

# IT Cybersecurity Newsletters

Monthly newsletters, from previous years, are available to stay informed and up-to-date on various security topics.

- [2025 Newsletters](#)
  - [Fraudulent Applications & Sensitive Information](#)
  - [SPAM & Maintenance Plan \(TLDR\)](#)
  - [Welcome Back](#)
- [2024 Newsletters](#)
  - [2024 Year in Review](#)
  - [CrowdStrike Incident](#)
  - [CyberSafe Holidays](#)
  - [Cybersecurity Awareness](#)
  - [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](#)
- [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](#)

# 2025 Newsletters

# Fraudulent Applications & Sensitive Information

## February 5, 2025

### Fraudulent Applications

A perfect storm of circumstances has led to a significant increase in fraudulent applications, in higher education, from so called “ghost students” or “Pell runners”. Community colleges have been particularly vulnerable – scammers apply for federal and state financial aid, pocket the funds and vanish without ever attending classes.

With the pandemic of 2020, institutions saw the prevalence of online scams. There was a shift from in-person to online and hybrid learning as well as the rise of AI (artificial intelligence) technology. This shift also made it difficult for professors to confirm the actual attendance rates of their students.

### How it Works

Ghost students are not real students. They are created by scammers often using stolen identities, social security numbers (SSN) and fabricated academic records to generate fictitious student profiles and apply for enrollment. Scammers employ bots or automated systems to submit multiple applications quickly, often targeting community colleges and online programs where admissions barriers are lower.

Upon acceptance, “students” apply for aid through FASFA (Free Application for Federal Student Aid) and stay in class until the census date, doing the bare minimum to remain registered, even using AI to generate essays, and avoid being dropped from a class for non-participation. Once the financial aid is disbursed, the “student” withdraws the funds and vanishes. Pell Grants, which do not require repayment, are a common target because they are ideal for immediate financial gain.

With acceptance, they also gain access to other institution provided resources, such as: cloud storage or VPN and student (.edu) email addresses to help them carry out other potential scams.

### Operational Impact

According to [Cybersecurity Ventures](#), global cybercrime costs are projected to skyrocket from \$9.5 trillion USD in 2024 to \$10.5 trillion by 2025. In 2024, several high-profile data breaches (e.g. AT&T, U.S. government agencies and universities and Bank of America) compromised organizations across various sectors. These breaches contributed to billions of people’s data being published on the dark web for ghost students to use.

Since 2010, community colleges and higher education institutions have flagged an estimated 20% to 36% of their student populations as potentially fraudulent. This practice has cost educational institutions millions and has prevented legitimate students from accessing online courses. In California, the problem has become so prevalent the U.S. Department of Education has been looking into the matter, with 48 investigations currently in progress.

## Key Indicators of Fraudulent Financial Aid Applications:

- Unusual patterns in address or email usage
- Sudden surges in applications
- Inconsistent borrowing amounts
- High withdrawal rates among students with Parent PLUS Loans (PSL)
- Suspicious FAFSA submissions
- Multiple student refunds going to the same account
- Discrepancies between reported income and loan amounts
- Clean ISIR (Institutional Student Information Record) records despite fraudulent documents
- Varying levels of student engagement based on fraudulent rings
- Registration for classes without prerequisites
- Forged Document Submission
- Identification of copied or pasted content within the application
- Identification of multiple applications originating from the same IP (Internet Protocol) address

The ongoing fight against fraud requires continuous modernization and vigilance, ensuring opportunities meant to help students are not exploited by bad actors. The complexities of shifting between in-person, virtual and hybrid learning have been met with an increasingly complicated and evolving cyber threat landscape where colleges have become primary targets of cyber threat actors.

Combating fraud is best accomplished through meaningful cybersecurity investment. The stakes are too high to ignore, and the tools to address these challenges are readily available. By prioritizing software such as: multi-factor authentication (MFA), biometrics and other types of identity security tools, institutions can ensure they remain a place of integrity and excellence in education.

## Reminder: Emailing Sensitive Information & Documents

We have noticed an increase in emails, with attachments requesting sensitive information, being blocked in Barracuda, McLennan Community College's (MCC) SPAM filter.

Barracuda is set up to filter incoming/outgoing emails to help protect MCC from potential harmful content, files, and data leakage. Sensitive information such as: social security numbers (SSN), W-2s, dates of birth (DOB), credit card numbers, bank account information, etc. will trigger a block if detected.

# SPAM & Maintenance Plan (TLDR)

## March 6, 2025

### TLDR (Too Long; Didn't Read)

The newsletters will now include a new section: TLDR (Too Long; Didn't Read). This will be a short summary of the newsletter, providing key points in a brief format for readers who may not have time to read the full article.

Key points:

- Add SPAM emails to [Barracuda SPAM filter](#) to [block on your own](#)
- Quarantined phishing emails in Barracuda do not need to be reported to the Help Desk
- To boost cybersecurity on campus, MCC will implement a regular [maintenance](#) plan

TLDR END

## SPAM

We often receive SPAM (unwanted email) daily. McLennan Community College (MCC) utilizes Barracuda to filter and block SPAM (or phishing) emails. Sometimes, SPAM still gets through. Did you know you are able to block SPAM on your own? For details on how to block, see: [IT Hub: Block SPAM](#) article.

## Quarantined Phishing Emails

Reporting phishing emails is important to help protect the MCC community from potential harmful content, files, and data leakage. Barracuda is set up to filter incoming/outgoing emails and block suspicious content.

Recently, a phishing email circulated appearing to be from the Chief of Human Resources (HR), Missy Kittner. Some individuals received the email in their inbox and reported the email as phishing to the Help Desk (thank you). Once the email was triggered as phishing, Barracuda began to block the additional emails as 'Quarantined'.

If a phishing email is quarantined, in Barracuda, you DO NOT need to deliver the email to your inbox to report as phishing to the Help Desk. In this case, Barracuda did its job. The Help Desk will work with the ISS team to purge all the phishing emails from everyone who received this email in their inbox.

# Maintenance Plan

MCC will soon implement a regular maintenance schedule for specific applications/systems used at the college. The schedule will be published on the MCC website: Information Systems and Services (ISS) under [Maintenance](#). Why are updates important? As mentioned in a [2023 Cybersecurity Awareness Month Newsletter](#), software updates are one of the easiest ways to boost cybersecurity.

Developers are constantly looking for clues cybercriminals are trying to break into their systems. To fix these issues and improve security, software companies release routine updates. These are important to protect against potential vulnerabilities and threats, ensure compliance and reduce legal risks, optimize performance, add new features and enhancements, address any bugs or errors, and prevent costly repairs by addressing issues before they escalate.

# Welcome Back

## January 8, 2025

Returning to campus after a long break can be difficult. We want to make sure you have what you need to hit the ground running!

Volume will be heightened with everyone slowly returning to campus. Our priority will be student-facing and classroom preparation requests. All other faculty/staff requests will be handled in the order they are received.

## Need Technical Assistance?

- **Create a ticket** – see [Tech Support](#)
- **Email** – [helpdesk@mclennan.edu](mailto:helpdesk@mclennan.edu)
- **Call** – 254-299-8077 or ext. 8077
- **Troubleshoot and find answers** (on your own) – see [IT Hub](#)

## Account Reminders

- **Account locked** – See [Account Locked](#) (IT Hub). This process may only be completed once every 24 hours.
- **'Change My Password' button not working** – Delete the MCC password reset email, close your browser (or restart your device), unlock your account, and then retry the password reset. See [Forgot Password](#) (IT Hub) for detailed instructions.
- **Password reset email incorrect** – Call the Help Desk at 254-299-8077.

## Brightspace Reminders

- **Course listings** may **not** be **available** until **3 days before** the semester's **start date**.
- **Login issues** – see [Tech Support](#).
- **All other technical support , contact Brightspace 24/7:**
  - Chat: On all Brightspace pages, you will find a blue button located on the lower, right side of the screen. The button will look like 2 chat boxes. This will allow you to chat with support or email them.
  - Call: 1-877-325-7778
  - Online Support: [Support Request Form](#)

## MyMCC Reminders



- **Account disabled** (due to too many login attempts) – see [Tech Support](#).
- **Login issues** – Try resetting your MCC password. Passwords with **special characters** are **not supported**, ONLY use numbers and letters in your new password.

## Classroom Technology Tips

- **Audio is not working**
  - Verify 'MUTE' is off on touch panel.
  - On the podium computer, click the speaker icon to see the playback device selected.
    - Verify 'ExtronScalerD' is selected.
    - If it is not selected, click the arrow next to the device and select it.
    - If 'ExtronScalerD' not listed, restart the podium computer and then follow the steps to select.
- **Image not displaying on podium computer**
  - Verify the monitor is on by pressing the 'Power' button (bottom, right-hand side of screen).
- **Image displaying on projector screen but NOT monitor**
  - Press Windows key (Window logo) + P.
  - Release the keys once the side menu appears and select 'Duplicate'.
- **Projector NOT displaying podium computer screen**
  - Select 'ON' from the touch panel and then select PC.
  - On podium computer, press Windows key (Window logo) + P.
  - Release the keys once the side menu appears and select 'Duplicate'.
  - Issue not resolved?
    - Right-click an empty area of the desktop and select 'Display Settings'.
    - Under 'Multiple displays' (at the bottom), click the drop-down and select 'Duplicate these displays'.

## Security Awareness

As an institution of higher education, we (students, faculty, and staff) are a top target for potential cybersecurity attacks. Data breaches can be costly and are often caused by human error.

Online safety is not only the responsibility of IT (ISS). Our goal is to empower you with safe computing practices and guides to help protect you, our data, and community.

We created a suite of security awareness information on our website, to provide you with the information you need. Various topics are listed under [Security Awareness](#). Check it out!

- [Cybersecurity Awareness](#) – annual training, latest security alerts, Central Texas Cyber Range (CTCR), and Cybersecurity Awareness Month (annually in October)
- [IT Cybersecurity News](#) – monthly newsletters on various topics
- [MCC Cybersecurity Incidents](#) – monthly stats for blocked emails, compromised accounts, phishing campaigns and victims

- [Protect College Data](#) – protect the workplace and remote work and travel
- [Protect Your Device](#) – protect desktops and laptops
- [Protect Your Identity](#) – protect your identity, top 5 and phishing scams

We look forward to the new year and a successful 2025!

# 2024 Newsletters

# 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.



---

**Bill To:**

McLennan Community College  
**Accounts Payable**  
1400 College Drive  
Waco, TX 76708  
USA

---

**Bill To:**

McLennan Community College  
**Mario Leal**  
1400 College Dr  
Waco, TX 76708-1402  
USA

### 2. Customer PO Number

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

SAP Order Number:	75503
Customer PO Number:	P0032642

SAP Order Number:	54554
-------------------	-------

### 3. Remittance Information

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

#### Remittance Information

Remit To:

Ellucian Company LLC  
62578 Collections Center Drive  
Chicago, IL 60693-0625  
USA

#### Remittance Information

**We encourage our customers to make payments electronically for convenience of both our customers and us.**

### 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.

#### ACH Information:

Bank of America  
100 West 32nd Street  
New York, NY 10001  
ABA# 071000039  
Beneficiary Name: Ellucian Company LLC  
Account # 81080-91099  
Email: electronic-payment-info@ellucian.com

#### ACH/WIRE Information:

Community Federal Savings Bank  
89-16 Jamaica Ave  
Woodhaven, NY 11421  
ACH/WIRE ABA# 026073150  
BIC/SWIFT: CMFGUS33  
Beneficiary Name: Ellucian Company L.P.  
Account # 8311955474  
Email: electronic-payments@ellucian.com  
**Please reference invoice number on all payment remittance.**

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 1<sup>st</sup> to be completed by October 31<sup>st</sup>. As of December 3<sup>rd</sup>, 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 1<sup>st</sup> Place

We would also like congratulate the MCC Cyber Team for winning 1<sup>st</sup> place in the [Cybersecurity Interdisciplinary Incident Response Competition \(CIIRC\)](#)! MCC competed against Baylor University (2<sup>nd</sup> place) and Texas A&M University (3<sup>rd</sup> 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 Awareness

## 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
<b>Wednesday, 10/2/24</b>	11 am - 1pm	Table outside, Student Life	Students/ Faculty/Staff	Have I been pwned?
<b>Wednesday, 10/16/24</b>	12:15 - 1:30 pm	Learning Commons Workshop, LTC 318 or Zoom: <a href="https://mclennan.zoom.us/j/2549998332">https://mclennan.zoom.us/j/2549998332</a>	Students/ Faculty/Staff	Stay Safe Online
<b>Wednesday, 10/30/24</b>	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 or 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 hanging, 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
<b>Wednesday, 10/16/24</b>	12:15 - 1:30 pm	Learning Commons Workshop, LTC 318 or Zoom: <a href="https://mclennan.zoom.us/j/2549998332">https://mclennan.zoom.us/j/2549998332</a>	Students/ Faculty/Staff	Stay Safe Online
<b>Wednesday, 10/30/24</b>	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<sup>th</sup> 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 <sup>1</sup>, 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 <sup>2</sup>, 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 it 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 'ExtronScalerD' 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.

# 2023 Newsletters

# 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 possibly 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](mailto: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
<b>Monday, 10/2/23</b>	1130am – 130pm	Table outside, MAC building	Students/faculty/staff	ISS – Cybersecurity Team
<b>Tuesday, 10/17/23</b>	12pm – 1pm	Presentation: Staying Safe Online, LTC 318	Students/faculty/staff	Jean Nixon, Academic Support & Tutoring
<b>Monday, 10/30/23</b>	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 manager 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 breach. 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 breach 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](mailto: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

**P**eruse the subject line – watch out for emails striking a sense of urgency

**E**xamine links or attachments – be on the lookout for forms requesting sensitive information

**A**ssess the content – personal information may be found online through public records/social media

**R**equest 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!