

2025 Newsletters

- [Fraudulent Applications & Sensitive Information](#)
- [SPAM & Maintenance Plan \(TLDR\)](#)
- [Welcome Back](#)

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
- **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!