2023 Newsletters

- Adware: What is it & How to Prevent it
- Cybersecurity Awareness
- Cybersecurity Awareness Month: Check In
- Cybersecurity Awareness Month: Have I been pwned?
- Cybersecurity Awareness Month: Kickoff
- Cybersecurity Awareness Month: Wrap Up
- Cybersecurity News & Training
- Malware
- Ransomware. Game Over.
- Spear Phishing vs Phishing: What's the Difference?
- Stay Safe for the Holidays

Adware: What is it & How to Prevent it

June 13, 2023

Spyware is harmful software. When installed on your device, it may send pop-up ads, redirect browsers to different websites, or secretly monitor user behavior. The hacker collects personal information, from your computer, without your consent, and sends the information to third parties to do damage or possible steal your identity.

5 Types of Spyware:

There are many different types of spyware – here are a few examples:

- Adware – displays unwanted advertisements (ads) on your device; often bundled with other software and may be difficult to remove
- Trojans – malicious programs disguised as legitimate software; once installed, may perform many harmful actions such as stealing personal information, or giving hackers remote access to your system
- Keyloggers – records everything you type on your keyboard; may include passwords or credit card numbers
- Password Stealers – designed to steal your login credentials; may capture passwords when you type them in or extract them from your device's memory
- Mobile Spyware – designed to target mobile devices and tablets; used to monitor calls, text messages, and location

Adware is the most common type of spyware; we will focus on this area below.

How does Adware work?

Adware, also known as advertisement-supported software, is created to show you ads forcibly, as a pop-up. The ads and offers you receive are based on websites you visit. The purpose is for creators and distributing vendors to make money through ads.

- Pay-per-click – paid each time you click on an ad
- Pay-per-view – paid each time ads are shown to you
- Pay-per-install – paid each time bundled software is installed on a computer

Adware quietly installs itself, onto your computer, through software. Search and browsing history may be tracked, to display ads targeted towards individuals. The hope is for you to click – accidentally or not – on the displayed ad and generate money for the developers.

Signs of Infection

If you experience any of the following symptoms, your computer may be infected with adware/spyware and/or another malicious program.

- Computer performs slower than normal and/or freezes/crashes
- Changes in your web browser homepage and/or search settings
- Difficulty loading the web browser
- Web pages do not display correctly
- Pop-up ads appear, even when you are not browsing the internet
- Internet speed is slower than normal
- Searches are redirected to sites you do not expect
- Ads appear out of context, or in places where you have not seen them in the past
- New extensions or toolbars appear on your browser
- New applications/icons appear on your computer

If you suspect your computer is infected, please take the following steps:

1. Disconnect your computer from the network
2. Disable the wireless connectivity
3. Contact the MCC Help Desk: (254) 299-8077 or helpdesk@mclennan.edu

Ways to Prevent Infection

Remember, adware is another way for cyber criminals to breach your company and cause financial or reputational harm. It is a scam, and you may be misled. To help prevent a possible infection, take the following steps:

- Keep your software up-to-date
- Turn on pop-up blocker in your browser
- Avoid free downloads, especially from questionable sources
- Avoid opening attachments/links sent via email, chat, or text unless you trust the source/sender
- Avoid clicking on pop-up window links or responding to questions in a pop-up window

Cybersecurity Awareness

September 6, 2023

We live in a digital age, where we interact with technology and the internet on a daily basis. This should make cybersecurity a top priority. What is Cybersecurity? The practice of protecting internet-connected systems, including hardware, software, and data, from attack, damage, or unauthorized access.

Cybersecurity Awareness Month (CAM)

Cybersecurity Awareness Month was launched by the National Cybersecurity Alliance (NCA) and the U.S. Department of Homeland Security (DHS) in October 2004 as a broad effort to help all Americans stay safe and more secure online.

Cybersecurity Awareness Month – observed every October – is a collaboration between the government and private industry to raise awareness about digital security. The goal is to empower everyone to protect their personal data from digital forms of crime.

History Highlights

2009

- DHS Secretary launched a Cybersecurity Awareness Month event in Washington, D.C. – became the highest-ranking government official to participate in the months' activities

2010

- STOP. THINK. CONNECT campaign launched – featured in the president's proclamation for the month, as the national cybersecurity education and awareness message
- NCA moved the launch, to sites around the country – previous sites included: Seattle and Bellevue, WA, Ypsilanti, MI, Omaha, NE, Boston, MA, Nashville, TN and Washington, D.C.

2011

- NCA and DHS developed the concept of weekly themes, during the month – made aspects of cybersecurity easier to communicate and aligned other groups with the specific themes

2023 Key Behaviors

The National Cybersecurity Alliance will focus on the following key behaviors for 2023 Cybersecurity Awareness Month:

- Enable Multi-Factor Authentication
- Use Strong Passwords and a Password Manager
- Update Software
- Recognize and Report Phishing

MCC Campus Events to Celebrate

Don’t get spooked by cybersecurity! During the month of October, the ISS – Cybersecurity Team will be celebrating Cybersecurity Awareness Month. Come join in the fun, learn about good cyber hygiene behaviors and ways to stay safe in this digital world.

Date	Time	Location	Audience	Sponsor
Monday, 10/2/23	1130am – 130pm	Table outside, MAC building	Students/faculty/staff	ISS – Cybersecurity Team
Tuesday, 10/17/23	12pm – 1pm	Presentation: Staying Safe Online, LTC 318	Students/faculty/staff	Jean Nixon, Academic Support & Tutoring
Monday, 10/30/23	1130am – 130pm	Table outside café, LTC building	Students/faculty/staff	ISS – Cybersecurity Team

Get Social

In October, use #CybersecurityAwarenessMonth to share tips, tricks or anything cybersecurity related!

Cybersecurity Awareness Month: Check In

October 17, 2023

Cybersecurity is a rapidly growing industry. It has become an essential part of every organization's strategy for sustainability, security, and growth. 2022 broke records for the number of cyberattacks, phishing scams, and data breaches. According the University of Maryland, hackers attack every 39 seconds 2,2,44 times per day. No one is immune from the threat of an attacker.

There is also a shortage of skilled professionals. A recent Forbes article estimated there are more than 700,000 open cybersecurity jobs in the U.S. with approximately 82,000 located in Texas. Industry growth and the need for a qualified workforce creates a unique opportunity.

Central Texas Cyber Range

In September 2023, Baylor University launched the Central Texas Cyber Range (CTCR). This is a joint venture between Baylor and McLennan Community College (MCC) to educate and train cybersecurity leaders, provide research, consulting, and engagement on the local, national, and international levels.

Both institutions are designated as a National Center of Academic Excellence in Cyber Defense (CAE-CD) by the National Security Agency and Department of Homeland Security.

Future initiatives, in development, include certification programs and bachelor's degrees in cybersecurity with a pathway from MCC to Baylor. MCC currently offers education through the Computer Information Systems & Multimedia program, with pathways to cybersecurity certifications and associate's level degrees. This expanded partnership allows us to educate and nurture future leaders in cybersecurity.

MCC Campus Event: Tuesday, October 17th

- **Who:** Presentation by Jean Nixon, Academic Support & Tutoring, for students, faculty, and staff
- **What:** Don't Open the Door to Strangers: Stay Safe on the Internet
- **When:** Tuesday, October 17th from: 12-1pm
- **Where:** LTC 318 or Zoom: https://mclennan.zoom.us/j/2549998332

Safety on the Internet is a vast and important topic that affects us all. We will discuss some simple tips and vocabulary words to better educate and protect ourselves while browsing the web, using social media, or shopping online. Join us tomorrow to learn more.

2023 Key Behaviors

- Enable Multi-Factor Authentication
- Use Strong Passwords and a Password Manager
- Update Software
- Recognize and Report Phishing

What's so important about **software updates**? Updates are one of the easiest ways to boost your cybersecurity. Developers are constantly looking for clues hackers are trying to break into their systems or holes for cybercriminals. To fix these issues, and improve security, software companies release regular updates. It is important to install the latest update, to receive access to the latest features and services, and get the best security.

Automatic Updates

Set up automatic updates to make your life easier. This will ensure updates are downloaded and installed as soon as they are available from the device, software, or app creator. You may have to restart your device to fully install the update. These can be scheduled to take place when you are not using your device, like the middle of the night.

Update from the Source

Before downloading anything, be sure you know the source. Only download from verified sources or your device's official app store. Remember, pirated, hacked, or unlicensed software can often spread malware, viruses, or other cybersecurity nightmares to your network. It isn't worth the risk!

Don't Fall for Fakes!

Have you ever come across a suspicious pop-up window, urgently demanding you download a software update? These are common on shady websites, or if there is malware already on your machine. These are attempts at phishing and are fake. Don't click any buttons on these pop-ups, and close the browser. Many web browsers will warn you if you are attempting to visit an unsecure web site. Heed the warnings, and don't take the bait!

Make it a Habit

If you decide against automatic updates, make it a habit to check and update your device and apps regularly. At a minimum, check monthly. Ideally, weekly checks are best. Often times, you will be notified when updates are available. It can be a pain to close out of your programs and restart your device, but make sure you update. Remember, updates are part of our digital lifecycle. If you

embrace them, you will have more peace of mind, the latest security, and the best new features!

QR Discount for Password Manager

Remembering all my passwords is so hard! This is where a password manger comes into play. This is similar to a vault with all of your passwords in one place. You only need to remember the vault combination to open and access all of your passwords.

Dashlane is discounting their password manager, for the month of October, for all MCC students, faculty, and staff. The QR code is 50% off the first year of service (regular cost is $60/ year).

Scan the QR code with your phone and enter code: mcl50 (Lowercase “L”). You must sign up by October 31, 2023, in order for the discount to apply.

Get Social

Do you have any tips or tricks? Share and tag your posts:

- #CybersecurityAwarenessMonth
- #BeCyberSmart
- #StaySafeOnline

Cybersecurity Awareness Month: Have I been pwned?

October 10, 2023

Have you ever heard the term “pwned”? The term is a typo of the word “owned” – the “o” and “p” are next to each other on the keyboard. The term implies someone has been controlled or compromised.

You may check your email address to see if you have been compromised in a data breach: https://haveibeenpwned.com/. If your email has been in a breach you will receive a message: Oh no – pwned! Don’t worry; it’s not the end of the world.

What to do? Password Tips:

If your email has been compromised, and you have not changed your password since the date of the breach; change your password. Keep these tips in mind, when creating a new password:

- Strong – long (at least 12 characters)
- Complex – combination of upper-/lower-case letters, numbers, and special characters
- Unique – never reuse – none of your passwords should look alike
- Multi-Factor Authentication (MFA) – enter your username and password, and prove your identity by responding to an email/text

QR Discount for Password Manager

similar to a vault with all of your passwords in one place. You only need to remember the vault combination to open and access all of your passwords.

Dashlane is discounting their password manager, for the month of October, for all MCC students, faculty, and staff. The QR code is 50% off the first year of service (regular cost is $60/ year).

Scan the QR code with your phone and enter code: mcl50 (Lowercase “L”). You must sign up by October 31, 2023, in order for the discount to apply.

Upcoming MCC Campus Events

Come see us! We have free giveaways and can answer any of your Cybersecurity questions!

Tuesday, October 17th

- **Who:** Presentation by Jean Nixon, Academic Support & Tutoring, for students, faculty, and staff
- **What:** Don’t Open the Door to Strangers: Stay Safe on the Internet
- **When:** Tuesday, October 17th from: 12-1pm
- **Where:** LTC 318 or Zoom: https://mclennan.zoom.us/j/2549998332

Monday, October 30th

- **Who:** Open to students, faculty, and staff
- **What:** ISS – Cybersecurity Team Event
- **When:** Today – Monday, October 2nd from: 1130am – 130pm
- **Where:** Table outside the LTC building

Get Social

Do you have any tips or tricks? Share and tag your posts:

- #CybersecurityAwarenessMonth
- #BeCyberSmart
- #StaySafeOnline

Cybersecurity Awareness Month: Kickoff

October 2, 2023

Happy Cybersecurity Awareness Month!

McLennan Community College (MCC) is recognized as a 2023 Champion Organization with the National Cybersecurity Alliance (NCA). We believe continuous education and learning is vital to protect personal and organizational data. The ISS – Cybersecurity Team hopes to bring awareness and understanding to students, faculty and staff about the part we all play in defending against cyber threats.

MCC Campus Event: Today, Monday, October 2nd

- **Who:** Open to students, faculty, and staff
- **What:** ISS – Cybersecurity Team Event
- **When:** Today – Monday, October 2nd from: 1130am – 130pm
- **Where:** Table outside the MAC building

Have you ever heard the term “pwned” [pronounced: OHND]? No, it is not misspelled. The term was first introduced in a video game and is a take on the word “owned” – the “o” and “p” are next to each other on the keyboard. The term implies someone has been controlled or compromised.

You may be wondering; have I been pwned? Come see us today to check if your email has been compromised. We have a QR discount code, for helpful tools, password tips and fun giveaways!

2023 Key Behaviors

Enable Multi-Factor Authentication

Use Strong Passwords and a Password Manager

- Update Software
- Recognize and Report Phishing

Passwords are the keys to your digital house. Just like housekeys, you want to do everything you can to keep your passwords safe.

Multi-Factor Authentication (MFA)

This is sometimes called two-factor authentication or two-step verification. It is a cybersecurity measure for an account and requires anyone logging in to prove their identity in multiple ways. Typically, you enter your username, password, and then prove your identity some other way, such as responding to a text message.

Why go through the trouble? MFA makes it extremely hard for hackers to access your online accounts, even if they have your password. It adds another layer of security and peace of mind.

Strong Passwords

All passwords should be created with three principles in mind: long, unique, and complex. Creating, storing and remembering passwords can be a pain, but the truth is passwords are your first line of defense against cybercriminals and data breaches.

Every password should be at least 12 characters long. Each account needs its own unique password – never reuse passwords. This way, if one of your accounts is compromised, other accounts remain secure. This does not mean changing one character or adding a “2” at the end – none of your passwords should look alike. Each unique password should be a combination of upper- and lower-case letters, numbers, and special characters.

Time for Hackers to Brute Force a Password

Many times, hackers obtain passwords through a brute force attack. They use automation and scripts to try and guess passwords. This allows hackers to make a few hundred guesses every second!

Brute force attacks make it easy for cybercrimes to hack simple passwords. The more characters in a password with the addition of numbers, upper and lowercase letters, and symbols, the odds of a brute force attack decrease significantly.

As you can see, in the table below – passwords with at least 12 characters using numbers and upper and lowercase letters – the time to hack is 53 years. Adding symbols increase the time to hack to 226 years!

Number of Characters in Password	Numbers Only	Lowercase Letters	Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters, Symbols
4-6	**Instantly**	**Instantly**	**Instantly**	**Instantly**	**Instantly**
7	**Instantly**	Instantly	**1 sec**	**2 secs**	**4 secs**
8	Instantly	Instantly	**28 secs**	**2 mins**	**5 mins**
9	Instantly	**3 secs**	**24 mins**	**2 hours**	**6 hours**
10	Instantly	**1 min**	**21 hours**	**5 days**	**2 weeks**
11	Instantly	**32 mins**	**1 month**	**10 months**	**3 years**
12	**1 sec**	**14 hours**	**6 years**	**53 years**	**226 years**

How often do I need to change my password? If your passwords are created with these principles, you do not need to change it. You only need to change if you are aware of an unauthorized person accessing your account, or the password was part of a data breech. If you frequently change your password, you risk reusing old passwords or creating similar/weak passwords.

Password Manager

Remembering all my passwords is so hard! This is where a password manger comes into play. This is similar to a vault with all of your passwords in one place. You only need to remember the vault combination to open and access all of your passwords. They take the form of apps or may be included automatically in your browser or operating system (OS). Apple's iCloud Keychain is an example of a password manger.

With a few clicks, you can generate new, secure passwords that are long, unique, and complex. The password manager automatically stores passwords and can autofill them when you arrive at the applicable site. When you log into a site, your password manager will ask if you want to store the password – click yes, and another account is secured. To keep it extra safe, secure it with MFA.

Password managers are best for keeping your passwords safe. Some advantages include: saves time, works across all your devices and OS, protects your identity, notifies you of potential phishing websites, and alerts you when a password has potentially become compromised.

Is this safe? Yes. Password managers use: encryption, multi-factor authentication, and zero knowledge. Your passwords are basically impossible to decode if a hacker tried to breech your password manger. The best password managers require MFA to login. This creates extra security and requires anyone trying to view your password from an unfamiliar device to login multiple ways. A password manager does not know what your password is – the company never stores your main password on the system's servers. You are the only one with the vault combination.

Get Social

Do you have any tips or tricks? Share and tag your posts:

- #CybersecurityAwarenessMonth
- #BeCyberSmart
- #StaySafeOnline

Cybersecurity Awareness Month: Wrap Up

October 30, 2023

Thank you for making MCC's 1st Annual Cybersecurity Awareness Month a success! We have one last event today and one more 2023 Key Behavior to cover: recognize and report phishing.

MCC Event: Today, Monday, October 30th

- **Who:** Open to students, faculty, and staff
- **What:** ISS – Cybersecurity Team Event
- **When:** Today – Monday, October 30th from: 1130am – 130pm
- **Where:** Table outside the café, of the LTC building

Did you miss our event on October 2nd? Come see us today to check if your email has been compromised (pwned). Or, try to spot the phishing email. We still have a QR discount code, for helpful tools, candy, and fun giveaways!

2023 Key Behaviors

- Enable Multi-Factor Authentication
- Use Strong Passwords and a Password Manager
- Update Software
- Recognize and Report Phishing

Cybercriminals like to go **phishing,** but you don't have to take the bait.

Phishing is when criminals use fake emails, social media posts, or direct messages (DMs) with the goal of luring you to click on a bad link or download a malicious attachment. Clicking on a link or file can hand your personal information over to cybercriminals or install malware onto your device.

No need to fear your inbox. With some knowledge, you can outsmart the phishers every day.

Recognize a Phishing Attempt

Remember the signs of a phishing email can be very subtle. It is important to review (take 4 seconds) and ensure an email is legit to avoid falling for it. We have discussed ways to recognize phishing attempts in previous IT Cybersecurity Newsletters – hopefully, these sound familiar.

- Does it contain an offer that's too good to be true?
- Does it include language that's urgent, alarming, or threatening?

- Is it poorly crafted writing riddled with misspellings and bad grammar?
- Is the greeting ambiguous or very generic?
- Does it include requests to send personal information?
- Does it stress an urgency to click on an unfamiliar hyperlink or attachment?
- Is it a strange or abrupt business request?
- Does the sender's email address match the company it's coming from? Look for little misspellings like pavpal.com (instead of paypal.com) or anazon.com (instead of amazon.com).

I see a phishing email. What do I do?

Don't worry; the hard part is recognizing the email is fake. If you are at MCC, and the email came from your work/student email, report it to helpdesk@mclennan.edu as quickly as possible.

If the email came to your personal email, don't do what it says. **Do not** click on any links – **even the unsubscribe link** – or reply back to the email. Use the delete button.

Remember, DON'T CLICK ON LINKS, JUST DELETE.

Summary of Cybersecurity Best Practices

The month is ending, but that doesn't mean cybersecurity best practices should end. Cyberattacks are possible all year round. Remember these best practices to help keep you cyber safe today and every day.

1. Create long, unique, and complex passwords for every account.
2. Do not reuse passwords.
3. Use two-step authentication and a password manager.
4. Setup automatic software updates.
5. Only download software from a verified source or your device's official app store.
6. Do not fall for pop-up windows, urgently demanding you download a software update.
7. Routinely check and update your device/apps either: monthly (minimum) or weekly (best).
8. Recognize phishing attempts; take at least 4 seconds to review and ensure an email is legit.
9. If you see a phishing email, remember: DON'T CLICK ON LINKS, JUST DELETE.
10. Report phishing attempts ASAP.

QR Discount Code for Password Manager

Remembering all my passwords is so hard! This is where a password manger comes into play. This is similar to a vault with all of your passwords in one place. You only need to remember the vault combination to open and access all of your passwords.

Dashlane is discounting their password manager, for the month of October, for all MCC students, faculty, and staff. The QR code is 50% off the first year of service (regular cost is $60/ year).

Scan the QR code with your phone and enter code: mcl50 (Lowercase “L”). You must sign up by October 31, 2023, in order for the discount to apply.

Get Social

Do you have any tips or tricks? Share and tag your posts:

- #BeCyberSmart
- #StaySafeOnline

Cybersecurity News & Training

April 3, 2023

Information Systems & Services (ISS) is made up of a few different teams. To keep the community informed and up-to-date with security awareness, our Cybersecurity Team plans to send out a monthly newsletter. Our goal is to help you better understand cybersecurity and provide you with the knowledge and skills to recognize, report, and prevent cyberattacks within MCC.

Cybercrime is on the rise. The easiest way for hackers to get to an organization is through you! Hackers may use different types of cyberattacks including: digital, in-person, or phone.

How does ISS help?

We have a Cybersecurity team who is dedicated to the safety of our community and the security of internet-connected systems and services. This team responds to events, develops standards, provides cybersecurity professional development, and audits IT systems.

Currently, we use Barracuda to filter and block SPAM or phishing emails.

Cybersecurity Training Starts This Week

Starting today, you will receive emails from KnowBe4 for training. This email will contain a link to the training. The training is one video. Training ends on 4/17.

The from address will be: **KnowBe4 <do-not-reply@training.knowbe4.com>**

The subject will read: **You've been enrolled in training**

This training is required in accordance with Section 2054.5191 of The State of Texas Government Code. Professional Development credit is not allowed for state mandated training.

How else can you help?

As students, faculty, and staff, please be aware. Phishing is the most common form of an attack. Here are a few red flags to keep in mind:

- FROM: an email from an unknown sender; you know the sender, but the email looks funny
- TO: you were copied on an email and you do not know the other people also in the email

- DATE: you receive an email you would normally receive during business hours, but it was sent at 4am
- SUBJECT: the subject line does not make sense or does not match the message content; the email is about something you never requested, or a receipt for something you never purchased
- CONTENT: the sender is asking you to click on a link to open an attachment; you have an uncomfortable feeling, or it seems odd
- ATTACHMENT: any attachment you receive, and you were not expecting
- HYPERLINKS: misspellings in the link; hyperlinks asking you to take action; when you hover your cursor over the link, and the link address is for a different website

Remember to: STOP, LOOK, and THINK before you click.

Malware

July 5, 2023

Malware, or malicious software, is a blanket term for any kind of software created to cause harm. Hackers create it to make money, steal data, spy, blackmail, or even prank. It is a serious crime. The most common way to spread malware is through email (SPAM/phishing).

According to the SonicWall Cyber Threat Report, education is the number one target industry for malware attacks (2022) – this is up from number three (2021). The top 5 target industries (1-5) are: Education, Healthcare, Finance, Retail, and Government.

4 Common Types of Malware

Malware is categorized by how it spreads or what it does. Below are 4 common types:

- Trojan – tricks users into installing malware by posing as a valid program
- Virus – inserts hacker's own code in other programs
- Spyware – allows access to user's keystrokes, passwords and other sensitive information
- Ransomware – encrypts important files on user's computer and requires user to pay to decrypt

Fun Fact

The first virus, Creeper (named after a Scooby-Doo cartoon character) was created in 1971, by programmer Bob Thomas. This was as an experimental computer program – not harmful – and displayed the message, "I'm the creeper: catch me if you can".

New Threat

Credential harvesting, or password harvesting, is one of the newest threats. Hackers use a tool to collect (harvest) usernames and passwords (credentials).

A common source of credential harvesting is phishing emails. Other avenues include: malware viruses, cloned website links, the use of unsecure third-party vendors, and ransomware.

How it Works

1. **Hacker sends a phishing email.**
   The hacker takes great care to create a phishing email that seems real, even adding logos and important titles. The subject seems applicable to the reader. Fear is used as a

motivator – with subjects such as unpaid parking ticket, past due invoice, etc.
2. **You are encouraged to click on a link and perform a task.**
   You are encouraged to act quickly, and click on a link to resolve the issue.
3. **Link takes you to a web page.**
   Along with an elaborate phishing email, the hacker also makes a replica of a real website that looks legitimate. What appears to be a valid site is actually the hacker's server. The server detects and captures any secure information you type into the password fields.
4. **You are tricked into entering your email address and password.**
   You see a short message and are encouraged to sign-in, using your cloud-based company email and password.
5. **Hacker retrieves the password from their server.**
   The information you entered goes straight to the hacker.
6. **Hacker exploits harvested credentials.**
   Once the hacker has the credentials, they may be used in a number of ways – carry out more attacks, take over bank accounts or employer files, or sold on the dark web.

In the News

In early June 2023, Stephen F. Austin (SFA) State University was hit by a cyberattack. This attack is at least the 12th confirmed in Texas since March 2022, according to Comparitech.

Other recent cyberattacks, in Texas, include: The City of Dallas, Mansfield Independent School District, Rice University, the City of Tomball and the Dallas Central Appraisal District. Follow this link to view the full article from The Daily Sentinel.

With so many attacks, Highlanders must stay vigilant.

How to Prevent

STOP, LOOK and THINK, before you click.

Remember the PHISHING red flags we mentioned in the April IT Cybersecurity Newsletter:

- **FROM:** an email from an unknown sender; or, you know the sender, but the email looks funny
- **TO:** you were copied on an email, and you do not know the other individuals in the email
- **DATE:** you receive an email you would normally receive during business hours, but it was sent at 3am
- **SUBJECT:** the subject line does not make sense or does not match the message content; the email is about something you never requested, or a receipt for something you never purchased
- **CONTENT:** the sender is asking you to click on a link to open an attachment; you have an uncomfortable feeling, or it seems odd
- **ATTACHMENT:** any attachment you receive and were not expecting
- **HYPERLINKS:** misspellings in the link, hyperlinks asking you to take-action; you hover your cursor over the link, and the link address is for a different website

Ransomware. Game Over.

August 2, 2023

Ransomware is a type of malware attack (harmful software) that converts (encrypts) a victim's data to code and prevents access until a ransom payment is made. Ransomware attackers often use techniques, such as phishing, to gain access to a victim or company's files and data.

Rise of Ransomware Attacks

As technology evolves, ransomware attacks are growing among businesses and consumers. In 2022, the United States (U.S.) saw the highest number of ransomware attacks. The U.S. came in first with 217,486,516 attacks. In comparison, the United Kingdom was second with 71,350,221 attacks (2023 SonicWall Cyber Threat Report).

Over the last few years, colleges and universities are increasingly being targeted. These attacks take down key systems, close schools for days, and prevent faculty/staff from accessing lesson plans and student data.

As digital citizens (anyone who uses computers, the internet, and digital devices), it is important to be aware and vigilant about basic, best practices in an increasingly connected world.

Most Common Types of Attacks

Crypto Ransomware or Encryptors

Encryptors is the most well-known and damaging attack. Files and data are encrypted within a system, making the content inaccessible without a decryption key.

Lockers

Lockers completely lock you out of your system making files and applications inaccessible. A lock screen displays the ransom demand, possibly with a countdown clock, to increase urgency and drive victims to act.

Scareware

Scareware is fake software which claims to have detected a virus, or other issue, on your computer and directs you to pay to resolve the problem. Some types of scareware lock the computer, while others simply flood the screen with pop-up alerts, without actually damaging files.

Doxware or Leakware

Leakware threatens to distribute sensitive, personal, or company information online. Many victim's panic and pay the ransom to prevent private data from falling into the wrong hands or entering the public domain.

One form of attack is police-themed ransomware. The attacker claims to be law enforcement and warns illegal online activity has been detected. To avoid jail time, you may pay a fine.

Ransomware as a Service (Raas)

Raas refers to malware hosted anonymously by a "professional" hacker. They handle all aspects of the attack: distributing ransomware, collecting payments, and restoring access. In return, they receive a portion of the payment.

Major Keys to Ransomware Protection

Back-Up your Files

Ransomware will look for files to encrypt or delete. Ensure all files are backed up to a secondary location such as a secure, cloud storage service or another storage media. This protection can make files inaccessible to edits or deletion by cybercriminals.

Only Use Secure Networks

Cybercriminals look for individuals connected to unsecured Wi-Fi networks to track their internet usage. Using a verified and secure network will help add a layer of protection.

Keep Security Software Up-to-Date

Outdated security software is an easy target for cybercriminals trying to infiltrate systems. Software updates are recommended to protect against new cyber threats.

Never Pay Ransom!

Cybercriminals are always trying to deceive and take advantage of individuals. If you suspect you have fallen victim to a ransomware attack, make sure to disconnect any devices from your network and contact our IT team immediately.

Remember: Stop. Think. Connect.

Spear Phishing vs Phishing: What's the Difference?

May 3, 2023

What is spear phishing?

Phishing is a generic, broad attack addressed to hundreds or thousands of recipients. In comparison, spear phishing is a targeted, personalized attack addressed to specific individuals. The goal is to gain confidential information for fraudulent purposes.

How does it work?

The attacker will identify and research their target to craft a highly personalized email and convince the victim to share data. The victim opens the email, containing malware, and the attacker now has access to steal data.

New Trend

A new trend, as mentioned in Futurism | Science and Technology News article is the usage and abuse of language processing tools, by cybercriminals. They use something like ChatGPT, which is driven by AI (Artificial Intelligence) and makes it easier to personalize spear-phishing emails. Often times, scam emails are easily identified with bad grammar errors or misspellings. Using AI changes that.

Spear phishing requires much time to plan, research and gather details about a target. AI could possibly automate this process completely, making this method more attractive to use. Criminals only need to scroll your social media, input the information into the GPT (Generative Pre-trained Transformer) which creates a highly-believable tailored email. The complexity of emails generated, by AI, even has the ability to bypass SPAM networks (such as our Barracuda).

How to Spot a Spear Phishing Attempt

Spot the sender – carefully review the sending email

Peruse the subject line – watch out for emails striking a sense of urgency

Examine links or attachments – be on the lookout for forms requesting sensitive information

Assess the content – personal information may be found online through public records/social media

Request confirmation – if something still does not seem right, do not reply, send a new email to the address you have on file to confirm

Stay Safe for the Holidays

November 9, 2023

The holidays are right around the corner. This is a prime time for holiday shopping scams and cyber threats. Bad people use this opportunity to take advantage of the holiday giving season – remain vigilant and take precautions. Don’t let a cybercriminal ruin your holiday!

Safe Social Media Posting

Posting photos and status updates over the holidays can be a simple and fun way to stay connected with your loved ones. While we may enjoy sharing photos of our winter getaway and gifts, it’s important to remember the content of these online posts could be dangerous in the wrong hands.

Avoid geotagging your location.

Many social media apps prompt users to add a location to their posts or to “check-in”. For public, social media profiles, this information can act as a potential treasure map for burglars. This data can be used to pinpoint the general area of your home.

Geotagging can become especially dangerous when your location check-ins suddenly move from your neighborhood to a tropical beach resort – indicating to thieves you are out of town and your house is likely empty.

Be sure to deactivate the geolocation feature on all your mobile devices. Even if you do not manually check-in to locations, an enabled location setting could still reveal where you are posting.

Never reveal your address.

Avoid posting photos of your neighborhood and the exterior of your house. These posts could reveal your home address to criminals who know where to look. If you do share, make sure no identification markers such as street signs, house numbers, unique decorations or architectural elements are present in the photo.

Wait until you are home to post vacation photos.

Resisting the urge to share photos of you living it up on your winter getaway can be difficult. Yet, any photos of you enjoying the white sand and blue skies of a beachfront resort are a clear sign to burglars your house is empty. Unplug, enjoy your vacation and save the photo sharing for when you return home.

Refrain from showing off your valuables.

It can be fun to show off your shiny new gifts to friends and family. Remember, sharing photos of your valuables online could make your home a potential break-in target for thieves.

Double check your privacy settings.

A best practice you should follow throughout the year is to regularly comb through your friends and followers lists to delete, or limit the viewing settings, of any connections you do not completely trust. Several social media platforms provide you with options to limit your posts' exposure to different groups.

Safe Online Holiday Shopping

Holiday shopping will soon be in full swing. Online shopping is often the most convenient way to buy for everyone on your list. Be sure to follow these tips to ensure your holiday is Merry and Bright!

Keep an eye on your bank statements.

Pay close attention to your financial records, such as bank statements and credit card transactions. Flag any suspicious activity (charges you do not recognize or did not make) and contact the institution immediately.

Know how much items cost.

When shopping online, have a general sense of how much the items you want to buy should cost. This will help you get an idea if an online store has prices too good to be true. In these cases, you may pay less, but what's the cost? You may receive an item not matching the description, a counterfeit item or not receive anything at all! A little bit of research can help protect you.

Remember the 4 key behaviors from Cybersecurity Awareness Month:

- Protect each account with a **unique, complex password** (at least 12 characters long) – and use a **password manager**
- Use **multifactor authentication** (MFA) for any account that allows it
- Turn on **automatic software updates,** or install updates as soon as they are available
- Know how to **identify phishing attempts,** and **report** phishing messages

Do not use public Wi-Fi (wireless network) for shopping.

Public Wi-Fi is convenient and sometimes necessary to use. However, public Wi-Fi is not very secure – you should never shop online or access important accounts (banking) while connected to public Wi-Fi. Do your online shopping at home. If you must buy a few gifts online, while away from your home, use a VPN (virtual private network) or mobile hotspot.

Happy Holidays!

This is the last MCC Cybersecurity newsletter for 2023. Due to the MCC winter break, there will not be a newsletter for December 2023. Have a safe and happy holiday season, and see you next year!