laptop or mobile device while working on the road, keep the device locked in the trunk. Look for a safe place to park, and enable the vehicle's alarm system for added security.

MAY 14

Certain types of attachment are more dangerous than others. Never open .Exe files from your email.

While viruses and malware can potentially be embedded in most types of files, there are certain types of files that you should never open regardless of the source. Files that end in .exe are executable programs and there should never be a reason for anyone you know to send you a .exe program. Files that end in .doc, .pdf or .xls are more likely to be safe but they should still not be opened if sent to you by an unknown sender. Only the last three letters matter in a file type. For example, a file ending with .doc.exe is still considered a .exe file and should not be opened.

MAY 15

Posting your email on websites could open you up to risks.

If you post your email address online, it can easily be taken and used for malicious purposes. You may begin to receive large amounts of Spam emails, or you may even get viruses sent to you. To mitigate this, alter your email address by changing the "@" symbol to the word "at" when displayed on your website.

MAY 16

Printed items can be compromised. Never leave sensitive or confidential papers on a printer or fax machine.

Physical documents can be risky because they can be easily viewed by anyone. To avoid compromising sensitive or confidential documents, always ensure that they are never left on a printer or fax machine. Documents that are not in use and do not need to be stored any longer should be shredded when appropriate per the records retention policy.

MAY 17

Personally identifiable information must be protected. Never transmit PII through unsecured emails.

Standard emails are stored in plain text and can be easily accessed by anyone who can monitor the network or an Internet service provider. To protect PII, you should only transmit PII through a secure email system that has been approved by the IT department.

MAY 18

Lost or stolen devices could lead to a data breach. Secure devices with a password, screensaver, & encryption.

If you access confidential or sensitive data through a mobile device, it could potentially be accessed when your device is lost or stolen. You can protect your device by securing it with a password and ensuring that it will lock with a password if it is left idle. You should also encrypt any important information on your hard drive to further protect yourself. An unsecured and unencrypted hard drive can be accessed directly even if the computer cannot be logged into.

MAY 19

Electronic and physical files must be retained during a litigation hold. Never delete or throw away these items.

When the organization is on a litigation hold, you must avoid deleting electronic files or destroying hardcopy files related to the litigation. The organization is required to maintain these files throughout the litigation proceedings. Litigation holds often affect all forms of media, including tape drives, backups of your data, and removable media containing the information.

MAY 20

Data sent through email may be accessible to others. You can protect your data by using a password-protected, encrypted ZIP file.

If you send files through an email, others may be able to access and read the data. Rather than sending an unencrypted file, you can add it to a ZIP file archive, which can password protect and encrypt the data. After sending your file, you should call the recipient and give them the password over the phone. Never transmit the password electronically, as an electronic communication may be intercepted along with the file.

MAY 21

Data not properly backed up could be lost forever. Protect data on your home computer with a cloud backup.

If you don't backup your data regularly, you may lose it. You can protect yourself through the use of a cloud backup system. A cloud backup system can usually be accessed from anywhere in the world and any device, provided that you have the password. Cloud backups are extremely stable and will back up your system automatically. Further, they are in a separate physical location from your data, allowing you to protect against fire and flood. Due to accessibility, use strong passwords to reduce security risk.

MAY 22

Your mother's maiden name can be used by identity thieves. Make sure you keep it safe.

In addition to passwords and birthdays, your mother's maiden name can also be used to steal your identity. A mother's maiden name has long been used as a verification question for financial accounts, and social media has made it so that maiden names are often displayed alongside married names.

MAY 23

Twitter is a completely public social media platform. Never post any personally identifiable data on Twitter.

Everything you post on Twitter is made public and is indexed by search engines. You should never post information that could be used to identify you on social media accounts, nor should you post any sensitive or confidential workplace information such as information about a client or an account. You should also avoid using a username that might include identifiable information.

MAY 24

Your email software can identify Spam. Flag unwanted emails as Spam to ensure emails are sorted correctly.

Don't just delete Spam mail. If you flag your Spam mail as Spam, your email software will move it to your Spam folder and will know to mark similar emails as Spam in the future. This will reduce the amount of time it takes to look through and sort your emails and will ensure that you don't accidentally open a Spam email that could potentially contain malicious materials.

MAY 25

Public devices may be infected with malware. Never enter personal data on untrusted computers.

Public computers, such as those at hotel business centers, libraries, or Internet kiosks may not be secured. They could be infected or have keyloggers on them, which could potentially compromise your data. You could also forget to log out, leaving your account vulnerable to intrusion. To avoid this, don't log into your account on a public computer and use a secured connection.

MAY 26

Fighting back doesn't work with bullies, especially on the web. Educate your child on proper responses.

Your child should never attempt to fight back against a cyber bully. There could be legal repercussions and the situation could simply escalate. Everything that is posted on the web will remain on the web forever. Rather than fighting back online, you should work with your child to fight back through the school system and legal channels. Document everything and report to authorities.

MAY 27

The internet can be a dangerous place. Educating your kids is the vital first step towards protecting them.

The Internet is now used extensively through the school system, and children are introduced to it at an early age. You can protect your children by setting firm ground rules and educating them about dangers. Let them know what they can and can't do while they're online and ensure that their online time is limited. Place the computer in an area of your home that is highly visible.

MAY 28

Cybercriminals can listen to your internet activity. Always use encryption when transmitting sensitive data.

Any time you send or receive data, even through a website, others may be able to hijack and read this data. To protect yourself, use encrypted signals. Never use a wireless connection that isn't protected and only use websites that use HTTPS when sending confidential information. Use a firewall and keep your security protection on at all times for additional protection.

MAY 29

Your data may be vulnerable to permanent loss. Use an external hard drive to backup your home computer.

Everyone has important information on their computer. If your hard drive fails or your computer otherwise ceases to work, you could lose essential documents that you need. You can avoid this by keeping an external hard drive that is set to automatically back up your documents. The only downside to this is that it could be damaged by flood, fire, or another event that could damage your home. Additionally backing up your system to a cloud storage network could avoid this risk.

MAY 30

Cyber bullying isn't just a matter for school officials. It's also a crime. Report to your local authorities.

Cyber bullying is a crime. If your child is the target of cyber bullying, you should document everything and contact both your child's school and the local authorities. This will increase the likelihood that the matter will be dealt with in an appropriate and productive way. It will also send a message to your child that they are protected and that what is happening to them is wrong.

MAY 31

Malicious insiders are a serious threat. Always use a password protected screen saver at work.

Many security breaches are internal rather than external. Malicious insiders may be able to access data through your computer at work. Using a password protected screensaver will ensure your computer cannot be accessed by someone else at work even when you leave your desk. Always lock your computer and set your screen saver to turn on automatically.

JUN

2018



SUN	MON	TUE	WED	THU	FRI	SAT
					<p>1 Avoid downloading free software. Free software might contain viruses, adware, or spyware.</p>	<p>2 Remember that all computer and network activity at the workplace is monitored for abuse.</p>
<p>3 Check your credit report if you think you might be the victim of identity theft.</p>	<p>4 Gut feelings are there for a reason. If something doesn't feel right, trust your instincts.</p>	<p>5 If your credit card is rejected, it may be a sign of identity theft. Take action immediately by contacting your bank.</p>	<p>6 Public Wi-Fi connections are often poorly secured. Protect yourself by using SSL connections.</p>	<p>7 Use parental controls on your home computer to protect your children by blocking inappropriate sites.</p>	<p>8 PII is typically protected through privacy laws.</p>	<p>9 Use access control lists to protect files stored on your organization's network.</p>
<p>10 Protect your computer. Malicious attackers can scan every computer on the Internet for undefended systems, so take precautions.</p>	<p>11 Lock away valuable data even inside secure buildings, since malicious individuals could penetrate our entry controls.</p>	<p>12 Protect your social security number: Never print it on checks and don't carry your SS card with you.</p>	<p>13 Only use trusted networks when connecting to the Internet. Cybercriminals can create fake hotspots to steal your data.</p>	<p>14 Your personal computer may become the target of attacks. Use a personal firewall to protect yourself.</p>	<p>15 Access badges and key cards are vital to physical security. Never let anyone else use your access & report it if it goes missing.</p>	<p>16 Suspicious emails could be attempts to gather sensitive data. Either delete suspicious emails or contact the sender directly.</p>
<p>17 Cyber bullying can be difficult to prove. Make sure all communications are well documented and saved.</p>	<p>18 Your computer can be physically damaged by weather and moisture. Always keep your home computer in a safe place.</p>	<p>19 Only install organization-approved applications on your computer.</p>	<p>20 Email and instant messaging services can be used to spread malware.</p>	<p>21 Data sent via email is not encrypted by default. Use secured, encrypted emails to ensure that your data is safe.</p>	<p>22 Mobile media can represent a security risk for personally identifiable information (PII).</p>	<p>23 Working remotely can carry security risks. Use a laptop cable lock for long training sessions or conferences.</p>
<p>24 Always make sure that you connect to the right Wi-Fi network. Network names may be misleading.</p>	<p>25 An improperly configured Wi-Fi router can be a huge security risk. Never install your own Wi-Fi router at work.</p>	<p>26 Turn off facial recognition and tagging in social media if you don't want unwanted information linked to you.</p>	<p>27 Games or animations emailed to you may have malware or viruses. Never accept or install these programs.</p>	<p>28 Unsolicited discount offers sent via IM are unsafe. Never click on links sent to you over IM from unknown individuals.</p>	<p>29 Never put sensitive or confidential information in an unauthorized system.</p>	<p>30 Confidential emails can be read over your shoulder. Make sure you have privacy when sending a confidential email.</p>

JUNE 1

Avoid downloading free software. Free software might contain viruses, adware, or spyware.

Free software is notoriously susceptible to viruses and other malware. If you do need to download free software, consult with your IT department regarding whether or not it is from a reputable company. Always scan software you download for viruses, regardless of source, and be cautious during the install process. A free software program may ask you to install software you don't need.

JUNE 2

Remember that all computer and network activity at the workplace is monitored for abuse.

Your IT department has an acceptable use policy (AUP) for computer systems, networks, and websites. Network and system administrators routinely enforce an organization's AUP by reviewing audit trails of user activity, which includes a variety of specific reports. For example, an exception report lists actions users unsuccessfully attempted to perform during the report's time period.

JUNE 3

Check your credit report if you think you might be the victim of identity theft.

Identity theft is a growing problem and criminals will try to steal from you by hijacking your personal or work credit card. If you suspect that a criminal has stolen your credit card to make unauthorized purchases, check your credit report as soon as possible. Alert your financial institutions about any suspicious or fraudulent charges. Contact any of the three major credit bureaus (Equifax, Experian, or TransUnion) to request a free credit report.

JUNE 4

Gut feelings are there for a reason. If something doesn't feel right, trust your instincts.

Often, you may pick up on suspicious situations subconsciously before you can consciously recognize them. If you feel troubled by an email, instant message, or even phone call you should trust yourself and investigate further. You may be the target of a scam artist. There is nothing to be lost by checking.

JUNE 5

If your credit card is rejected, it may be a sign of identity theft. Take action immediately.

Having your credit card inexplicably rejected isn't just embarrassing--it can also be a warning sign. If your credit card is rejected you should immediately call the number on the back of the card to talk to your credit card company. Your credit card could have been frozen due to suspected identity theft. Many banks will freeze your credit card if they see you making purchases in an area far away or completing transactions that are otherwise unusual for you. Your card could also potentially be declined because an identity thief has maxed it out. Either way, you will want to resolve the situation quickly.

JUNE 6

Public Wi-Fi connections are often poorly secured. Protect yourself by using SSL connections.

Public Wi-Fi connections may not have appropriate encryption or security. Secure Sockets Layer (SSL) connections are encrypted methods of connecting to the web. Whenever you connect to sensitive data through a website you should be using an SSL connection. You can identify a website that is protected by an SSL connection by looking for "https://" rather than "http://" at the beginning of the URL. An SSL connection will also have a lock icon next to the URL.

JUNE 7

Use parental controls on your home computer to protect your children by blocking inappropriate websites.

There are many websites with adult materials that may be easily accessed by children. When your children are browsing the web, you can protect them by using parental controls to block inappropriate websites. You can install software that is specifically meant to do this, and most browsers today come with extensions or applications that can be used for web filters and parental control.

JUNE 8

Personally identifiable information (PII) is typically protected through privacy laws.

PII, or Personally Identifiable Information, is a protected subset of information that is considered sensitive and confidential. This data is almost always required to be secured by local privacy laws. If you are not clear about the requirements for compliance regarding PII, or if you're not sure whether you deal with PII, you should contact your supervisor immediately. Proper protocols and technology must be in place to protect PII.

JUNE 9

Use access control lists to protect files stored on your organization's network.

When it comes to storing files on your organization's network, it's crucial to control access to sensitive information. Use Access Control Lists, or ACLs, to safeguard your data. An ACL specifies the access rights that each person has to any particular item on the network including directories, groups of files, and individual documents. With an ACL, you can designate whether a person or a group of people (such as all your organization's programmers or managers) can read or change a file, copy or move files from one directory to another, or run an application.

JUNE 10

Protect your home computer. Malicious attackers can scan computers online for undefended systems.

An unprotected computer that's always connected to the Internet can seem like an unlocked door to cybercriminals. Use a password that doesn't appear in the dictionary (combine letters and numbers) and change it on a regular basis. Install a firewall on your desktop or laptop computer to protect your equipment against unauthorized access from hackers. When they run scans for unsecured ports on your computer, the firewall will block them. When not using your computer, turn it off or put it to sleep.

JUNE 11

Lock away valuable data even inside secure buildings. Malicious individuals could penetrate entry controls.

Once a malicious person or criminal gains physical access to your organization's building, they can use a number of techniques to steal data. They will shoulder surf (looking at screens as people work on their computers), eavesdrop on conversations, and even rifle through your desk, purse or wallet for information. Lock away sensitive information in your desk or filing cabinet, use a password-protected screensaver and securely store your personal belongings to foil them.

JUNE 12

Protect your social security number: Never print it on checks and don't carry your SS card with you.

Social Security numbers were designed to be used for tracking benefits for Americans, but now a wide variety of institutions use them to identify people, such as banks and medical organizations. Do not pre-print your SS number on checks, because once you issue a check, you have no idea what kinds of people will have access to it. Combined with your name, address and other details, criminals can use your SS number to wipe out your bank account and steal your identity. Avoid carrying your SS card with you.

JUNE 13

Only use trusted Wi-Fi networks. Cybercriminals create fake hotspots to steal your data.

When away from the office or your home network, you may be tempted to use a free Wi-Fi connection to get on the Internet. For example, you go to a coffee shop and want to check your email or do some online research. However, criminals can easily set up a free, innocent-looking hotspot that gives you online access while eavesdropping on all your data. Avoid untrusted public Wi-Fi spots when working with your organization's sensitive data.

JUNE 14

Your personal home computer may become the target of attacks. Use a personal firewall to protect yourself.

To ensure that intruders cannot get into your home computer and steal or manipulate your data, use a personal firewall. Most computers will come with a firewall, such as the "Windows Firewall," already installed – be sure it is turned on. You may also want to invest in a subscription-based antivirus and malware solution that also includes virus scanning and firewall protection. Your firewall must remain active at all times to ensure that you are protected.

JUNE 15

Access badges and key cards are a vital component to physical security. Never let anyone else use your access badge or key card and report it immediately if it goes missing.

Access badges and key cards are used to physically secure areas of a workplace and reduce the possibility of internal theft. You should never let anyone else use your access badge or key card. If you lose your badge or card, immediately report it to security so that it can be disabled. Getting it replaced is better than experiencing a potential security breach.

JUNE 16

Suspicious emails could be attempts to gather sensitive or confidential information. Either delete suspicious emails or contact the sender directly.

If you receive a suspicious email that asks for sensitive or confidential information, whether it be personal information or workplace information, you should delete the email. If the email came from someone that you know or do business with, send an email back or call them directly to verify that they sent the email. Only send an email back if you are certain that it came from the email address of the person you know.

JUNE 17

Cyberbullying can be difficult to prove. Make sure all communications are well documented and saved.

Cyberbullying can occur through instant messenger or through social media platforms. It can be difficult to prove cyberbullying because the perpetrators may delete their accounts or posts. If your child is being bullied, make sure that you print physical copies and save digital copies of the bullying so that it cannot be erased. Document everything; cyberbullying is a crime.

JUNE 18

Your computer can be physically damaged by weather & moisture. Always keep your computer in a safe place.

Your home computer is not only vulnerable to cyber attack. It's also vulnerable to fires, floods, and heat. Make sure that your home computer is placed in a cool, dry part of the home. Your computer should ideally be elevated off the floor to avoid dust and dirt.

JUNE 19

Only install organization-approved applications on your computer.

Software that is found online – whether commercial, public domain, freeware, or shareware – could potentially be embedded with malware or Trojan Horses. Always acquire your software through a reputable source, and be extremely skeptical about freeware, public domain, and shareware programs. Before installing anything, scan it with your virus and malware protection software and make sure that your antivirus solution is running at all times.

JUNE 20

Email and instant messaging services can be used to spread malware.

Messages sent through email and IM may link to malware or viruses. You should avoid clicking on links or installing files that you receive through these services – even something that looks like a document or an image may be unsafe, especially if it comes from an unknown sender.

JUNE 21

Data sent through email is not encrypted by default. Use secured, encrypted email to ensure your data is safe.

Sending data through ordinary email is extremely unsafe; anyone who can tap into the lines between you and the recipient can look at your email or the recipient's email and steal your information. If you need to send personal, confidential, or sensitive information through email, use a secured email service. Secured emails are encrypted and will be protected against theft. You may ask the Help Desk for guidance on how to send a secured email.

JUNE 22

Mobile media can represent a security risk for personally identifiable information (PII). Avoid putting any PII on a mobile device without permission.

There are many security risks associated with the use of mobile media; it may fall into the wrong hands and be compromised. Seek written permission from management before placing PII on a mobile device or accessing PII from a mobile device.

JUNE 23

Working remotely can carry some security risks. Use a laptop cable lock for training sessions or conferences.

When working remotely, there may be personal or confidential information on your laptop. If you are working on your laptop for long periods of time in a public place, consider using a laptop cable lock. A laptop cable lock will prevent the possibility of the physical theft of your computer, should you need to walk away from the device. Even a computer that is password protected and encrypted could pose a security risk if the entire device is stolen.

JUNE 24

Always make sure that you connect to the right Wi-Fi network. Network names may be misleading.

Whenever you're connecting to a new Wi-Fi network, you should ask someone what the correct Wi-Fi name should be. You should never assume based on name which Wi-Fi connection is the correct one; anyone can create a Wi-Fi access point under any name designed to collect information. A Wi-Fi network named "CoffeeShopGuests" at a coffee shop may be created by someone who is actually down the street. Once you are connected to a Wi-Fi access point, the data you transmit can become vulnerable.

JUNE 25

An improperly configured Wi-Fi router can be a security risk. Never install your own Wi-Fi router at work.

Though a personal Wi-Fi router may seem convenient, it can be a substantial security risk within a business environment. Rather than attempting to install your own personal Wi-Fi router, ask the Help Desk if you need Wi-Fi access.

JUNE 26

Turn off facial recognition and tagging in social media if you don't want unwanted information linked to you.

On social media accounts, facial recognition and tagging may be used to automatically identify you within photographs. This is not always desirable, especially if you like to separate your work life from your personal life. You should always turn off facial recognition in your account settings. You may also alter your settings so you can't be tagged in photographs without your consent.

JUNE 27

Games or animations emailed to you may have malware or viruses. Never accept or install these programs.

Games or animations that are sent to you through email may have malware or viruses contained within them. This is true even if they are from a trustworthy source; the sender may not realize they are infected themselves. Never accept or install any programs sent to you via email; only acquire software through reputable vendors and always scan anything you install with a virus scanner.

JUNE 28

Unsolicited discount offers via instant message is unsafe. Never click on links sent by unknown users over IM.

Unsolicited discount offers may be sent to you via an IM to collect personal data from you, or to infect your system with malware. Never click on links that are sent to you over IM from an untrusted source and be suspicious of links even if they seem to have been sent to you from a known source; some viruses may hijack user's ID and send links or files out under their name.

JUNE 29

Never put sensitive or confidential information in an unauthorized system.

Unauthorized systems, such as web mail services, cloud storage services, or hosting services, may not be secured or trustworthy. You should never put sensitive or confidential information on these systems. Business-related data should only be stored on systems that have been specifically designated for business use.

JUNE 30

Confidential emails can be read over your shoulder. Be sure you have privacy when sending email.

Not all security and data breaches need to be high tech. Confidential or sensitive information could be gathered by simply looking over your shoulder as you send an email. As an example, banking data could be memorized at a glance by someone walking past. Always make sure that no one else is in view of your screen when you send confidential information.

JUL

2018



SUN	MON	TUE	WED	THU	FRI	SAT
Learn about the classification and sensitivity levels of data used in your organization, and protect it accordingly. 1	Safeguard personally identifiable information. Follow your organization's data retention and destruction policies for PII. 2	Keep devices and laptops with you when working remotely. Thieves will steal unattended equipment. 3	Only write down and store essential and necessary information. 4	Stay one step ahead of credit card thieves: devote a single credit card for online purchases to minimize your risk. 5	New threats occur all the time. Protect your web browsing by keeping your plugins updated. 6	Public Wi-Fi is insecure. Do not use banking websites when on public Wi-Fi. 7
Do not use email or IM to send or retransmit inappropriate content. 8	Change your password often. Rigorous password management helps protect your organization's confidential information. 9	Use anti-spyware software to help prevent hackers from monitoring your computer activity. 10	Keep your data secured from cyber criminals through privacy, encryption and good habits. 11	Protect PII by only sharing information with those that need to know. 12	Get prior approval before accessing workplace information on a personal computer or mobile device. 13	Be suspicious of URL shortener links. Use a preview tool to check suspicious shortened URLs before clicking. 14
Stick to reputable news sites during major events. Criminals use SEO to trick you into visiting malware sites. 15	Never forward emails that you think might be infected with malware. 16	Shorter passwords can be guessed easily by hackers. Always use long passwords. 17	Malware hides itself as anti-virus software solutions. Never install software when sent unsolicited alerts. 18	People may be listening to you speak. Don't talk about sensitive information when in public. 19	If an email is suspicious, delete it. 20	Pirated copies are illegal. Never make pirated copies of software, movies, music, or other media. 21
Keeping your password will reduce risk. Never share passwords, challenge questions, or access tokens. 22	Viruses cause damage if left unaddressed. Always notify the help desk immediately if you suspect an infection. 23	Deleted data is recoverable unless it is removed with a wipe program. 24	Use access control lists to protect files stored on your organization's network. 25	Always turn off bluetooth when it is not needed. 26	If you see someone without a badge in a restricted location, report it immediately. 27	Websites requesting sensitive information may not always be secured. Ensure sites use encryption. 28
A poorly secured Wi-Fi network can be very dangerous. Using a good password will minimize your risk. 29	Data shared on the internet can never be deleted. Never share information online that you don't want everyone to see. 30	Downloads can sometimes occur without you knowing. Protect yourself against drive by downloads with antivirus software. 31				

JULY 1

Learn about the classification & sensitivity levels of data used in your organization, and protect it accordingly.

Your organization classifies data according to how sensitive it is to help users be aware of the protocols they must follow to protect it. Be aware of the classification levels to keep this information safe. The highest level of sensitive data includes health information, credit card numbers, driver's license data, bank accounts and ID numbers issued by the state or other institutions. Exposure of this data violates people's privacy and can lead to financial crimes as well as identity theft. Restrict access to this information on a need-to-know basis and log all attempts to look at sensitive data.

JULY 2

Safeguard personally identifiable information. Follow your organization's data retention and destruction policies for PII.

Personally Identifiable Information (PII) that your organization keeps on file about customers, clients, and employees can be used by criminals to raid bank accounts and steal people's identity. Understand and implement all the data retention and destruction policies for PII. For example, maintain a schedule for shredding confidential paper documents. Learn which systems are authorized for storing PII, and use them exclusively, avoiding insecure servers and backup drives. Use software tools to securely wipe data from drives when it is no longer needed.

JULY 3

Always keep devices & laptops with you when working remotely. Thieves will steal unattended equipment.

When you are out in the field and working remotely, remember to keep a close eye on your smartphone and laptop. Don't leave your device unattended, such as when getting up to order more coffee at a cafe or if you need to use a bathroom. It only takes a few seconds for a criminal to strike.

JULY 4

Only write down and store essential and necessary information.

Your organization has established rules for what kind of information is essential for storage, such as contracts, proposals, and financial statements. These types of documents constitute an official record that could be used in a lawsuit, so you'll need to store them for as long as specified by governmental rules and your organization's internal policies. After the mandated storage period, follow your organization's rules for document destruction.

JULY 5

Stay one step ahead of thieves: devote a single credit card for online purchases to minimize your risk.

If you have more than one credit card, it might be tempting to use them all when you are shopping online at different sites. However, it's prudent to designate one credit card for all your Internet transactions. That way, if an organization you're buying items from is attacked by hackers, you will only need to report one credit card stolen to your financial institution and you'll easily know which of your credit cards is affected. Additionally, you'll still be able to use your other credit cards to purchase vitally needed goods and services while you await replacement of the stolen card.

JULY 6

New threats occur all the time. Protect your web browsing by keeping your plugins updated.

Keep your web browser's plugins updated to protect yourself from threats. The newer versions of plugins will close security holes, ensuring safer web browsing. You can set your plugins to update automatically if you don't want to keep them manually updated.

JULY 7

Public Wi-Fi is insecure. Do not use banking websites when on public Wi-Fi.

On public Wi-Fi, any data you transmit could potentially be viewed by someone else. You should not transmit any personal, confidential or sensitive data when you're using a public connection. This includes banking activities, bill paying, and anything else of a financial or private nature.

JULY 8

Do not use email or instant messaging to send or retransmit inappropriate content. Follow the acceptable use rules of your organizations for data transmission.

It might seem like harmless fun to forward an off-color joke or other inappropriate material that a friend has sent you via email or social media. However, doing so could result in a public relations disaster and even expose your organization to a lawsuit. When in doubt, ask yourself what your supervisor would think if he or she received a copy of the message you sent.

JULY 9

Change passwords often. Rigorous password management will protect your organization's confidential data.

Your IT department will spell out the rules for password management and you need to follow their guidance to protect the safety of your organization's computer network. Change your password as often as the IT department mandates. The longer you go between new passwords, the more opportunities hackers have to crack (guess) your password.

JULY 10

Use antispyware software to help prevent hackers from monitoring your computer activity.

Spyware often masquerades as a game or a free and useful utility to help you work more efficiently. But once installed, it will gather your keystrokes, usernames, and passwords, keeping track of what you write and sending the information back to criminals without your knowledge. Ensure your antivirus software also protects against spyware and is always kept up to date.

JULY 11

Keep your data secured from cyber criminals through privacy, encryption and good habits.

Cyber criminals are usually motivated by data itself; they aren't usually attempting to obtain physical assets, merely information. For that reason, you should always take precautions to protect your organization's data. Ensure that data is only accessed by those that need to use it, encrypt all of your data regardless of format, and keep good password habits such as changing your password often and always using different passwords for different applications.

JULY 12

Protect PII by only sharing information with those that need to know.

It's extremely important to protect the Personally Identifiable Information (PII) of your clients; in some areas, it's even a requirement. Personally Identifiable Information includes, but isn't limited to, names, addresses, dates of birth, and other biographical information. You can protect PII by operating on a need to know basis; only release Personally Identifiable Information to those that have a requirement and authorization for that information. This will reduce your overall risk.

JULY 13

Get prior approval before accessing workplace information on a personal computer or mobile device.

Sometimes you need to work from home, but this can sometimes represent a security risk if not handled correctly. To reduce your risk, always request prior authorization before working from home and only work from devices that have been approved for use, such as a work laptop.

JULY 14

Be suspicious of links posted by URL shorteners. Use a preview tool before clicking on shortened URLs.

In an effort to trick unsuspecting Internet users into clicking on links to websites that harbor dangerous malware, malicious hackers will use shortened URLs and post them via social media. Do not click on a suspicious link, even if a trusted friend has sent it to you (his or her account may have been compromised with malware to send you link Spam). Instead, use a preview tool to learn where a suspicious shortened link goes before you actually click on it.

JULY 15

Stick to reputable news sites during major events. Criminals use SEO to trick you into visiting malware sites.

Legitimate websites use search engine optimization, or SEO, to include relevant keywords to help Internet searchers find the information they want. Criminals create websites with SEO poisoning, stuffing pages with inappropriate amounts of popular keywords to get a boost in search engine results. Clicking on a link for this kind of site, you'll be redirected to a malicious website.

JULY 16

Never forward emails that you think might be infected with malware.

When you receive an email or an instant message from someone, even a person you recognize and trust, never forward items that you think could be infected with malware. You risk infecting the machines of other people in your organization. Malicious hackers will send seemingly innocent messages with tempting subject lines, such as an invitation to look at a funny video. The message may come from a person whose account has already been attacked, enabling hackers to use it to automatically send messages to everyone in the address book.

JULY 17

Shorter passwords can be guessed easily by hackers. Always use long passwords.

Hackers often crack passwords using programs that try different passwords until they find the right one. Longer passwords take much longer to guess because they have many more possibilities. A six character alphanumeric password, regardless of what the password is, has approximately 19 billion possible configurations. A seven character password has over a trillion possible configurations. While both of these numbers may sound high, a program can crack a six character password in under an hour.

JULY 18

Malware sometimes hides itself as anti-virus software solutions. Never install software from unsolicited alerts.

Some malicious programs will disguise themselves as an anti-virus solution. You may be browsing the web and receive a pop-up advertisement that says that your computer is at risk and that you need to install software to clean it. You should never install software that asks you to install it through an unsolicited alert. If you do install this software, it is likely to install malicious programs on your computer. Your current antivirus and malware solution should be able to detect any real risks on your machine and will never ask you to install something to remove them.

JULY 19

People may be listening to you speak. Don't talk about sensitive information when in public.

When you're in public and speaking on your mobile phone anyone could be listening. Don't discuss sensitive information such as workplace information or personally identifiable data while you're in public. Someone could gather enough information from you to either log into one of your accounts or even steal your identity. Instead, excuse yourself from the conversation until in private.

JULY 20

If an email seems suspicious, delete it. Don't open an email from unknown senders or unsolicited attachments.

Learn to recognize suspicious emails and delete them without opening them. An email is suspicious if it comes from someone you don't know, if it has attachments on it that you didn't request or if the subject line doesn't appear to have any relevance to you. Think before you click: opening a suspicious email could expose you to viruses or malware.

JULY 21

Pirated copies are illegal. Never make pirated copies of software, movies, music, or other media.

Having and distributing pirated copies of media is illegal and leads to a violation of copyright laws. Never make pirated copies of software, movies, music, or other media, and do not download these items over the organization's network. Even if you already have a purchased copy of the media, downloading it from a peer-to-peer network may still be prohibited.

JULY 22

Keeping your password secret will reduce risk. Never share passwords, challenge questions, or access tokens.

Your password's strength cannot protect you if it is not kept a secret. You should never share passwords, challenge question answers, or access tokens with another person and there should never be a reason another person needs to access your account. If someone needs access to your device you can create a guest account with limited permissions instead. If there are files that another person needs to access that only you can access, you should inquire with a supervisor regarding granting these permissions to the other person.

JULY 23

Viruses cause more damage if left unaddressed. Notify the help desk immediately if you suspect an infection.

When a virus is not properly dealt with it can cause damage to your computer, compromise confidential information, and even infect other systems. To ensure that viruses are dealt with properly and quickly, you should let the Help Desk know the second you suspect that a virus has been introduced to your system. Signs of a virus may include your computer reacting in an unpredictable way, your computer running slowly, or your computer having programs installed that you do not remember installing on your own.

JULY 24

Deleted data is recoverable unless it is removed with a wipe program.

Your computers and mobile devices may have confidential or sensitive data on them. Simply deleting this data is often not enough to remove it entirely; the data may remain somewhere on the device even if it does not seem visible. You can use a data wipe program to ensure that your sensitive data is deleted before giving someone else your device.

JULY 25

Use access control lists to protect files stored on your organization's network.

When it comes to storing files on your organization's network, it's crucial to control access to sensitive information. Use Access Control Lists or ACLs to safeguard your data. An ACL specifies the access rights each person has to any particular item on the network, including directories, groups of files, and individual documents. With an ACL, you can designate whether a person or a group (such as programmers or managers) can read or edit a file, copy or move files from a directory, or run an application.

JULY 26

Always turn off bluetooth when it is not needed.

Hackers can use an open Bluetooth connection to compromise your laptop, tablet, or smartphone. They can then steal your personal information. Always turn off Bluetooth if you aren't using it.

JULY 27

If you see someone without a badge in a restricted location, report it immediately.

Security may be compromised physically rather than digitally by intruders. You should always report anyone suspicious you see in a restricted location. Someone without a badge or someone attempting to access a location without the appropriate credentials may be attempting to steal information or physical items from the organization.

JULY 28

Websites requesting sensitive data may not be secured. Ensure it uses encryption before submitting your data.

There may be times when you need to submit sensitive information through a website. Even a legitimate website may still be dangerous if it is not using encryption to collect your data. Before submitting any sensitive information, make sure that the website is using an SSL connection. SSL connections use "https" rather than "http" in the URL.

JULY 29

A poorly secured Wi-Fi network can be very dangerous. Using a good password will minimize your risk.

It's important to choose a good Wi-Fi password if you want to maintain the safety of your wireless connection. Do not use information such as your address or street name, as those nearby will easily be able to guess it. Also avoid naming your Wi-Fi connection something that relates to a password or your name. A proper password is long, complicated, unique, and random.

JULY 30

Information shared on the internet can not be deleted. Never share data online you don't want people to see.

Anything that is shared through the Internet cannot be truly deleted. This applies even to social platforms that claim to delete items, such as Snapchat. Once something is shared through the Internet, it can be saved and distributed by another person. Never share anything online that you don't want everyone to see.

JULY 31

Protect yourself against drive by downloads with antivirus software and good habits.

Drive by downloads are downloads that occur either without permission or without your knowledge. They usually occur when you are visiting a site that is infected with malware. To avoid drive by downloads while at work, only visit sites necessary to fulfill your duties.

AUG

2018



SUN	MON	TUE	WED	THU	FRI	SAT
			It's important to protect your passwords. If you suspect your password is compromised, change it. 1	Links may not go where they seem to go. Hover over them to see their true location. 2	Mobile devices with old operating systems may be vulnerable. Always ensure that your mobile OS is updated. 3	Keep digital copies of important documents as you travel in case they are stolen. 4
Never bring sensitive information into shared meeting areas. 5	Jailbreaking a phone compromises its security features. Never jailbreak or root a phone. 6	Sticking out makes you a target. When traveling, try your best to blend in with the locals. 7	Robbers often case their targets first. Avoid putting high value items such as computers in view of windows. 8	It's easier to reverse charges on credit cards. Always use a credit card rather than a debit card for transactions. 9	Social media data can be used by identity thieves and for other malicious purposes. Set your data to private. 10	There are "bad neighborhoods" on the web. Protect yourself by only visiting sites you need for work. 11
Social engineers may use your personal data against you. Never trust anyone without proper credentials. 12	Never write down your password. Create a password you can memorize. 13	Any link can be dangerous. Avoid links unless they are from a trusted source. 14	Sensitive data can be overheard. Do not give sensitive or confidential information over the phone in public. 15	USB cords are used for more than charging. Only charge devices on trusted computers. 16	Clutter makes it more difficult to secure physical documents. Adhere to the clear desk policy. 17	Phishing tactics may direct you to fake contact information. Make sure the number you're calling is legitimate. 18
Kids need protection online. Monitor the sites they are viewing. 19	Public cloud storage can be hacked. Secure your data with encryption. 20	Social media is public data. Never post confidential, sensitive, or trade secret information. 21	Older browsers may have security issues. Only use the latest version of a browser. 22	Learn to identify suspicious emails. Vague introductions and typos are common in phishing and malware. 23	Physical documents may also be at risk. Protect paper documents. 24	Anyone can view your screen in public. Do not view sensitive information where others can see it. 25
Protect your data with regular backups. External drives and off site backups will ensure that your data is protected. 26	Social engineers prey on the good-mannered. Don't be afraid to say no. 27	Pay attention to your mail. When identity theft occurs, your mail may stop coming. 28	Never open suspicious emails; opening them may cause system damage. 29	Protect your kids online: place computers in a public area so you can keep an eye on what they're doing. 30	Be responsible for your data: Data security is everyone's concern. 31	

AUGUST 1

It's important to protect your passwords. If you suspect your password has been compromised, change it.

Your password may be compromised if you view multiple sign-in failures on your account, if another account that you use the same or a similar password to has been accessed by someone else, or if you notice strange activity on your account. If your password has been compromised, all of the data it leads to has also been compromised. It's very important to change your password if you believe that someone else has accessed your account. Make sure that your new password is completely unique.

AUGUST 2

Links may not go where they seem to go. Hover over them to see their true location.

A link can appear to go anywhere, but it may not always go where it says it does. Move your mouse over a link without clicking on the link to see the actual address of the site. If the address differs at all from your expectation, you should not click on the link. If you do not see a tool tip or a status that displays the link address, you can right click and copy the link and then paste it into a text file to see where the link leads.

AUGUST 3

Mobile devices with old operating systems may be vulnerable. Always ensure that your mobile OS is updated.

Old operating systems on mobile devices could be vulnerable to old security issues. Mobile devices often contain sensitive or confidential information that needs to be secured. If your mobile device asks you to update your operating system, you should do so as soon as possible. You can also go into your mobile device's settings and set it to update itself automatically.

AUGUST 4

Keep digital copies of important documents as you travel. If your documents are stolen, you will have a copy.

When you're traveling, you should scan all of your important documents and keep them in an email folder. You'll be able to access your important documents even if you lose your documents or they are stolen. An email address can be accessed from anywhere, unlike local files that you might store on a mobile device. You can also keep documents encrypted on a cloud file server.

AUGUST 5

Never bring sensitive information into shared meeting areas.

Shared meeting areas can be very vulnerable to insider threats. Do not bring sensitive information into shared meeting areas such as conference rooms. Only bring the data you need for each meeting to reduce the possibility of risk exposure.

AUGUST 6

Jailbreaking a phone compromises its security features. Never jailbreak or root a phone.

Jailbreaking a phone is the act of removing or compromising a phone's preinstalled operating system so that you gain complete control over the phone's settings and the applications on it. Jailbreaking can be dangerous because it will turn off many of the security features that are on the phone. When you jailbreak your phone you will no longer be able to get security updates from the phone's manufacturer. Phones contain a tremendous amount of personal and sensitive information and must be protected at all times. To keep your data safe, you should never jailbreak or root a phone.

AUGUST 7

Sticking out makes you a target. When traveling, try your best to blend in with the locals.

Thieves, pickpockets and con artists will often try to pick tourists out of a crowd. Avoid any telltale signs that you're a tourist when you travel abroad, such as bright new sneakers, fanny packs or large cameras slung across your neck. Instead, try your best to dress casually or in the same fashion as the locals. If you are approached by a stranger while traveling, keep your guard up.

AUGUST 8

Robbers often case their targets first. Avoid putting high value items such as computers in view of windows.

Putting expensive items such as desktop computers or laptops close to your windows may increase the likelihood of break-ins. Having high value items next to windows makes it easier for a thief to grab them quickly and can make you a target. When possible, keep any windows that face the street covered with blinds or drapes and keep high value items away from these windows. Make sure your windows are always closed and locked when not in use.

AUGUST 9

It's easier to reverse charges on credit cards. Always use a credit card rather than a debit card for transactions.

Credit card companies can easily reverse fraudulent charges. It is much harder to get a transaction on a debit card reversed because the bank will need to replace the cash taken from your account. While the transaction is processing, you will be without these funds. If you want to protect yourself from the possibility of fraudulent charges and avoid this inconvenience, you should always use a credit card for transactions. Debit cards should only be used to access cash from an ATM.

AUGUST 10

Social media information can be used by identity thieves and for other malicious purposes. Only allow friends to view your posts.

Social media accounts can reveal quite a lot about you and this information could potentially be used by identity thieves and others with malicious intent. You can counter this by altering your social media privacy settings and by only adding people you know to your friends list. Set your account profile and posts to only be visible to your friends, not the public and not "friends of friends." The "friends of friends" setting could leave you vulnerable in the event that one of your friends accidentally adds someone they don't know to their friends list.

AUGUST 11

There are “bad neighborhoods” on the web. Protect yourself & your workplace visiting sites you trust.

Online “bad neighborhoods” are websites which have questionable content, including malicious programs and viruses. You can easily stumble into a bad neighborhood by visiting unknown sites. When at work, you should only go to the sites you need to in order to complete your duties. This will reduce the risk you may subject your work computer to viruses or other malicious material.

AUGUST 12

Social engineers may use your personal data against you. Never trust anyone without appropriate credentials.

Social engineers are individuals who will call you and pretend to be either within your organization or with a service that is attempting to work with your organization. They will often pretend to need confidential information from you and will claim to have the clearance to access this information. A social engineer might call and say that they are troubleshooting your web service and need an administrative password; they may use your social media to determine your position within the organization. Never give out any information to anyone without verification of their credentials from management.

AUGUST 13

Never write down your password. Create a password you can memorize.

When writing down your password, you leave yourself open to anyone who has physical access to the location that you have stored your password in. Rather than writing down a password, make sure that you have created a password you will remember. Use password reminders and challenge questions to help you in the event that your password is forgotten and needs to be reset.

AUGUST 14

Any link can be dangerous. Avoid links unless they are from a trusted source.

Clicking on a link can bring you to a virus or other malware. You should never click on a link unless you are certain they have come from someone you trust. This includes links on websites, in emails, or sent through instant messages.

AUGUST 15

Sensitive data can be overheard. Do not give sensitive or confidential information over the phone in public.

If you need to give any confidential or sensitive information to someone over the phone, first ensure that you cannot be overheard by anyone else. Never discuss confidential organization data or personal, sensitive information while in a public space.

AUGUST 16

USB cords are used for more than charging. Only charge devices on trusted computers.

A USB cord can be used to transfer data as well as charge a device. Whenever you connect a device to a computer, both the device and the computer may be compromised. If you have a device that charges through USB, only connect it to trusted computers. Connecting such a device to a public computer could represent a security risk. You can also purchase an adapter that will allow you to charge the device directly in an electrical outlet.

AUGUST 17

Clutter makes it more difficult to secure physical documents. Adhere to the clear desk policy.

The more you have on your desk, the more likely it is that you have sensitive or confidential data that is not properly stored. Make sure that your desk is cleared at the end of every day to ensure the security of sensitive documents. Never keep sensitive or confidential documents out when they are not necessary: keep them stored whenever you are not actively using them.

AUGUST 18

Phishing tactics may direct you to fake contact information. Make sure the number you’re calling is legitimate.

Before trying to contact your bank, credit card company, or other financial institutes, make sure that you are calling the right number. Phishing tactics may offer contact information that appears to be legitimate but truly leads to them. Look at your most recent bank statement or the back of your credit card to find the correct contact information. Otherwise, you may be contacting someone who is interested in stealing your personal data.

AUGUST 19

Kids need protection online. Monitor the sites they are viewing.

There are many things on the Internet that may not be safe for a child to view. Use child safety software to track the websites that your child goes to and check them on a regular basis. You may also view their web history, but know that web history can often be altered by a technology savvy child. Discuss any problematic sites with your child and explain to them why they should not be viewed. You can also move the computer into a public space to ensure that you are always aware of what your child is viewing.

AUGUST 20

Public cloud storage can be hacked. Secure your data with encryption.

Public clouds can be vulnerable to hacking because they are easy to access and often used by many individuals. Do not store any of the organization’s data on public cloud storage without permission. Any data you store on a public cloud should be encrypted.

AUGUST 21

Social media is public information. Never post confidential, sensitive, or trade secret information.

Information on your social media accounts can be released to the public even if you have a private account that is only accessible to your family and friends. Never post or share confidential, sensitive, or trade secret information on your social media accounts or anywhere else on the web.

AUGUST 22

Older browsers may have security issues. Only use the latest version of a browser.

Any old web browser may have unpatched security issues that have since been discovered. Only use the latest version of a browser to access the web. Set browsers to auto update to the most recent version so your computer is protected from new exploits.

AUGUST 23

Learn to identify suspicious emails. Vague introductions and typos are common in phishing & malware.

Emails with an unprofessional appearance are often not legitimate and should be discarded. This includes: emails that have a generic header, such as "Dear Client," emails that contain a large amount of typos, and emails that are generally not formatted in a professional manner. Any links or attachments in these emails should be ignored and avoided.

AUGUST 24

Physical documents may also be at risk. Protect paper documents.

Paper documents can be even more easily accessed, copied, or used for malicious purposes than digital files. Make sure that documents are always stored safely and that they are shredded when they are to be discarded. Do not keep sensitive or confidential paper documents in an open area where they can be accessed; put away any of these documents at the end of the day. A copy of a confidential or sensitive paper document must be treated the same as the original document.

AUGUST 25

Anyone can view your screen in public. Do not view sensitive information where others can see it.

Shoulder surfing is a practice by which others attempt to view your screen over your shoulder. You may not see someone doing this. You should be very careful not to display any sensitive or confidential information where other people can easily see it. If you need to work on any sensitive data in a public location, make sure that your screen is facing a wall and that there are no reflections in which it could be viewed.

AUGUST 26

Protect your data with regular backups. External drives and off site backups will ensure data is protected.

Many things can lead to a loss of the data on your home computer. Fires, floods, earthquakes, and even something as simple as a damaged hard drive could erase all of the information you have. Protect yourself in your home with an external drive and protect yourself off-site with web backups or cloud backup solutions. Remember that your backups should be password protected and encrypted just like your computer is.

AUGUST 27

Social engineers prey on the good-mannered. Don't be afraid to say no.

Social engineers try to convince people to do things by preying on their urge to be good-mannered and polite. If someone asks you to give them personal information or to give them access to confidential information, don't be afraid to be direct and say no. A social engineer encounter can be through telephone, email, or even in person. Anyone suspicious should be denied access until you can verify their identity.

AUGUST 28

Pay attention to your mail. When identity theft occurs, your mail may stop coming.

You need to be vigilant about the possibility of identity theft. If you have noticed that much of your mail has stopped coming, an identity thief might be after you. A common tactic is to file a change of address so that they get all your mail; they can then piece together information about you from the mail that they receive.

AUGUST 29

Never open suspicious emails; opening them may cause system damage.

Suspicious emails often contain programs that will harm your computer system if you open them. Rather than inspecting a suspicious email, delete it right away. There are many ways you can identify a suspicious email: it may come from a stranger, be riddled with grammar issues, or urge you to open a file or link. You should also ensure that your virus protection is automatically scanning the emails you receive for additional system security.

AUGUST 30

Protect your kids online: place your children's computer in a public area so you can keep an eye on them.

Despite how responsible your children are, don't give in to their requests to keep computers in their bedrooms. Always place your kids' computers in a public area, such as the living room or family room. Position the monitor so it faces outward, enabling you to shoulder surf and see what's going on. Check browsers search history to keep tabs on the content your kids are accessing.

AUGUST 31

Take responsibility for your data: Data security is everyone's concern.

Like a chain, data security is only as secure as its weakest link. For this reason, everyone is responsible for protecting important and sensitive data. Anyone who can access data has the potential to cause data security issues. Regardless of your position within an organization, you must remain vigilant regarding data security. Security protocols should be applied to every employee in the organization who interacts with the organization's data.

SEP

2018



SUN	MON	TUE	WED	THU	FRI	SAT
						Don't display sensitive data on your screen in public places. 1
Items can be lost easily when traveling. Only take what you need with you and lock up your valuables. 2	Your access badge could be used by a malicious insider. Always know where your badge is. 3	Fake websites may masquerade as official ones. Navigate to your bank accounts by manually typing in the address. 4	Kids may be in danger online. Teach them what they can and can't share over the internet. 5	Reducing access to your files keeps them safer. Use access control lists to ensure safety. 6	Don't allow others to follow you through secure entryways without swiping their own access card. 7	Strangers on your computer may attempt to access confidential files. Never let a stranger use your computer. 8
Phishing is a technique by which a scammer asks you for confidential data. Never give sensitive data to unknown persons. 9	Online bullying can become very serious. Talk to your kids about what to do when bullied. 10	Hackers may know your router's default settings. Change the username and password for new routers immediately. 11	Talk with your children about internet safety before they go online. 12	Social media is viewable by anyone. Do not post anything regarding the organization without consent. 13	Plugins can be security risks. Only use the plugins you need. 14	Legitimate emails usually don't demand immediate action. Be skeptical if they do. 15
Acceptable use still applies at home. Follow all policies even when working remotely. 16	Investment fraud can be costly. Never invest money in something you don't understand. 17	It's important to password protect all sensitive information. Create easy to remember but complex passwords. 18	Viruses & malware may link computers together to perform tasks. This is damaging to your system and others. 19	Classify new documents & emails you create following the guidelines defined in the data classification policy. 20	Know where the nearby fire extinguishers are and know how to use them. 21	Do not install software on your work computer unless it has been approved and is authorized for your computer. 22
Save your work regularly to ensure that you do not lose information. 23	Never leave your ID badge or key card unguarded. 24	Printed sensitive data should be shredded when it is being disposed of. 25	The internet is provided to increase work efficiency. Don't let the internet interfere with your work. 26	Passwords alone cannot always provide protection. Use two-factor authentication for sensitive accounts. 27	USB drives can carry viruses. Never plug in a free or found USB drive into your computer. 28	Always follow governmental regulations and policies on retaining and destroying sensitive data. 29
Protect your data with secure storage and transmission. Otherwise, your data may be vulnerable. 30						

SEPTEMBER 1

Don't display sensitive data on your screen in public places.

Mobile device security goes beyond simply ensuring that your data is encrypted and your connections are secured. If you display sensitive data on your computer screen in a public place, it may be read by others. Confidential data should never be viewed in a public place in a way that it can potentially be seen by someone else. Instead, you should always view your sensitive data in private. If you must complete work in a public location, face your back to the wall.

SEPTEMBER 2

Items can be lost easily when traveling. Only take what you need with you and lock up your valuables.

It can be very easy to lose important items when you travel. Take only the credit cards, identification and cash that you need with you, and minimize the total amount of items that you carry at once to reduce the possibility that you might lose track of them. Any important or expensive items that are not carried on you should be locked up in a hotel safe. This includes a backup payment method, such as an additional credit card, that can be used if you lose your other items. Copy your identification information and leave the copies in the safe for additional security.

SEPTEMBER 3

Your access badge could be used by a malicious insider. Always know where your badge is.

Someone inside the organization – including both coworkers and visitors – could use your access badge to reach confidential organization data. Always ensure your badge is on your person at all times. Wearing your badge at all times is the best way to avoid losing it. If your badge does go missing, report it lost immediately. This is true even if you find your badge again later; the badge could be taken, used and then returned.

SEPTEMBER 4

Fake websites may masquerade as official ones. Navigate to your bank accounts by manually typing the URL.

A fake website will often look almost identical to an official website. You could click on a link that looks legitimate in an email and be directed to a site that is not the same URL. The only way to absolutely ensure that you log into the proper website is to manually type the URL into your browser. Do not click links to your financial institution's website, as they are not always legitimate.

SEPTEMBER 5

Kids may be in danger online. Teach them what they can and can't share over the internet.

Children don't always know what is and isn't appropriate to tell people over the Internet. Make sure that your children know what personal information is in terms that they can understand and who they should and shouldn't be speaking with. Explain to your children why certain information should not be shared. Having an open and honest discussion with your child is the best way to prepare them to be responsible and safe and to help them understand the importance of privacy.

SEPTEMBER 6

Reducing access to your files keeps them safer. Use access control lists to ensure files are accessed properly.

Access control lists allow you to control who can view your files and whether they can read, modify or delete them. Using access control lists will ensure that only those who need your files can view them and that they can't do anything to the files that you don't desire. By reducing the overall exposure of your files, you can decrease risk.

SEPTEMBER 7

Don't allow others to follow you through secure entryways without swiping their own access card.

Everyone must swipe their own ID access cards. If they still refuse to swipe their ID access card, notify security and provide them with the details of the event. Most of these entry control systems record an audit trail of who enters, which door, and when.

SEPTEMBER 8

Strangers on your computer may attempt to access confidential files. Never let a stranger use your computer.

Strangers may attempt to gain access to your computer so that they can access sensitive or confidential documents. They may give you a reason that they need to use your computer, such as a personal favor. Anyone on your computer will have access to the files and systems that you have access to. You should never let a stranger access either your work or home computer.

SEPTEMBER 9

Phishing is a technique by which a scam artist asks you for confidential information. Never give personal or sensitive information to someone you don't know.

Phishing techniques may vary, but they usually involve attempts to trick you into revealing personal or sensitive information. As an example, a scam artist may pretend to be an employee of your bank and ask you for your confidential bank login information. You should never give anyone sensitive or confidential data through email or instant messaging even if it appears to come from someone you know or a company you do business with. Call your bank directly if you receive a request.

SEPTEMBER 10

Online bullying can become very serious. Talk to your kids about what to do when bullied.

Many children experience bullying online. Online bullying can be very harmful because it cannot be escaped, even when at home. In order to protect your children from the consequences of bullying, you should talk to them about the actions they can take to take control of the situation. Children should know that there are serious repercussions for bullying and that they should always tell an adult if bullying does occur. Let them know that they can always talk to you about it.

SEPTEMBER 11

Hackers may know your router's default settings. Immediately change usernames & passwords for new routers.

Wi-Fi routers usually come with default settings for the username and password. Hackers may be able to figure out your password using this default information. Once in your router, a hacker may be able to view your network traffic or even lock you out of your own network. When you get a new Wi-Fi router you should follow the manufacturer's directions to change both the username and password. Make sure that the password is long, difficult to guess and not related to the network name.

SEPTEMBER 12

Talk with your children about internet safety before they go online.

Your kids may have a limited understanding of potential dangers that they face when accessing the Internet. Before they go online, explain that they should never reveal personal information about themselves, such as where they live or their date of birth. Instruct them to tell you about anyone making inappropriate contact with them, such as through online chatting or email. And supervise your younger children whenever they surf the Web, to keep them from being exposed to harmful materials.

SEPTEMBER 13

Social media is viewable by anyone. Do not post anything regarding the organization without prior consent.

Social media can be seen by anyone even if your account is private; anything you post could be shared on the Internet and it cannot be deleted once others have begun sharing it. You should get written permission before you post anything online.

SEPTEMBER 14

Plugins can be security risks. Only use the plugins you need.

While plugins can make browsing easier, plugins can also represent security risks. Keep the amount of plugins you use at a minimum. Uninstall or disable any plugins that you are not using and keep the plugins that you do use updated often to protect yourself against security issues. Only install plugins from reputable companies.

SEPTEMBER 15

Legitimate emails usually don't demand immediate action. Be skeptical if they do.

If an email is sent to you that requests that you take an immediate action, you should be skeptical. Rather than responding to the email, you should call or otherwise directly contact the sending party for more information. Immediate action is usually used to make you rush, so that you don't notice other warning signs.

SEPTEMBER 16

Acceptable use still applies at home. Follow all policies even when working remotely.

Acceptable use policies are designed to be used regardless of where you work. Whether you are working from home or on a business trip, you should still be following acceptable use policies to protect both yourself and the organization.

SEPTEMBER 17

Investment fraud can be costly. Never invest money in something you don't understand.

The majority of investment fraud schemes, such as Ponzi schemes, Pyramid schemes, and Pump and Dump Schemes, take advantage of an investor's ignorance regarding the methods that they purport to use. Never invest in anything that you do not understand. It is likely that it does not work in the way that the investor says it does.

SEPTEMBER 18

It's important to password protect all sensitive information. Create easy to remember but complex passwords.

Longer, complex passwords are more difficult for a person to guess and thus will secure data much better than shorter, simpler passwords. Try to create password phrases and substitute letters for numbers and symbols to increase the complexity. A password phrase may be something as simple as "remember to buy milk." With substitutions and symbols, this becomes "R3m3mb3r2buym1lk." This is a very difficult to guess but easy to remember password.

SEPTEMBER 19

Viruses & malware may link computers together to perform tasks which is damaging to your system & others.

Some viruses and malware may not do anything perceivable to your computer but instead use your computer. A botnet is an amalgam of many computers that are linked together to complete a purpose, such as a malicious attack against a third-part target. While these viruses and malware may not harm your system, they may be used to damage another system or to commit some form of crime. Signs that your computer may be in a botnet include the computer running sluggishly or transmitting data when it should not be. Your virus protection software should be kept current and always on to protect you from this.

SEPTEMBER 20

Classify all new documents and emails you create following the guidelines defined in data classification policy.

Apply the proper classification labels to the documents and emails that you create, such as private or confidential, and then protect the new information asset following the data classification policy. The labels will remind you and others who need to access the information that they must keep the data secured at the appropriate level.

SEPTEMBER 21

Know where the nearby fire extinguishers are and know how to use them.

If a fire is detected, first sound the alarm to notify management and personnel of the risk to safety, and to begin evacuation procedures. If it is safe to do so, use the fire extinguisher following the prescribed procedures to attempt to extinguish the fire.

SEPTEMBER 22

Do not install software on your work computer unless it has been approved and authorized for your computer.

Unauthorized software can contain viruses and other forms of malware, and can cause conflicts with other applications. The software must be properly accounted for and follow proper licensing requirements. If you need software that is not approved or authorized for your computer, contact your supervisor or the IT department.

SEPTEMBER 23

Save your work regularly to ensure that you do not lose information.

Hardware and software can malfunction and power can be unstable. These phenomena can cause a computer to lock up or shut down unexpectedly, which makes regularly saving your documents essential. On a PC, type "Ctrl" and "S" at the same time to quickly save your work. On a Mac type "cmd" and "S" at the same time. Get in the habit of doing this regularly.

SEPTEMBER 24

Never leave your ID badge or key card unguarded.

These items should be worn or with you at all times and never lent out. If you lose your ID badge or key card, report it as soon as you realize one of these items is missing.

SEPTEMBER 25

Printed sensitive data should be shredded when it is being disposed of.

Attackers have been known to search the trash of potential victims to gain access to sensitive and valuable information. The data classification policy describes what classifications of documents must be physically destroyed (shredded) prior to disposal.

SEPTEMBER 26

The internet is provided to increase work efficiency. Don't let the internet interfere with your work.

Access to the Internet is intended to help you work more effectively. Though you are free to occasionally use the Internet for personal tasks, it's important that you never allow Internet usage to affect your work. Never use the Internet at work for obscene, sexually explicit, threatening, or illegal activity, and avoid the consumption of excessive resources such as bandwidth. This includes websites, emails, instant messaging, and other online tasks. If in doubt, consult the Help Desk regarding acceptable use policies.

SEPTEMBER 27

Passwords alone cannot provide sufficient protection. Use two-factor authentication for sensitive accounts.

Two-factor authentication is a special type of security that involves two separate types and stages of authentication. Usually, two-factor authentication uses something you "have" along with something you "know". ATMs use two-factor authentication by requesting your ATM card and your PIN, while many online accounts require that you both have a password and verify your identity with your phone or another device. Other forms of two-factor security authentication might include a token or a removable media device, such as a USB drive.

SEPTEMBER 28

Usb drives can carry viruses. Never plug in a free or found USB drive into your computer.

Once plugged into a computer, a USB drive can transfer a virus or other malware to your system. You should never plug in a USB drive that you have received for free or found somewhere in your office; even if the USB drive was found at work, it might still have a virus on it. Keep your USB drives clearly marked to prevent any confusion between you and your coworkers and always keep them in a specific place.

SEPTEMBER 29

Always follow governmental regulations and policies on retaining and destroying sensitive data.

Certain types of data must be stored securely for a set amount of time and then disposed of in a secure fashion. The amount of time for data retention varies from location to location and also depends on the nature of the information (such as medical or financial records). Always be aware of the data retention and destruction policies in your local jurisdiction as well as the information security policy. Determine whether data is public, private, or confidential when preparing it for storage and removal. Ask your supervisor for guidance whenever you are in doubt.

SEPTEMBER 30

Protect your data with secure storage and transmission. Otherwise, your data may be vulnerable.

Most users have sensitive data on their computer that could be used for malicious purposes: bank account information, personal information, and more. To protect this data, you should always use the appropriate encryption protocols for both storage and transmission. Encryption protocols seal stored data behind a virtual lock, protecting the data from hackers. Storage devices, such as a hard disk drive or a flash drive, should be encrypted and you should use secure Wi-Fi and SSL (secure socket layer) protection when transmitting sensitive information. Look for HTTPS in the web address to verify the data is being transmitted securely.

OCT

2018



SUN	MON	TUE	WED	THU	FRI	SAT
	Only use authorized devices to access workplace data. 1	Protect your kids online through monitoring and parental controls. 2	Protect your backups as you would protect your primary data. 3	Follow your organization's records retention & destruction policy. Emails constitute an official "written" record. 4	Secure your data when stored and transmitted through encryption. 5	Cancel credit cards and contact your bank immediately if you think you have become the victim of identity theft. 6
Look for a security icon (usually a padlock) when using wireless networks to see if Wi-Fi is secure. 7	Save your files to a location that is automatically backed up. 8	Social engineers will try to convince you to let them into a secure building without a key card or key code. Don't fall for it! 9	Use your computer with the assumption that everyone can see what you're doing. You might be audited for acceptable use. 10	Protect your home computer by using strong passwords and never reusing passwords. 11	Use caution when disclosing personal data such as pin numbers. 12	Manage your passwords with safety in mind: do not use words found in any dictionary, in any language. 13
Never give out information without verifying the identity of the requester. 14	Sending email over a Wi-Fi connection? Be sure your email system uses encryption or the Wi-Fi connection is secure. 15	Beware of accepting free or found USB flash drives. They may contain viruses and malware that will compromise your computer. 16	Protect your identity by shredding personal documents at home. 17	Simply clicking on a link can infect your computer with malware. Never click on suspicious links in social media posts. 18	Con artists may construct fake social media accounts. If you feel suspicious about a profile or a person, trust your instincts. 19	Spam emails use the "unsubscribe" option to see if your email address is active. Don't unsubscribe from mailing lists you did not subscribe to. 20
Any email could potentially contain or link to a virus. Avoid clicking on links in emails and don't open any unknown email attachments. 21	Always be near the fax machine when receiving sensitive information. Anyone can read your faxed documents. 22	Phishing techniques may be used to trick you into clicking harmful links. Never click on suspicious links. 23	Cyber bullying isn't just a matter for school officials. It's also a crime. Report any instances of cyber bullying to your local authorities. 24	Fraud occurs through bank accounts and credit cards without notice. Check your bank statements often to protect yourself. 25	Sending confidential data via email or IM may expose to risk. Never send valuable data through these methods at work. 26	Using the same password for multiple accounts exposes you during a single security breach. 27
Viruses and malware can infect devices or computer via email attachments, links from any source, USB drives, and other ways. 28	Always be on guard against thieves looking to steal your laptop or mobile devices. 29	Expensive equipment and jewelry can easily be lost when traveling. Avoid taking or displaying these items on trips. 30	Your instant messages are not private when at work. Don't say anything you wouldn't want your employer to read. 31			

OCTOBER 1

Only use authorized devices to access workplace information.

Always follow your organization's device security policy. When using a laptop, desktop, smartphone, or other device while working remotely, your device must meet minimum security requirements to keep unauthorized people from accessing critical workplace information. For example, you will need to use a robust login and password system on your smartphone, and only connect to the Internet through a virtual private network. Configure your device so that you can wipe it from remote in case it is lost or stolen. When in doubt, contact your supervisor to verify that your device is authorized for use and has the latest security updates.

OCTOBER 2

Protect your kids online through monitoring and parental controls.

Protecting your children online can be a challenge. Have your kids use their own computer with parental controls turned on, and place their computer in a visible and well-trafficked area such as the dining room or living room. Regularly check on what they are doing online, and limit their Internet use to a specific time every day. This will ensure they are constantly monitored and safe.

OCTOBER 3

Protect your backups as you would protect your primary data.

Common methods of protecting backup data include password protection, encryption, and labeling. Provide a password when backing up your data if your software offers this option. You'll also need to provide that password when you restore the backup.

OCTOBER 4

Follow your organization's records retention & destruction policy. Email constitutes an official "written" record.

Every email that you receive, send, and forward becomes part of the official "written" record that can be used in a court of law. Always follow your organization's policy about retaining and destroying records. This means that you might need to hold onto email that you would ordinarily want to delete, such as to free up storage space. You might need to keep the messages for a specific amount of time, depending on local governmental and industrial regulations. Authorities often need to access copies of emails during the course of an investigation.

OCTOBER 5

Secure your data when stored and transmitted through encryption.

Unless you encrypt your data, it will not be protected when saved to a hard drive or transferred over the Internet. Unencrypted data can easily be accessed. Take action to encrypt your sensitive information and never transmit unencrypted data over the Internet. If uploading or otherwise transmitting data, ensure that the recipient is properly secured as well. You can secure your data through the use of a program that encrypts hard drives and other media, or by packing your data in a ZIP or RAR file that is password protected. Many flash drives and external drives also offer password protection features natively.

OCTOBER 6

Cancel your credit cards and contact your bank if you think you have become the victim of identity theft.

Once a criminal has stolen your personal information and committed identity theft, it's important to act quickly to minimize any potential harm. Begin by contacting your financial institutions to cancel your credit cards and order replacements. Check your online banking account and change your login information immediately. You will also want to change passwords for your email and any sites that you log into. For added security, sign up with a credit monitoring service to alert you to any fraudulent attempts.

OCTOBER 7

Look for a security icon (usually a padlock) when using wireless networks to see if Wi-Fi is secure or not.

For Windows 7 and 8, Apple computers, Android devices, and iOS devices, look for a padlock icon (secure) or an alert icon (not encrypted) next to the name of a Wi-Fi network. If there is no padlock icon, do not trust the network and avoid logging in to any accounts, such as your email or bank account, if you access the Internet via the unsecured wireless network.

OCTOBER 8

Save your files to a location that is automatically backed up.

Computer storage can fail and files can be overwritten. To avoid losing any of your important data, ensure that you are saving your files and documents to a location that you know is being backed up automatically, such as a network directory. Automated backups should also be checked on a regular basis to ensure that they are completed as scheduled.

OCTOBER 9

Social engineers will attempt to convince you to let them into secure buildings even though they don't have a key card or key code. Don't fall for it!

Malicious individuals who want to steal our physical or information assets often try to get into our facilities by posing as a fellow employee or a vendor who lost his or her card key. They've even been known to dress as repair technicians, complete with fake uniforms with the logo of an actual vendor. If someone without a keycard asks you to let them into a secured building, offer to contact security or your supervisor who can verify their identity and grant them access to the building if it's appropriate to do so.

OCTOBER 10

Use your computer with the assumption you might be audited for acceptable use of equipment.

Most of us are familiar with the idea that cookies help identify us to advertisers and website owners when we visit websites. However, your computer type, model, operating system, and even what version of web browser you are using are also known to every site that you visit. This combined data results in another method to identify you and the types of information you access.

OCTOBER 11

Protect your home computer by using strong passwords and never reusing passwords.

Your home computer often holds extremely important data. You can protect your home computer through the use of a strong password, such as a long password that contains a variety of special characters. Changing your password often also increases your security. Never use your work password for your home computer, as this can represent a security risk for both you and work.

OCTOBER 12

Use caution when disclosing personal information such as PIN numbers.

Never share your PIN code, even with someone at your bank, and change it if you believe it has been compromised.

OCTOBER 13

Manage your passwords with safety in mind: do not use words found in any dictionary, in any language.

To keep your online accounts safe, you need to carefully manage your passwords. Don't use words from any dictionary, because criminals can use automated programs to run an entire dictionary against your account password in practically no time and gain access to your organization's information. Use numbers or other characters, include upper case and lower case letters, and otherwise change your password until it no longer can be found in any dictionary.

OCTOBER 14

Never give out information without verifying the identity of the person requesting it.

A social engineer is a person who attempts to get confidential information purely through social skills, such as by calling and asking for passwords or other sensitive information. They will often claim to be a member of your organization or an organization that works directly with you, and may even know detailed information about your organization and your coworkers. Never give out information, such as passwords, to anyone without verifying their identity first. When in doubt, consult your supervisor.

OCTOBER 15

Sending email over a Wi-Fi connection? Be sure your email system uses encryption or secure Wi-Fi network.

Email systems often send messages in plain text with no encryption. If your email is not encrypted and you are using an unsecured Wi-Fi connection, you are literally broadcasting your email messages to anyone within range of your computer, so anyone with the right software who is near you can easily listen in. To prevent this, make sure that either your email system uses encryption or that you are connecting via a secure Wi-Fi connection (WPA2).

OCTOBER 16

Beware of free or found USB flash drives. They may contain viruses or malware to compromise your computer.

We're accustomed to getting free promotional items, such as t-shirts or coffee mugs with company logos on them through the mail and at trade shows. Think twice before accepting a USB flash drive as a gift or using a flash drive that you've found in some random location. Criminals often put viruses and malware on USB drives and leave them around, hoping victims will pick them up and use them in their computers. Protect your organization's computers and network by avoiding found or "gift" USB drives.

OCTOBER 17

Protect your identity by shredding personal documents at home.

Many identity thefts occur every year through the use of physical documents that were thrown away in the trash. Rather than throw out your personal information, invest in a small shredder and shred all of your documents before you get rid of them.

OCTOBER 18

Simply clicking on a social media link can infect your computer with malware. Never click on suspicious links.

Hackers often post messages on social media sites with links to malware. For example, they might hijack a friend's account and then post a message saying they are "Stuck in London" and need you to send money. To avoid these traps, never click on suspicious links in social media posts.

OCTOBER 19

Con artists may construct fake social media accounts. If you feel suspicious, trust your instincts.

There are many con artists who create social media accounts to get close to others and get information from them. They may even claim to have gone to the same school you did or know other people that you know. If you feel suspicious at all about a person online, you should trust your instincts and block them. Do not add anyone to your social media accounts that you don't know.

OCTOBER 20

Spam emails may use the "unsubscribe" option to determine whether your email address is active.

Spam emails may prompt you to unsubscribe from them. When you click the unsubscribe link, you could potentially be redirected to malware. The Spam sender could also use your response to determine your email account is active; they could then either continue sending you emails or even sell your email to another spammer. Don't unsubscribe from unsolicited emails.

OCTOBER 21

Any email could potentially contain or link to a virus. Avoid clicking on links or opening attachments in emails.

Emails can expose you to viruses or malware in two ways: through a link or through an attachment. Do not click on links in emails that appear suspicious or come from people you don't know. Do not open unidentified email attachments. Any type of email attachment could potentially contain malware. Even email attachments that you recognize or requested should be scanned by your virus scanning software before you open them.

OCTOBER 22

Always be near the fax machine when receiving sensitive data.

When you receive a fax of a sensitive or confidential document, those around the fax machine could read it or even make a copy of it. You should always wait by a fax machine when you're receiving sensitive documents to avoid compromising the data. Once you have received the data, you must treat it as a sensitive document: avoid placing it where it could be viewed by others and destroy it properly when you no longer need it.

OCTOBER 23

Phishing techniques may be used to trick you into clicking harmful links. Never click on suspicious links.

Phishing emails may be sent to you asking you to click on a link. Once you click on the link you may be directed to an infected website which will install spyware on your computer. Always be skeptical about links sent to you via email. Do not click on links that come from unknown senders or that do not go to where they claim they are going to.

OCTOBER 24

Cyber bullying isn't just a matter for school officials. It's also a crime. Report any cyber bullying to authorities.

Cyber bullying is a crime. If your child is the target of cyber bullying, you should document everything and contact both your child's school and the local authorities. This will increase the likelihood that the matter will be dealt with in an appropriate and productive way. It will also send a message to your child that they are protected and that what is happening to them is wrong.

OCTOBER 25

Fraud may occur through bank accounts and credit cards without notice. Check your statements often.

Fraudulent or simply incorrect transactions may occasionally hit your bank accounts or credit cards without you noticing. Some criminals will even test out new bank accounts or credit cards by putting through very small transactions, which will usually go unnoticed. Check your statements every month and follow up on any unusual activity. Even a small deposit in your transactions might actually be a criminal trying to determine whether your account is active.

OCTOBER 26

Transmitting confidential or sensitive information via email or IM may expose data to risk.

The transmission of confidential, private, sensitive, proprietary, or valuable information through email or IM may represent a significant security risk. Email and IM channels are usually unencrypted, allowing anyone to intercept or view this information. If you need to send sensitive data for business reasons, contact the help desk to find out more about sending encrypted data.

OCTOBER 27

Using the same password for multiple accounts could expose all your accounts following a single security breach. Use unique passwords for each account.

If you use the same password for multiple accounts, you increase your overall risk. The breach of a single account could potentially lead to the breach of all of your accounts, because when a hacker knows your username and password on one service, he or she will try the same login information on other services. Instead, use unique passwords for every account you have and change them often. Email addresses, personal banking, web services, mobile devices, and work computers should all have separate passwords.

OCTOBER 28

Viruses and malware can infect a device or computer via email attachments, links from any source, USB drives, and many other ways.

There are many ways in which malware may infect a system. USB drives, emailed files, instant messaging, web links, and applications are all among the major ways that a virus may be introduced. Comprehensive antivirus utilities may be used to scan risky files, and you can protect yourself and your system by avoiding any links, files, and removable media devices.

OCTOBER 29

Always be on guard against thieves looking to steal your laptop or mobile devices.

You should always secure your mobile device or laptop, especially when traveling or in an unfamiliar area. Your mobile device or laptop may have sensitive personal information on it or even confidential business data. Never bring a device that contains work information anywhere if it isn't necessary, and always keep an eye on your mobile device or laptop. Encrypt the data on your device or laptop, and ensure that it is password protected. If using a laptop for a long time in a single location, use a cable lock.

OCTOBER 30

Protect your data with secure storage and transmission. Otherwise, your data may be vulnerable.

Most users have sensitive data on their computer that could be used for malicious purposes: bank account information, personal information, and more. To protect this data, you should always use the appropriate encryption protocols for both storage and transmission. Encryption protocols seal stored data behind a virtual lock, protecting the data from hackers. Storage devices, such as a hard disk drive or a flash drive, should be encrypted and you should use secure Wi-Fi and SSL (secure socket layer) protection when transmitting sensitive information. Look for HTTPS in the web address to verify the data is being transmitted securely.

OCTOBER 31

Your instant messages are not private. Don't say anything you wouldn't want your employer seeing.

While at work, your email and instant message conversations are part of your workplace's data. You should never introduce anything into this professional data that you would not want your boss or colleagues to see. Always remain professional while you are at work and while you are talking to your colleagues.

NOV

2018



SUN	MON	TUE	WED	THU	FRI	SAT
				<p>New threats are constantly being developed. Protect your computer and devices with auto OS updates. 1</p>	<p>If you are suspicious about a call, ask for more information and report the incident to it security. 2</p>	<p>Identity theft can lead to a damaged credit score. Place stolen credit cards on fraud alert. 3</p>
<p>Network sharing can be dangerous. Turn off sharing when using your laptop in a public place. 4</p>	<p>Social media is viewable by anyone. Make sure your opinions are seen as your own, not the organization's. 5</p>	<p>Records should never be destroyed because they contain evidence of misconduct or embarrassing information. 6</p>	<p>Identity thieves may use unsolicited credit offers to gather information. Opt out. 7</p>	<p>If you don't know who an email is from, don't click on any hyperlinks or pictures in the email. 8</p>	<p>Don't allow others to view sensitive information on your screen over your shoulder. 9</p>	<p>Report any instances of fraud or attempted fraud you become aware of. 10</p>
<p>Turn in any information assets, such as USB drives, that you find to the security or IT department. 11</p>	<p>Be sure operating system and application updates on your computer are occurring on a regular basis. 12</p>	<p>Report the loss of any data assets, like printed docs, laptops, USB drives, smartphones, etc. to IT as soon as you become aware. 13</p>	<p>If you reuse passwords, a breach of one account becomes a breach of all of your accounts. Never reuse your passwords. 14</p>	<p>Some malware programs will require you pay to unlock your system. Avoid "ransomware" with good system security habits. 15</p>	<p>Computers aren't the only things with hard drives. Printers and fax machines need to be wiped clean before being disposed of. 16</p>	<p>Phishing attempts may be used to steal bank login details. Never use a link sent to you via email to access your bank account. 17</p>
<p>Your child may become the target of cyber bullying. Talk to your child about bullying and watch them for any behavioral changes. 18</p>	<p>You may not always be able to detect a phishing attack. If you believe you have fallen victim, contact the help desk. 19</p>	<p>Children often bully others, but that doesn't make it acceptable. If your child is becoming a cyber bully, take action immediately. 20</p>	<p>"Trolls" intentionally attempt to disrupt forums and blogs. Always ignore trolls; there is nothing to gain by arguing with them. 21</p>	<p>Data not properly backed up could be lost forever. Protect the data on your home computer with a cloud backup system. 22</p>	<p>Your personal home computer may become the target of attacks. Use a personal firewall to protect yourself. 23</p>	<p>Cyber bullying isn't just a matter for school officials. It's also a crime. Report any instances of cyber bullying to your local authorities. 24</p>
<p>Allowing remote access to your computer could let others use your computer from anywhere in the world. Turn off access for security. 25</p>	<p>Use a secure, encrypted channel, like a virtual private network (VPN) when working remotely to reduce security risks. 26</p>	<p>If you are hosting a visitor, be sure the visitor signs in at the front desk and is escorted at all times. 27</p>	<p>To reduce the risk of losing data during power spikes and failures, use a battery backup uninterruptible power supply. 28</p>	<p>Verify the identity of those who ask for information in person or over the phone, before you release any information. 29</p>	<p>For wireless network connections, be sure to use Wi-Fi protected access version 2 (WPA2). 30</p>	

NOVEMBER 1

New threats are constantly being developed. Protect your home computer and personal devices by automatically installing OS updates.

Home computers, laptops, tablets, smart phones, and other personal devices can be vulnerable to the latest threats if they are not frequently updated. Set your computers and devices to automatically download and install operating system updates as they are released. This will ensure that even new threats will not be a risk.

NOVEMBER 2

If you are suspicious about a call, ask for more information and report the incident to IT security.

Anyone can call and ask for information. If you believe that someone is attempting to get sensitive information from you or to get you to complete a task that could lead to a security breach, ask them for their name, number, and what they want. Report the incident to IT security before fulfilling any of their requests. The IT department will let you know if the request was legitimate.

NOVEMBER 3

Identity theft can lead to a damaged credit score. Place stolen credit cards on fraud alert with all three Reporting Agencies.

After reporting a stolen credit card to your credit card agency, you should also contact the three national credit reporting agencies to place a fraud alert on your account. Experian, TransUnion and Equifax can freeze your account to ensure that there are no new changes to your credit, such as new accounts being opened in your name.

NOVEMBER 4

Network sharing can be dangerous. Turn off sharing when using your laptop in a public place.

The sharing feature that lets you share music, videos, documents, and printers with other computers in your home can represent a security risk if you use it in a public place. Others could use this feature to view or even alter documents that you have on your computer. When using your laptop in a public location, turn off the sharing feature entirely.

NOVEMBER 5

Social media is viewable by anyone. Make sure your opinions are seen as your own, not the organization's.

Anyone can view your public social media accounts. If you make it known that you work for the organization, put a disclaimer on your social media accounts stating that any opinions you post are your own.

NOVEMBER 6

Records should never be destroyed because they contain evidence of misconduct or embarrassing information.

Never destroy documents simply because they are embarrassing or show instances of misconduct. This is true even if the documents expose illegal acts or are damaging to the organization. To destroy documents in this fashion would be considered an instance of a cover up. Hand any concerning documents to the appropriate supervisory staff instead.

NOVEMBER 7

Identity thieves may use unsolicited credit offers to gather information. Consider opting out.

Everyone gets unsolicited credit offers in the mail, but not all of these credit offers are legitimate. Identity thieves may send out these offers in an attempt to gather personal information from you. Consider opting out of all unsolicited credit card offers. If you are interested in a credit card, apply directly with the credit card service rather than responding back to unsolicited mail and only work with reputable credit card companies.

NOVEMBER 8

If you don't know who an email is from, don't click on any hyperlinks or pictures in the email.

Attackers embed hyperlinks to malicious websites into phishing emails in an attempt to infect your computer. If the email could possibly be legitimate, don't trust the link in the email. Look up the legitimate website independently and manually type the URL (Universal Resource Locator - like <http://www.inspiredelearning.com>) into the address bar, rather than clicking on the potentially bogus hyperlink in the suspicious email.

NOVEMBER 9

Don't allow others to view sensitive information on your screen over your shoulder.

This is called "shoulder surfing" and is one way that valuable information can be stolen. This type of attack takes advantage of the courtesy or trust offered by the victim.

NOVEMBER 10

Report any instances of fraud or attempted fraud you become aware of.

If you notice something "just a little off" in the records, or in another person's actions, this might be an indication of inappropriate or suspicious activities. There may be a simple and innocent mistake, or there may be something much more serious happening. Report these peculiarities to management and allow them to take a closer look as necessary.

NOVEMBER 11

Turn in any information assets, such as USB drives, that you find to the security or IT department.

Don't read the documents. Don't turn on the laptop computer. Don't plug in the USB flash drive. Don't access the CD or DVD disks. These supposedly "lost" documents and devices could contain misinformation or malicious software that could infect your computer and the network with eavesdropping or other types of malware.

NOVEMBER 12

Be sure operating system and application updates on your computer are occurring on a regular basis, typically at least weekly.

Your computer's operating system, applications, and antivirus software require regular updates. Without them, they become progressively more vulnerable to attack. These software components should be configured to update automatically. Report any update failure notices to the IT department.

NOVEMBER 13

Report the loss of any information assets, like printed documents, laptops, USB drives, smartphones, etc. To the IT or security department as soon as you recognize the items are missing.

The loss of devices is costly, but the loss of the information stored on the document or device is substantially more costly. The IT department has procedures to minimize the losses and can do it better when they can react quickly after the loss.

NOVEMBER 14

If you reuse passwords, a breach of one account becomes a breach of all of your accounts.

If you use the same password for all of your accounts and a single account is breached, all of your accounts will become vulnerable. Always use completely unique passwords for each of your accounts. Don't use variations of your password for separate sites, such as a base password that has a single alteration each time; these can be guessed.

NOVEMBER 15

Some malware programs will require that you pay to unlock your system. Avoid "ransomware" through good system security habits and do not make any payments.

Malware programs called "ransomware" will infect your computer and demand that you pay a "ransom" to the creator of the program to remove it. You should never pay the ransom requested; this will only give the creator of the program access to your personal and financial information. You can avoid ransomware by keeping your operating system updated, using an antivirus program and conducting regular system scans. Ransomware can be removed the same way as malware using an antivirus program.

NOVEMBER 16

Computers aren't the only things with hard drives. Printers and fax machines need to be wiped clean before being disposed of.

Printers and fax machines must have their hard drives completely wiped clean before being disposed of. These machines often keep copies of the last documents they printed or faxed in their memory. If you do not wipe their memory before disposing of them, you may put sensitive or confidential data at risk. Simply deleting the hard drive is not always enough because remnants of the data may be left behind. There are recycling companies that specialize in the destruction of data on these types of machines before breaking the machines down.

NOVEMBER 17

Phishing attempts may be used to steal bank login details. Never use a link sent to you via email to access your bank account.

Emails from your bank may be duplicated by con artists who are seeking to acquire your login details. These emails may appear to originate from your bank and may ask you to click a link to login and verify your information. Often, these emails may be extremely convincing and completely mimic the format of your bank. The link will often lead to a website that looks like your bank but is not. Always go to your bank directly by typing the URL into your browser. Never click on a link within an email to go to your bank.

NOVEMBER 18

Your child may become the target of cyberbullying. Talk to your child about bullying and watch them for any behavioral changes.

Cyberbullying can occur at any time and the signs of cyberbullying can be subtle. Every child is different. Watch for any behavioral changes in your child. If your child is ordinarily talkative, he or she may become unusually quiet. A usually obedient child may become disobedient or sullen. Make sure that you talk to your child about cyber bullying and monitor their Internet use. Cyberbullying can take a very serious emotional toll on a child and it isn't always easy to spot.

NOVEMBER 19

You may not always be able to detect a phishing attack. If you believe you have fallen victim, contact the help desk.

Many phishing attacks can be quite convincing and you may not realize that you have fallen victim to one until too late. If you feel that you may have accidentally given out sensitive or confidential data, you should immediately contact the Help Desk. They will be able to determine whether the email or call you received was legitimate.

NOVEMBER 20

Children often bully others, but that doesn't make it acceptable. If your child is becoming a cyberbully, take action immediately.

There are many reasons why children may begin bullying others. If you suspect that your child has been bullying others online, you should take action to get your child professional help. Your child may be acting out for reasons you aren't aware of, but the problem needs to be addressed immediately. Cyberbullying is a crime, and your child may face legal repercussions for their actions.

NOVEMBER 21

"Trolls" intentionally attempt to disrupt forums and blogs. Always ignore trolls.

Internet "trolls" are mean-spirited individuals who attempt to disrupt forums, blogs and social media accounts. They will often lash out to try to provoke an emotional response and they may come in groups. You should never try to argue with a troll; they already know they are wrong, they are simply trying to irritate you.

NOVEMBER 22

Data not properly backed up could be lost forever. Protect your computer data with a cloud backup system.

If you don't backup your data regularly, you may lose it. You can protect yourself through the use of a cloud backup system. A cloud backup system can usually be accessed from anywhere in the world and any device, provided that you have the password. Cloud backups are extremely stable and will back up your system automatically. Further, they are in a separate physical location from your data, allowing you to protect against fire and flood. However, they can also represent a security risk if not properly secured because of their accessibility, so always use a strong password with your cloud backup service.

NOVEMBER 23

Your personal home computer may become the target of attacks. Use a personal firewall to protect yourself.

To ensure that intruders cannot get into your home computer and steal or manipulate your data, use a personal firewall. Most computers will come with a firewall, such as the "Windows Firewall," already installed. Be sure it is turned on. You may also want to invest in a subscription-based antivirus and malware solution that also includes virus scanning and firewall.

NOVEMBER 24

Cyberbullying isn't just a matter for school officials. It's also a crime. Report cyberbullying to authorities.

Cyberbullying is a crime. If your child is the target of cyberbullying, you should document everything and contact both your child's school and the local authorities. This will increase the likelihood that the matter will be dealt with in an appropriate and productive way. It will also send a message to your child that they are protected and that what is happening to them is wrong.

NOVEMBER 25

Allowing remote access to your computer could let others use your computer from anywhere in the world. Keep remote access turned off to protect yourself.

The remote access setting of your computer allows others to connect to your computer from anywhere in the world. You should always have your computer set to deny remote access connections. Go to Windows -> Control panel -> System and Security -> System -> Remote Settings and select "Don't allow connections to this computer" under "Remote Desktop."

NOVEMBER 26

When connecting into the organization's network from a remote location, use a secure, encrypted channel, like a virtual private network (VPN).

Attackers can steal data in transit over the Internet if the data is not encrypted. To protect data in transit, be sure the VPN is established before sending or receiving information assets. Contact the IT department for more details.

NOVEMBER 27

If you are hosting a visitor, be sure the visitor signs in at the front desk and is escorted at all times.

Visitors should also always wear a visitor badge and return the visitor badge before leaving.

NOVEMBER 28

To reduce the risk of losing data during power spikes and power failures, use a battery backup uninterruptable power supply (UPS) on your computer.

The UPS knocks down hazardous voltage spikes that could damage your computer, and provides a few minutes of power from the battery to your computer when the power fails. This will give you the opportunity to save your work, close the applications, and shut down your computer cleanly.

NOVEMBER 29

Verify the identity of those who ask for information in person or over the phone, before releasing information.

You should also never give out information about other employees, remote network access, organizational practices, or strategies to any unknown individual.

NOVEMBER 30

For wireless network connections, be sure to use Wi-Fi protected access version 2 (WPA2).

WPA2 provides authentication to allow access for only authorized users and also encrypts all data in transit over the wireless connection, securing it from attackers. At home, use WPA2 Personal or WPA2 Home. At work, use WPA2 Enterprise. This is the strongest authentication and encryption mechanism available and helps to protect your information.

DEC 2018



SUN	MON	TUE	WED	THU	FRI	SAT
						Links can be misleading. Before clicking on a link, take another look. 1
Sensitive data can become vulnerable when accessed through public computers. 2	Scams may be disguised as investment opportunities. Be skeptical of any opportunities you receive via email. 3	Pass phrases are more secure than traditional passwords. Use long pass phrases when securing sensitive data. 4	Hackers can take control of a computer and use it for their own purposes. Keep your computer secured at all times. 5	Identity thieves often target large retail chains to steal customer data. Pay attention to the news for data breaches. 6	SMiShing is a type of phishing by mobile phone. Learn to recognize the signs. 7	Printed docs need to be protected just like the originals. Keep them secured when working from home. 8
Con artists may approach you with free prizes that require hidden fees. Never accept a free prize that has a catch. 9	Scammers target you via social media accounts. Don't accept connections requests from individuals you don't know. 10	Malware and other security threats can be anywhere on the web. Protect yourself with a web filter. 11	Scammers keep contacting you even after you've rebuked them. Block them to reduce the possibility of issues in the future. 12	Anyone with access to your computer or device could potentially infect it with malware. 13	Do not write down your passwords on a list. 14	Choose long and complex passwords. 15
Hover over hyperlinks in email messages to see where they really lead. 16	Don't open windows or pop open external doors unless it is specifically authorized. 17	If you see someone without an ID badge, escort to the security desk or report to security right away. 18	Social networks can be used to spread malware. Never click on unknown links or downloads through social media accounts. 19	Online auctions can be dangerous. Never give out personal information to a seller on an online auction service. 20	Malware may hijack your computer's webcam. If you notice your webcam's light on, immediately take action. 21	Your mother's maiden name can be used by identity thieves. Make sure you keep it safe. 22
Twitter is a public social media platform. Never post personally identifiable information. 23	Your email software can learn to identify spam. Flag unwanted emails as Spam to ensure security. 24	Public computers may be infected with malware or have other security issues. 25	Fighting back doesn't work with bullies, especially on the web. Educate your child on proper responses. 26	If you suspect your child is bullying others, talk to them now. They need to understand the consequences of their actions. 27	Personal firewalls are able to monitor and manage connections to and from your computer. 28	Areas that require a badge or key card to access are restricted. Always securely close the door behind you. 29
Social engineers gain your trust then request sensitive information. Always be skeptical of unknown people. 30	Identity theft can happen at any time. Check your credit report regularly to protect yourself. 31					

DECEMBER 1

Links can be misleading. Before clicking on a link, take another look.

Don't just click on links that you have received through email or instant messenger. Even if the link text looks like a URL, the link could be going somewhere else. Instead, move your mouse pointer over the link without clicking on it. Look at where the link is going in the status bar. If the link is not going where it should be or is pointing to a file (such as a .exe), don't click on the link.

DECEMBER 2

Sensitive data can become vulnerable when accessed through public computers.

Whether you are in a café or a hotel's business center, the computers you use may not be secured properly. The computers in these public centers may be infected with malicious software or could otherwise have serious security vulnerabilities. You may even accidentally leave confidential or sensitive information on the computer after you're done. Only use your own computer when you need to work away from the office.

DECEMBER 3

Scams may be disguised as investment opportunities. Be skeptical of investment opportunities through email.

If you receive an unsolicited investment opportunity through email, it's very likely a fraud. These scams often claim to be able to make you large amounts of money in short amounts of time or with a very small initial investment. You should ignore any investment opportunities that you have not inquired directly about. If it seems to be too good to be true, it probably is.

DECEMBER 4

Pass phrases are more secure than traditional passwords. Use long pass phrases when securing sensitive data.

A pass phrase is a long phrase that is used in place of a password, such as "IamGoingtoEataPie!" Pass phrases are easier to remember than traditional passwords and more difficult for a hacker to guess. Use proper capitalization and punctuation in your pass phrase to increase its complexity and make it even more secure. Use a phrase that you'll find easy to remember and resist the urge to write it down or store it in a computer file.

DECEMBER 5

Hackers can take control of a computer and use it for their own purposes. Keep your computer secured and learn to recognize the signs of infection.

A virus or malicious program may not directly damage your computer but may instead turn it into a zombie. A zombie computer is a computer that a hacker can direct to complete certain tasks, such as attacking another target. Always keep your devices secured with antivirus protection to avoid this and complete a full system scan if you suspect your computer has been compromised. A compromised computer may begin running sluggishly, start crashing or begin performing tasks on its own.

DECEMBER 6

Identity thieves often target large retail chains to steal customer data. Pay attention to any data breaches.

Identity thieves may break into the computer systems of large retail chains and steal customer data, such as credit card information or other personal information. To protect yourself, you should keep current on the news. If a chain that you shop at has been breached, your data is likely not safe. You should take immediate action to protect yourself, such as freezing your credit report.

DECEMBER 7

SMishing is a type of phishing done by mobile phone. SMishing is just as dangerous as phishing: learn to recognize the signs.

SMishing involves text messages sent to you in an attempt to get you to visit a link or send personal or confidential data to the sender. The text message may claim to be from your cell phone provider and request your payment information, or may prompt you to click on a link and fill out a form to gain access to a prize. You should delete any unsolicited text messages; they are almost always attempts to gain personal or confidential data from you.

DECEMBER 8

Printed documents need to be protected just like the originals. Keep them secured when working from home.

When working remotely from home you may occasionally need to print out workplace information. Printed workplace documents must be protected with the same levels of data security as the originals. The same destruction rules apply to a copy. Workplace documents should be shredded after they have been used and should never be left in public areas.

DECEMBER 9

Con artists may approach you with free prizes that require hidden fees.

If you have won a free prize, the prize should be entirely free. Con artists may attempt to scam you out of money by claiming that you have won a prize but that you need to pay government taxes or customs fees on the value of the item. You will either never receive the item or end up paying more than the item is truly worth. If someone offering you a prize tells you that you need to pay them for taxes, shipping or any other hidden fees, it is a scam. Stop all communication.

DECEMBER 10

Scammers may target you through social media accounts. Don't accept friend or connection requests from individuals you don't know.

Con artists and identity thieves may conduct scams through social media accounts. They may befriend you so that they can get enough information about you to steal your identity. They may even try to access your friend list so that they can attempt to scam your family and friends. To protect yourself from this, always make sure that you know someone before adding them to your social media accounts and make sure any sensitive or identifying information about you is hidden from those not on your friend list.

DECEMBER 11

Malware and other security threats can be anywhere on the web. Protect yourself with a web filter.

When browsing the web you may stumble upon a website that contains malware or viruses. You can protect yourself by using a web filter. Web filters scan the websites you view to determine whether they are safe. If the website is not safe, the web filter will block the site and will send you an alert to let you know that the site you're trying to access could be dangerous. Web filters are often integrated into antivirus solutions as a part of a more comprehensive security system.

DECEMBER 12

Scammers may keep contacting you even after you've rebuked them. Block them to reduce the possibility of issues in the future.

Once you have identified someone as a scammer you should block them to prevent them from contacting you again. On most instant messenger services, you can simply right click on the person's name and then select the "block" option. This will ensure that they cannot contact you or even see you online. You can also block emails by going into your options and adding the person's email address to your "Blocked Addresses" lists. If you do not block a scammer, they may continue bothering you or sending you potentially harmful files and links.

DECEMBER 13

Anyone with access to your computer or mobile device could potentially infect it with malware. Never let friends or family use your computer.

Friends or family members, especially children, could unintentionally infect your computer or mobile device with malware. When this occurs, all of the data on the computer or device could become compromised. If your computer has access to your workplace information, you should never let anyone else use it. This is true even if you create a guest account for them to use.

DECEMBER 14

Do not write down your passwords on a list.

This list can be lost or stolen giving someone else access to all of your most sensitive information. If you have more passwords than you can remember, an approved password vault application might be a good solution. Contact the IT department to show you how to securely store this sensitive information.

DECEMBER 15

Choose long and complex passwords.

The longer a password is, in most cases, the stronger it is. Use combinations of upper case alpha characters, lower case alpha characters, numbers, and symbols in your passwords. You can generate a password that is easy to remember by using the first letter of each word in a sentence and substituting numbers for words like "to" and "for." For example, "I enjoy going to the movies twice per month." would be "leg2tmtpm."

DECEMBER 16

Hover over hyperlinks in email messages to see where they really lead.

A hyperlink that says "Bank.com" could actually lead to another location, because the text of a hyperlink can be anything at all. However, if you hover over the link with your mouse cursor, a tooltip will show the actual destination.

DECEMBER 17

Don't open windows or prop open external doors unless it is specifically authorized.

Leaving doors or windows open can give attackers access to valuable physical and information assets, and can lead to threats to employee safety. Close and lock open doors and windows, then report the details to management or the security department.

DECEMBER 18

If you see someone without an id or visitor badge, politely escort the person to the security desk for sign in or report it to security right away.

Identification badges help keep criminals and other malicious people out of our facilities by letting everyone know who belongs in our facilities and who doesn't. By recognizing and reporting anyone who does not have an ID badge, you're helping keep our facilities safe and secure.

DECEMBER 19

Social networks can be used to spread malware. Never click on unknown links or download files through social media accounts.

Links and files on social networks can include viruses and malware. Never click on links from people that you don't know and don't download files that are sent to you through a social media platform. Be skeptical of any links that look unusual, such as a link that comes from someone you haven't spoken to in a long time. Even someone you know could have their account hacked and used to send out malware.

DECEMBER 20

Online auctions can be dangerous. Never give out personal information to a seller on an online auction service.

Sellers on online auction sites may attempt to steal your identity or your other personal information. A seller on an online auction should not need any personal information from you to complete the transaction, send your goods, or receive your payment. The seller should receive all of this information directly from the auction site. Never communicate with a seller outside of the auction site and never attempt to complete the sale on another site.

DECEMBER 21

Malware may hijack your computer's webcam. If you notice your webcam's light on, take action immediately. Some malware programs will access your computer's webcam and begin streaming the video without your permission. You can tell whether your webcam is active by looking at the camera's light; if the camera's light is on and you are not currently recording, someone else has hijacked your computer. Place a piece of opaque tape over your webcam's lens immediately and then run a malware scanner to remove the software that is enabling the camera.

DECEMBER 22

Your mother's maiden name can be used by identity thieves. Make sure you keep it safe.

In addition to passwords and birthdays, your mother's maiden name can also be used to steal your identity. A mother's maiden name has long been used as a verification question for financial accounts, and social media has made it so that maiden names are often displayed alongside married names.

DECEMBER 23

Twitter is a completely public social media platform. Never post any personally identifiable information.

Everything you post on Twitter is made public and is indexed by search engines. You should never post information that could be used to identify you on social media accounts, nor should you post any sensitive or confidential workplace information such as information about a client or an account. You should also avoid using a username that might include identifiable information, such as part of your name or your year of birth.

DECEMBER 24

Your email software learns to identify spam. Flag unwanted emails as spam to ensure they are sorted correctly.

Don't just delete Spam mail. If you flag your spam mail as spam, your email software will move it to your spam folder and will know to mark similar emails as spam in the future. This will reduce the amount of time it takes to look through and sort your emails and will ensure that you don't accidentally open a spam email that could potentially contain malicious materials.

DECEMBER 25

Public computers may be infected with malware or have other security issues. Never use untrusted computers.

Public computers, such as those at hotel business centers, libraries or Internet kiosks, may not be appropriately secured. They could be infected or have keyloggers on them, which could potentially compromise your data. You could also forget to log out, leaving your account vulnerable to intrusion. To avoid this, don't log into your account on a public computer. When traveling for work, use your work computer and always use a secured Internet connection.

DECEMBER 26

Fighting back doesn't work with bullies, especially on the web. Educate your child on the proper responses.

Your child should never attempt to fight back against a cyberbully. There could be legal repercussions and the situation could simply escalate. Everything that is posted on the web will remain on the web forever. Rather than fighting back online, you should work with your child to fight back through the school system and legal channels.

DECEMBER 27

If you suspect your child is bullying others, talk to them now about the consequences of their actions.

Kids don't always understand the effect they can have on others or the legal consequences of their actions. If you suspect that your child is bullying others online, you should talk to them to determine the extent of the problem. Let them know cyberbullying is a crime and how badly they could hurt others. Consider getting professional help if cyber bullying is a symptom of a larger problem.

DECEMBER 28

Personal firewalls are able to monitor and manage connections to and from your computer.

A personal firewall can reject connections coming into and going out from your computer and will prompt you any time a new connection has been attempted. By using a personal firewall, you can control access to your computer and ensure that programs don't attempt to send information out when you don't want them to. Always keep your personal firewall on to maintain security.

DECEMBER 29

Areas that require a badge or key card to access are restricted. Always securely close the door behind you.

Any area that requires security clearance, such as a badge or key card, to access is an area that must be protected from intrusion. You should always make sure that you close the door securely behind you, even if you are going to be going in and out quickly. In the time that it takes you to enter and exit, someone else could do the same.

DECEMBER 30

Social engineers gain your trust then request sensitive information. Always be skeptical of unknown people.

Anyone can call to ask you for sensitive information. Social engineers will often call and pretend to work for your organization. Some of them may even be able to give you details about your department, your position, and the information they need. It's important to never release any information to someone who you don't know and who has not had their credentials verified. When you are talking to a new person, you should verify their identity and get authorization before sharing information.

DECEMBER 31

Identity theft can happen at any time. Check your credit report regularly to protect yourself.

Identity theft is becoming more common and can happen at any time. You can protect yourself from identity theft by checking your credit report on a regular basis. Look for any irregularities and notify credit bureaus at once if you notice anomalies.



 inspired eLearning®
education for your enterprise