2024 Newsletters

- 2024 Year in Review
- CrowdStrike Incident
- CyberSafe Holidays
- Cybersecurity Newsletter
- Hello Spring: Tidy up Tech
- Help us Secure our World
- Identity Management Day
- IT Exception Request
- Online Romance & Dating Scams
- Scam Alert: AT & T Data Breach
- Splash into Summer Safely
- Welcome Back to Campus: Tech Tips
- World Password Day

2024 Year in Review

December 4, 2024

Cybersecurity awareness continues to be an important issue at McLennan Community College (MCC). We receive phishing scams on a daily basis and rely on you, our customers, to help us identify and quickly address these threats.

Last month, ISS received a targeted phishing attack (spear phishing) requesting payment for an invoice. Ellucian is a legitimate vendor invoice for ISS. At first glance, the invoice appeared to be legitimate. The scammer clearly did their research – the template, colors, logo, etc. all seem to be correct. Let’s take a closer look.

1. Bill To

Accounts Payable is on the real invoice, but the fake invoice lists Mario Leal, Chief Information Technology Officer.

Invoice_Bill To

2. Customer PO Number

The Customer PO Number is on the real invoice but is missing from the fake invoice.

Invoice_Customer PO

3. Remittance Information

Ellucian, the vendor, is on the real invoice, but the fake invoice only has a statement to encourage electronic payment.

Invoice_Remittance

4. ACH Information

Bank of America is on the real invoice and Community Federal Savings is on the fake invoice. The email address is also different on the fake invoice – it is missing the ‘-info’, at the beginning of the correct email address.

Invoice_ACH_Info
Image not found or type unknown

Phishing attacks are not always obvious, with misspellings; it can be the subtle differences. Remember to **STOP, LOOK,** and **THINK**, before you click!

As we close out 2024, let’s take a look back at the highlights.

What did we learn?

We covered various, Cybersecurity newsletter topics, over the past year:

- Online Romance & Dating Scams
- Tidy up Tech – Spring Cleaning Tips
- Identity Management Day
- World Password Day
- Scam Alert: AT&T Data Breach
- Summer Safety
- IT Exception Request
- CrowdStrike Incident
- Cybersecurity Awareness
- Help Us Secure Our World
- Cybersafe Holidays

Cybersecurity Awareness Month (CAM)

October is National Cybersecurity Awareness Month, and 2024 was the second annual celebration for MCC. This year we collaborated with several departments/individuals across campus: Dr. Jeremy McCormick, Program Director of Computer Information Systems (CIS), Student Life, MARCOM, the MCC Library, and Jean Nixon, Sr. Lab Instructor. We held 3 different events:

- 10/02 – Have I been pwned?
- 10/16 – Learning Commons Workshop: Stay Safe Online
- 10/30 – Can you spot the phishing email?

On average, our event participation increased, from 2023 to 2024, by 400%! Thank you to everyone who came out to make this such a successful event!

Cybersecurity Awareness Training

Education is one (1) of the top five (5) target industries for cybersecurity attacks. As a Texas state agency, MCC is also required to conduct cybersecurity training on an annual basis.

Annual training, through KnowBe4, began on October 1st to be completed by October 31st. As of December 3rd, our completion percentages are as follows:

Training Completion Percentages

Cybersecurity awareness training completion percentages

Training Status	Employees (faculty & staff	Board of Trustees (BOT)
Complete	86%	100%
Past Due (incomplete or in progress)	14%	0%

Human Resources (HR) Onboarding: Cybersecurity

In July 2024, we worked with HR to implement a Cybersecurity section in HR onboarding, for all new employees. In November 2024, we expanded our session to also include Cybersecurity Awareness Training (via KnowBe4).

That’s our year in review. Thank you for all of your continued support. We wish you a joyful holiday season and look forward to what the new year will bring in 2025!

CrowdStrike Incident

August 7, 2024

On Friday, July 19, 2024, the world experienced the largest global IT outage in history – 8.5 million Windows devices encountered an error screen known as the “blue screen of death”. This affected companies ranging from banks to airlines to hospitals. What happened? Let’s examine to see what we can learn.

Who is CrowdStrike

At the heart of the outage is a cybersecurity vendor called CrowdStrike. They develop software to help companies detect and block hacks. CrowdStrike is known as an “endpoint” security firm – they remotely connect to their client’s laptops or mobile devices (endpoint) to apply cyber protections. Many companies use and install their software on their machines, across their organization.

What happened?

Before updates are applied, best practice is to perform a patch “sandbox test”. This is where an update is applied in a safe, environment to observe, analyze and ensure everything still functions as expected. If all goes well, then proceed with applying the update to production. CrowdStrike skipped the patch testing step and applied the full update in production.

Their software requires deep access to a computer operating systems (OS) to scan for threats. In this case, machine’s running Microsoft’s Windows OS crashed due to an issue in the way a software update issued by CrowdStrike, interacted with Windows. Because of their cybersecurity footprint, once the update was applied, this caused a global outage.

What can we learn?

This event is an opportunity to reflect on what organizations should be doing to improve resilience. McLennan Community College (MCC) has plans to review these areas, as part of our Cybersecurity Roadmap.

Response

This event demonstrates the need for every organization to have a robust incident response plan in place – a set of instructions on how to respond and recover systems in this type of incident. Organizations should evaluate the effectiveness of their response plans to determine any gaps.

Plans should be reviewed regularly and tested to minimize the impact to recover quickly.

Business Contingency Plan (BCP)

After an incident such as this, many organizations engage in implementing business continuity plans (BCPs) – help organizations recover and restore mission-critical functions in events. Organizations frequently experience challenges in this area during a ransomware event, with no plan to rebuild the resources to support mission-critical functions. To prepare, organizations should conduct a business impact analysis (BIA) and integrate the information into BCPs, reducing the risk of prolonged business disruption.

Single Point of Failure (SPOF)

CrowdStrike was the single point of failure (SPOF) in this incident – a design flaw in the system, that poses potential risk. SPOF could lead to a situation where just one error or malfunction causes the whole system to stop working. To avoid this, ideally, if a system fails, another should be in place to immediately take its place – adding redundancy (duplicate system). A redundancy should exist anywhere a SPOF currently exists.

Software Supply Chain

The scale of this event has highlighted the risks of cyber events affecting supply chains more than any event in recent history. With financial transactions stalled and hospitals unable to provide care, we cannot blindly accept updates from software impacting key systems. Organizations should consider and plan for incidents like this and have negative consequences on their supply chains as part of their BCP.

For organizations lucky enough to avoid any adverse impact from this event, it's crucial to recognize this could have happened to any organization just as easily. It is better to be prepared than to be lucky.

CyberSafe Holidays

November 6, 2024

The holiday season is generally a time to relax and reconnect with family and friends.

Cybercriminals also love the holiday season – they see it as the perfect time to take advantage of you, and attacks skyrocket. Phishing for example, increases by more than 150 percent (above average) according to Barracuda.

During the holiday season, it is important to be extra vigilant when shopping, giving, or booking travel plans. Don’t let cybercriminals steal your holiday fun! Keep the following in mind to better protect your personal information.

Shopping Online

- **Use secure Wi-Fi.** Using free Wi-Fi to shop online, at your favorite coffee shop is convenient but is not cybersafe. Use a VPN (virtual private network) or your phone as a hotspot to shop.
- **Lock down your login.** Create a long and unique passphrase for all your accounts, and use multi-factor authentication (MFA) when possible.
- **Resist the urge.** Be wary of offers too good to be true – no matter how tempting. Only buy from trusted and established online retailers.
- **Think before you click.** Pay attention to emails you receive. Don’t open emails from unknown senders or click on links in suspicious messages.
- **Shop securely.** Make sure you are shopping on a protected site (using SSL – secure sockets layer). This encrypts the data between a website and a browser. The easiest way to know is to look at the URL in the browser’s address bar – look for an **s** in **https** (http is not secure).
- **Pay wisely.** Use a credit card or pre-paid debit card, instead of a debit card linked to your bank account. Or, use a reliable, established third-party payment service (e.g. Google or Apply Pay).
- **Monitor your accounts.** Check your online financial accounts regularly for suspicious spending. Take advantage of text and email alerting services many banks and credit card companies offer.

Giving Online

- **Do your research.** Never feel pressure to give on the spot. Visit the IRS website to learn what types of organizations can get tax-deductible donations. Learn about charities and

how they spend the money they receive.

- **Ignore unsolicited requests.** Be wary of emails and phone calls asking for donations, especially organizations unfamiliar to you. Instead, visit their website directly or call to donate.
- **Think before you pay.** Never wire money or send cash. Pay by credit card; or, if donating online, make sure the website is secure by looking for the **https** at the beginning of the URL.
- **Double check the website.** Check the URL carefully – cybercriminals often create fake websites very similar to the real organization. Check the spelling of the organization's name for discrepancies.

Traveling

- **Disable auto-connect on your devices.** If your mobile phone or tablet automatically connect to wireless networks or Bluetooth devices, disable those features. When you want to connect, do so manually.
- **Secure your device.** Keep track of your laptop, smartphone, tablet, and even accessories, such as USB (universal serial bus) drives.
- **Avoid shared computers.** If using computers at hotel business centers or other places, with shared systems, avoid making purchases or logging into email. You do not know if the systems are up to date with the latest security software or if the machines are safe.

MCC Cyber Team Wins 1st Place

We would also like congratulate the MCC Cyber Team for winning 1st place in the Cybersecurity Interdisciplinary Incident Response Competition (CIIRC)! MCC competed against Baylor University (2nd place) and Texas A&M University (3rd place) at the Cyber Range, as part of the Central Texas Cyber Initiative (CTCI).

CIIRC was a three-day, student competition to simulate real world events occurring in business. The competition scenario simulated a business environment suffering cyber-attacks. Teams had to identify and analyze the attacks, determine and address recovery, public consequences, financial ramifications, engage in a press conference, report to the U.S. Securities and Exchange Commission (SEC) according to regulations, and many other related activities.

In the debrief, the Baylor staff administering the competition offered many complementary remarks about the MCC team and were very impressed with their performance. This demonstrates the caliber of our students, faculty, and administration. This is an example of who we send out into the world.

Cybersecurity Newsletter

September 4, 2024

Cybersecurity Awareness Month is an international initiative, celebrated each October, to highlight actions everyone can take to stay safe online. McLennan Community College (MCC) is proud to be a Champion and support this initiative.

Theme: Secure Our World

The theme for Cybersecurity Awareness Month 2024 is “Secure Our World”. Launched in 2023, Secure Our World empowers everyone to understand the simple ways to protect yourself, your family and your business from online threats.

We are increasingly connected through digital tools and more of our sensitive information is online. This convenience comes with risks. Each of us has a part to play in keeping ourselves an:

- Use Strong Passwords and a Password Manager
- Turn on Multifactor Authentication (when possible)
- Update your Software
- Recognize and Report Phishing

Fast Facts

According to the National Cybersecurity Alliance 2023 Oh Behave! Report:

- **84%** of people considered **online safety a priority.**
- Only **38%** of people **use unique passwords** for all their accounts.
- About **1/3** of respondents **began using** a **password manager** after receiving cyber training.
- **79%** of respondents were **familiar** with **Multifactor authentication (MFA)**.
  - **70%** of those, know how to use MFA.
- Only **36%** of people always **install software updates** when they become available.
- **69%** of people express **confidence** in their ability to **identify phishing**
  - **51%** of Americans actively **report Cybercrime**, particularly instances of **phishing**

MCC October Events

In celebration of Cybersecurity Awareness Month, MCC will be collaborating with different departments to host events around campus. We will have free giveaways and security tips to stay

safe online. Come join us!

MCC Events

MCC Events

Date	Time	Location	Audience	Topic
Wednesday, 10/2/24	11 am - 1pm	Table outside, Student Life	Students/ Faculty/Staff	Have I been pwned?
Wednesday, 10/16/24	12:15 - 1:30 pm	Learning Commons Workshop, LTC 318 or Zoom: https://mclennan.zoom.us/j/2549998332	Students/ Faculty/Staff	Stay Safe Online
Wednesday, 10/30/24	11 am - 1pm	Table Outside Student Life	Students/ Faculty/Staff	Can you spot the phishing email?

October 1 – 31, 2024– visit the MCC Library to see the CS display or do a CS theme crossword puzzle or word search.

Reminder: Faculty & Staff

- MCC will conduct CS training, at some point during the month of October. Be on the lookout!
- Before purchasing any software, please check with ISS to make sure it is safe and compatible.

Hello Spring: Tidy up Tech

March 13, 2024

Spring is not only a good time to clear out the dust and clutter in your closets and home, it’s also a good time to tidy up your digital stuff.

A messy digital life makes personal information and data vulnerable to bad actors. Here are some tips on how to clean and organize your devices and the information they store.

Clean Up Your Passwords and Find a Password Manager

Chances are you have some old, unsecure passwords needing to be cleaned up, or you are using the same password for multiple accounts. If the idea of going through every website you use seems overwhelming, use a password manager. Most smartphones (iOS, Android) have a built-in password manager, as do several web browsers.

Password managers not only store passwords and suggest strong ones; but the best options, alert you if you are using a duplicate or weak password, and prompt you to change it. This is a great way to toss out unsecure passwords and replace them with fresh, strong ones.

Delete of Cancel Unused Accounts

You may be surprised how many online accounts you have and do not use. Reduce the number of places and ways you may be at risk by deleting unnecessary account clutter. Think of it as clearing out a junk drawer of gadgets you forgot you had.

Look through your bookmarks. Critically review the sites and services associated with them. If you have not used an account in some time, log in one last time, remove all personal info, and deactivate it.

Unfortunately, major breaches happen regularly, and you may not be aware a site you used has been hit. Meanwhile, your name, password, and info associated with that account (such as your credit card) are in the hands of hackers. Limit your exposure. Close those old accounts.

Unsubscribe and Archive Email

Remember those unopened emails, lurking in your inbox? Unsubscribe or opt-out of lists no longer serving your interests. Be sure to empty the trash folder and archive any emails in your inbox you do not need but want to store for future access. Evaluate your email folders and filters and decide whether they are sorting messages in a way that works for you, or if you need to update.

Delete Old Photos You Don't Need

Photos. Estimates show the number of photos taken globally, in 2023, was around 1.6 Trillion (Rise Above Research). Photos and videos are the most common culprit, taking up storage space on your device.

Instead of letting them sit there, make something special with them. Create an album, wall handing, or pop them into a digital picture frame for your kitchen or living room. Although, it can be difficult to delete all those cute photos of your dog, start small. Delete old screenshots, duplicate videos, and blurry photos to help free up space.

Delete Old Apps You Don't Need

The most surefire way to declutter your device is to remove apps you no longer use. Apps can take up a wide range of space in your device's internal storage. Some apps, such as online games, can take up to 1 GB of storage space.

Before you delete an old app, be sure to close the account, associated with the data. Delete the username and password as well. This ensures the data, associated with the app, is taken out of circulation.

Once the account is closed, then delete the app. Follow the same procedure for computers and laptops, as they too may have account data stored elsewhere other than on your device.

Update Your Computer and Mobile Device Software

Microsoft, Apple, and Google release new versions of their operating systems every one to two months. These updates not only provide critical security patches but can also improve your device’s functionality by increasing speed and providing new features.

Software updates should not be ignored as they usually include important security improvements to protect your devices against the latest cybercriminal tactics. Step away from the ‘remind me later’ button and update your software.

Securely Dispose of Old Device

Don’t throw your old electronics in the trash. Not only is it bad for the environment, it also contains old data and personal information. It is not enough to just delete your data. You must wipe it from your devices. To do this:

- Perform a factory reset on your phone or other devices (where applicable).
- Remove any memory cards or hard drives.
- Consider using a disk cleaning software on your computer.

Once you have wiped your old device, take it to an e-waste recycling location to securely dispose.

Help us Secure our World

October 2, 2024

Cybersecurity Awareness Month highlights the growing importance of cybersecurity in our daily lives. This initiative reminds us there are simple actions we can take every day to protect ourselves, our families, and businesses from online threats.

The theme of Cybersecurity Awareness Month is *Secure Our World* and focuses on the top four ways to stay safe online:

1. Use Strong Passwords and a Password Manager
2. Turn on Multifactor Authentication (when possible)
3. Update your Software
4. Recognize and Report Phishing

Cybersecurity Awareness Month continues to build momentum and impact with the goal of providing everyone with the information they need to stay safe and more secure online. McLennan Community College (MCC) is proud to support this critically important online safety awareness and education initiative, this October.

Cybersecurity Awareness Month is led by the Cybersecurity and Infrastructure Agency (CISA) and the National Cybersecurity Alliance. For more information about ways to keep you and your family safe online visit CISA: Cybersecurity Awareness Month and Stay Safe Online: Cybersecurity Awareness Month.

MCC October Events

In celebration of Cybersecurity Awareness Month, MCC will be collaborating with different departments to host events around campus. We will have free giveaways and security tips to stay safe online. Come join us!!

MCC Events

MCC Events

Date	Time	Location	Audience	Topic
Wednesday, 10/2/24	11 am - 1pm	Table outside, Student Life	Students/ Faculty/Staff	Have I been pwned?

Date	Time	Location	Audience	Topic
Wednesday, 10/16/24	12:15 - 1:30 pm	Learning Commons Workshop, LTC 318 or Zoom: https://mclennan.zoom.us/j/2549998332	Students/ Faculty/Staff	Stay Safe Online
Wednesday, 10/30/24	11 am - 1pm	Table Outside Student Life	Students/ Faculty/Staff	Can you spot the phishing email?

October 1 – 31, 2024– visit the MCC Library to see the CS display or do a CS theme crossword puzzle or word search.

Identity Management Day

April 3, 2024

Identity (ID) Management Day aims to inform about the dangers of improperly managing and securing digital identities, by raising awareness, sharing best practices, and inspiring individuals and organizations to act.

Established in 2021, in partnership with the National Cybersecurity Alliance (NCA), ID Management Day is a day to educate business leaders, IT decision makers, and the general public about the importance of identity management. It is celebrated annually on the second Tuesday of April, which is April 9 th for 2024.

What is ID Management?

ID Management is the organizational process to ensure individuals have the appropriate access to technology resources. It involves a careful review of each user's role and responsibilities.

Only the necessary rights and resources should be assigned to each user. These privileges should be periodically reviewed and adjusted as needed.

Why is it important?

Cybersecurity incidents involving compromised identities continue to be the most common cause of a data breach for businesses, and account takeover for individuals.

- 84% of organizations suffered an identity-related breach and 78% experienced direct business impacts (Identity Defined Security Alliance).
- Account takeover attacks increased by 354% year-over-year in 2023 (Sift’s Q3 2023 Digital Trust & Safety Index).

Principles of ID Management

Below are six key principles to ensure ID Management systems are efficient and secure.

Principle of Least Privilege (PoLP)

Gives users the least amount of privileges necessary to perform their job functions. This minimizes exposure to sensitive information and reduces the risk of data breaches. Only the necessary rights and resources should be assigned to each user.

Role-Based Access

Manages access to resources based on the roles of individual users, within an organization. Instead of assigning permissions to individual users, permissions are assigned to roles, and users are assigned to these roles. This streamlines the administration of access rights and ensures users only have access to the resources they need for their roles.

Zero Trust

Assumes nothing inside or outside an organization can be trusted by default. This means continually verifying every access request to ensure it is fully authenticated and authorized before access is granted. Trust must be earned, not assumed, and it must be re-earned with each new access request.

Single Sign-on

Allows users to log in once and gain access to multiple applications or systems without needing to log in again. This not only enhances user convenience but also reduces the risk of password-related security breaches.

Multi-Factor Authentication (MFA)

Requires more than one method of authentication, from independent categories of credentials, to verify the user’s identity. These methods could be something the user knows (like a password) or something the user has (like a fingerprint).

MFA adds an extra layer of security and makes it harder for unauthorized users to gain access. Even if a bad actor manages to acquire a user’s password, they would also need the additional factor(s) to access the system.

Password Policies

Rules designed to enhance security by encouraging users to create reliable, secure passwords, and use them properly. These policies may require users to change their passwords regularly, avoid using easily guessable passwords, and use a mix of characters in their passwords.

McLennan Community College (MCC) continues to improve cybersecurity across campus. We will continue to educate and communicate as we progress in these areas.

IT Exception Request

July 3, 2024

Over the past several months, McLennan Community College (MCC) has expanded our Cybersecurity footprint.

ISS focused on Security Awareness to help you understand the important role you play in keeping our campus safe. There's now a whole suite of webpages to educate you about keeping you, your family, and our community safe. We completed a project to implement a logging and auditing tool (Splunk) to help us quickly detect and eliminate potential Cybersecurity threats. ISS also implemented our Information Security Controls Catalog.

New Cybersecurity Manager

Our latest news is the hiring of the new Cybersecurity & Online Technologies Manager: John Segovia! John has a wealth of Cybersecurity knowledge, and we look forward to the contributions he will make as he leads and expands our Cybersecurity efforts. John will begin sending these newsletters next month.

What is an IT exception request?

Our controls are in place to secure our systems. Sometimes systems may have a valid reason for not meeting one or more of these standards. For these situations, we created an IT exception request, to help document and mitigate the risk. This is similar to requesting an "exception to the rule".

When do I submit an exception?

Any exception to these security controls, or IT policy, must be requested by a current MCC employee and approved by Cybersecurity.

Examples of possible requests:

- Administrator rights
- Use out-of-date software
- Use out-of-date operating systems (e.g. Windows 7, instead of Windows 11)
- Unblock certain websites/countries from the firewall

Request an Exception

To request an exception, complete the IT Exception Request (via Softdocs Etrieve). You will need to supply the following information:

- Detailed description of the specific exception request
- Business justification, or why you need the exception
- Business impact, if the exception is denied

The exception request will be reviewed by Cybersecurity. You will be notified if your request is approved/denied or requires additional information to decide.

Term of Approved Exception

Approved exceptions will be valid for a period of time, as determined by Cybersecurity.

Appeal of Denied Exception

Should your request be denied, and you wish to appeal, work with your supervisor to appeal with the Chief Information & Technology Officer (CITO), Mario Leal.

We understand this is a learning process for everyone. If you are unsure if you need an exception, please feel free to ask us. We are happy to work through your concerns, with you.

Online Romance & Dating Scams

February 7, 2024

It’s February and Valentine’s Day is right around the corner.

Almost a third of Americans said they used an online dating service or app according to a recent Pew survey [1], and 10% of people in a relationship said that they met their partner online. These stats are even higher for younger people.

Unfortunately, though, all this online romance creates opportunities for scammers. Ick!

What is a Romance Scam?

Romance scams (also called sweetheart scams), refers to scams involving online dating.

Essentially, a bad actor creates a fake online profile, fires up the charm, and attempts to stir up romantic feelings in potential victims—especially students. After some not-so-innocent flirtation, eventually, the scammer asks for money.

Pay Attention to Red Flags

Romance scammers try to be as convincing as possible, which can now include using artificial intelligence-powered deep-fake video or audio technology. Still, many cybercriminals follow a similar scam pattern. Look out for some red flags when cybersurfing for love. The person:

- Requests money for urgent matters, such as medical expenses or a plane ticket to see you. Never send money to someone you haven't met in person.
- Requests hard-to-track forms of payment, like pre-loaded gift cards.
- Claims to live far away from you, often in a foreign country. They might also say they are in the military and serving overseas.
- Breaks promises to see you in person.
- Wants to push the conversation from the dating app to other messaging platforms like WhatsApp, Signal, or Telegram.
- The relationship feels like it is moving very fast.

Break up with Scammers

If you suspect you or a loved one are the victim of a romance scam, take action:

- Immediately stop communicating with the scammer.
- Not any identifiable information you may have on them, such as their email address or phone number. Take screenshots and write down any contact information.
- Contact your bank or credit card company if you've been scammed out of money.
- File a report with Campus Police.
- Report the scam to the FTC (Federal Trade Commission) and the FBI (Federal Bureau of Investigation) Internet Crime Complaint Center (IC3).
- Alert the website, platform, or app where you met the scammer. They might have more information on the scammer that can help investigators.

Did You Know?

Americans reported losing a heartbreaking **$1.3 billion** to romance scams in 2022, according to the Federal Trade Commission [2], and the number is likely higher due to underreporting.

Safeguard Your Heart (and Wallet) From Scammers

By adopting a few privacy habits, you can limit what scammers can learn about you.

Share with Care

Think before posting about yourself and others on social media or online dating services. Consider what a post reveals and who can see it.

Check Your Settings

Consider setting your social media profiles to “private”. This makes it harder for scammers to target and communicate with you.

Think Before You Click

Be wary of messages that push you for immediate action or ask for personal information.

This is a red flag for phishing. Never share personal info via email or text if you do not know the sender.

Use Reverse Image Search

Do a reverse image search of the flirty account’s profile picture.

You may see that image belongs to a completely different person, or has been affiliated with different online identities. If this is the case, there is a high chance the person behind the fake profile picture is trying to scam you.

Scam Alert: AT & T Data Breach

May 22, 2024

McLennan Community College (MCC) received reports of a text message scam, appearing to be from Mario Leal, Chief Information Technology Officer (CITO).

The text message targets employees and asks you to confirm if you received the message. An example has been provided below.

Sample Fraudulent Text

Hello [employee name], please give me a quick response when you get this message. Thanks

Mario Leal

Chief Information & Technology Officer

McLennan Community College

If you respond to the initial text, you may receive the following message:

I'm in a meeting right now, I have a task that I want you to handle for me right now. Are you available?

AT&T Data Breach

AT&T announced 73 million current and former customers had their personal information stolen in an AT&T data breach. Account data includes: customer's full name, email address, mailing address, phone number, social Security number, date of birth and AT&T account number and passcode.

The breach appears to be from 2019 or earlier. AT&T is unsure if the information came from AT&T or one of its vendors. The data leak first came to light in 2021, as hackers claimed they had stolen customer data and would put the information up for sale. In March 2024, the stolen personal information was discovered on the dark web, according to the creator of Have I Been Pwned.

If you are an AT&T customer and worried about your data, see What is AT&T doing for the 73 million accounts breached?

Scam Text Messages & Phishing

Data breaches, such as AT&T, puts individual's information out, open to the public. Scammers use this information to create phishing (scam) emails or smishing (scam) texts.

Many users are aware of the dangers of responding to suspicious emails. With text messages, users let their guard down and usually respond more quickly. Here are a few signs of smishing texts:

- Tone of the message conveys a sense of urgency
- Strange or abrupt business request
- Phone number is spoofed - looks like it is coming from someone you know or trust
- Claims to be from a colleague, family member or friend, but does not sound like them

Remember to protect your identity and Recognize Phishing.

What to do now?

If you receive this or a similar scam, **DO NOT** respond or click on any links. You may contact Tech Support if you have any questions or need to report an issue.

Splash into Summer Safely

June 5, 2024

Temperatures are heating up, and it’s time for a little fun in the sun! Vacations are a great opportunity to relax, reconnect and embark on new adventures. Before you depart, add a simple cybersecurity checklist, along with your packing routine.

Fake Reviews

Did you know scammers can buy fake online reviews? Scams for hotels, Airbnb’s, rental cars and special activities, at your destination, has become common practice.

Look out for nearly identical reviews under different customer personas, or seek out reviews from external third parties, such as the Better Business Bureau (BBB).

Apps & Official Websites Only

Once you finalize your travel plans, you expect to receive email confirmations and updates from airlines and hotels. Hackers know this and craft phishing emails to target you.

To avoid this, install official apps or use the official website for travel alerts. Remember, a web address with “https://” (WITH an s) means the site takes extra security measures. However, an “http://” (withOUT an s) address is not secure.

Travel Light & Protect Physical Devices

Limit the number of devices you take to help limit your risk. Ensure your devices and chargers are with you at all times, while traveling. If you must leave items in your hotel, lock them in a safe or in your luggage. Never leave your devices unattended in public places or with a stranger. Not only can they be physically stolen, but a thief could also access your personal information.

Check Privacy & Location Settings

Review your privacy, security and location tracking settings on web services and apps. Consider limiting how and with whom you share information. Location tools come in handy while navigating a new city, but they can also expose your location – even through photos and social media. Turn off location services when not in use.

Update Software & Backup Files

Ensure everything is up-to-date on the devices you plan to take. Updates often include important security patches to protect you from the latest threats. Cybercriminals are always on the lookout for weaknesses in outdated software, to exploit and gain unauthorized access. Keep devices updated, during your travels, by turning on “automatic updates”.

Back up the data, on your devices, to an external hard drive or a cloud service. If your device is lost or stolen, and you cannot access, you will not lose all of your information. Regular backups also protect you from data loss, due to device failures or malware infections.

Setup the 'Find my Device/Phone' Feature

Not only does this feature allow you to locate your phone, it gives you the power to remotely wipe data or disable the device if is gets into the wrong hands.

Secure Home Network

While on vacation, consider turning off your router, unless you need it for smart home devices. An idle router can be an easy target for cybercriminals.

By turning it off, you are eliminating a potential entry point for hackers who might try to compromise your home network. If you need to keep it on, ensure it is secured with a strong, unique password and the firmware is up-to-date.

Stop Auto Connecting

Some devices will automatically seek and connect to available wireless (Wi-Fi) networks and Bluetooth. Bluetooth enables your device to connect wirelessly with other devices, such as headphones or automobile infotainment (in-car entertainment) systems.

These features can provide cybercriminals access to your devices. Disable these features so you only connect to Wi-Fi and Bluetooth when you want. If you do not need them, switch them off.

Avoid Public Computers

Avoid public computers in hotel lobbies and internet cafes. If you must use, clear the cache and browsing history, and delete all the temporary files from the computer. Keep your activities generic or go incognito (private browsing).

Avoid making online purchases or accessing your accounts on public computers. If you do log into accounts, never allow the browser to remember your ID and password. When you are finished, logout. Simply closing the browser does not log you out of accounts.

Financial Protection

Use a credit card instead of a debit card, for added financial protection. Notify your financial institutions of your travel dates and only shop and bank on familiar, secure sites.

Remember cybersecurity is a journey, not a destination. Stay vigilant, follow these tips, and you will be well on your way to a safer, more secure summer vacation. Safe travels!

Welcome Back to Campus: Tech Tips

January 2, 2024

Welcome back to campus!

Returning after a long break may not be easy and getting back to your routine may feel difficult. We want to make sure you know what steps to take and who to contact if you run into any Tech Support issues.

Tech Assistance

Below are some reminders, tips and links to resolve common issues. If you need technical assistance, you may request this support by calling: **MCC Help Desk** at **254-299-8077/ext 8077** or visiting the Tech Support webpage to create a ticket.

Prioritization

Volume will be heightened with everyone slowly returning back to campus. Student-facing service requests and classroom preparation requests will be prioritized first. All other faculty/staff requests will be processed in the order they are received.

Account Reminders

Account Locked

- Try the 'Unlock Account' (IT Resources & Services page) - this may only be completed every 24 hours.

Change My Password Button Not Working

- Delete the MCC password reset email, close your browser (or restart your device) – then ‘try to Unlock Account’ (IT Resources & Services page).

Password Reset Email Incorrect

- Contact the Help Desk.

Brightspace Reminders

New Student Access

- Must wait 24 hours AFTER registration, for access to be available.

Courses

- May take up to 24 hours, AFTER registration, to show in Brightspace.
- Only courses, for the CURRENT semester, will be available in Brightspace

Future Courses/Semester

- Will NOT be available until 1-2 days prior to the class start date.

Technical Support

Excluding login issues, contact Brightspace 24/7:

- Call: 1-877-325-7778
- Tech or Chat Support: https://community.brightspace.com/support/s/contactsupport

MyMCC Reminders

Account Disabled

- Too many login attempts, contact the Help Desk for assistance.

Login Issues

- Try resetting your MCC password.

Passwords

- Special characters are not supported - ONLY use numbers and letters.

Office/Extension # Changes

- Faculty/Staff - submit the change via MyMCC to ensure the Online Directory is updated and applicable individuals are notified.

Classroom Technology Tips

Audio Not Working

- Verify 'MUTE' is off on touch panel
- On podium computer, click the speaker icon to see playback device selected
  - Verify 'ExtronScalerD' is selected
  - If not selected, click the arrow next to the device and select
  - If 'ExtronScaleD' not listed, restart the podium computer - follow the steps to select

Image Not Displaying on Podium Computer

- Verify the monitor is on - press the 'Power' button (bottom, right-hand side of the screen)

Image Displaying on Projector Screen but NOT on Monitor

- Press Windows Key (Windows logo) + P
- Release the keys once the side menu appears - select 'Duplicate'

Projector Not Displaying Podium Computer Screen

- Select 'On' from the touch panel, then select PC
- On podium computer, press Windows key (Windows logo) + P
- Release the keys once the side menu appears - select 'Duplicate'
- Issue not resolved?
  - Right-click empty area of the desktop and select 'Display Settings'
  - Under 'Multiple displays' (at the bottom), click the drop-down and select 'Duplicate these displays'

Additional Helpful Links

- Request MCC Tech Support: Create Help Desk Ticket
- IT Resources & Services: Current Students, Faculty & Staff
- IT Resources & Services: Faculty & Staff

World Password Day

May 1, 2024

World Password Day is observed annually, on the first Thursday in May. The goal is to raise awareness about the need to take better care of our passwords and develop better password habits.

History of World Password Day

Prior to technological advances, passwords were uncommon and mostly used by secret societies. Below is a brief history of how World Password Day was created:

- **1961**–Massachusetts Institute of Technology (MIT) creates the computer password so multiple people can use a shared computer system.
- **1976**–public-key cryptography (encrypts data with two different keys: public and private) is created so two people can authenticate (validate) each other without exchanging a cryptographic key.
- **1978**–researchers publish the first study of its kind, which demonstrates that guessing passwords, based on a person's identity, is easier than cracking passwords with computers.
- **1986**–two-factor authentication emerges and is adopted.
- **2013**–World Password Day is created.

Risk of Weak Passwords

Passwords provide an added layer of security, making it more difficult for unauthorized individuals to access our data. Weak passwords put our personal information at risk. A weak password can be easily guessed or cracked by attackers. This can lead to identity theft, financial loss, and other serious consequences.

Cybercriminals use brute force (automation and scripts) to try and guess passwords. The more complex the password, the odds of a brute force attack decrease significantly. Check the chart to see how long it would take to crack your password.

Time to Crack Password

Time to Crack Password

Number of Characters in Password	Numbers Only	Lowercase Letters	Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters & Special Characters
4-6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 second	2 seconds	4 seconds
8	Instantly	Instantly	28 seconds	2 minutes	5 minutes
9	Instantly	3 seconds	24 minutes	2 hours	6 hours
10	Instantly	1 minute	21 hours	5 days	2 weeks
11	Instantly	32 minutes	1 month	10 months	3 years
12	1 second	14 hours	6 years	53 years	226 years

NordPass – password manager – conducted research on password habits, over the past few years. They created a list of the Top 200 Most Common Passwords. Open the link, and scroll to the bottom to view the list.

The default filter is All Countries, or you may select a specific country. The information is listed by: rank, password, time to crack, and count (number of times used).

Tips to Create Passwords

Follow these best practices when creating passwords:

1. **Strong**– at least 12 characters long
2. **Complex**– combination of upper-/lower-case letters, numbers, and special characters (when possible)
3. **Unique**– never reuse, none of your passwords should look alike – e.g. changing 1 character or add a 3 at the end
4. **Multi-Factor Authentication (MFA)**– enable (when possible) – requires you to enter your username and password, then prove your identity – e.g. responding to an email/text

Password Trends for 2024 and Beyond

As technology changes and bad actors develop increasingly sophisticated means of attack, best practices around passwords and protecting accounts may change too.

Password-less authentication, such as biometric identifiers (i.e. fingerprint) and single sign-on (SSO), are becoming more popular. For now, passwords are the most common way to secure accounts and prevent unauthorized access. As with physical valuables, we must ensure our digital valuables are secure.