ITS CORNER

ISSUE 05: BUILDING A SECURITY CULTURE AT OCCC

CONTENTS

01. Smart Cyber Habits
02. Why It Matters
03. What ITS Is Doing
04. Password Best Practices

CYBERSECURITY IS EVERYONE'S RESPONSIBILITY

This October, Cybersecurity Awareness Month reminds us that security is not just an IT task. **Everyone on campus plays a role.** Whether you are at home, on campus, or using your phone, good cyber habits help protect you and the OCCC community.

SMART CYBER HABITS

- **Use Strong, Unique Passwords**: A strong password is your first line of defense. Use a passphrase that is easy to remember but hard to guess. See the "Best Practices" section at the end of this newsletter!
- **Change Your Password Every 90 Days:** OCCC requires all users, including students, staff, and privileged accounts, to **update passwords every 90 days.** This ensures stolen or compromised passwords quickly lose their value.

Stay Up to Date: Install updates for your computer, phone, and apps. Updates fix security flaws before attackers can exploit them.

Be Careful on Public Wi-Fi: Avoid logging into sensitive sites on unsecured networks like coffee shop Wi-Fi.

Think Before You Click: Phishing is still the top cyber threat. Pause before opening unexpected emails, attachments, or links. If you receive a phishing email, use the reporting feature!

Back Up Your Data: Save important files in OneDrive, SharePoint, or another secure location. Backups protect against mistakes, malware, and hardware failures.

Change Passwords Every

90 DAYS

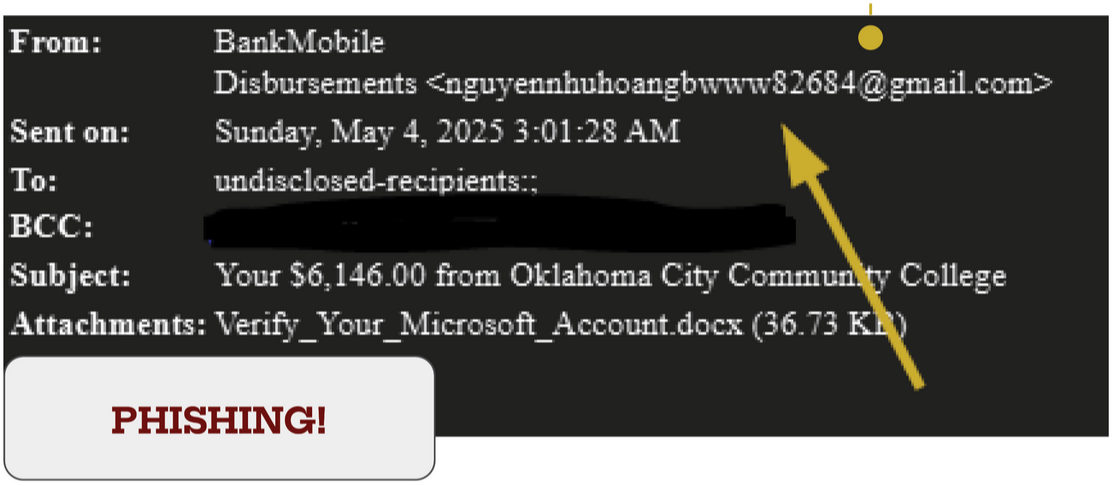
REAL THREATS

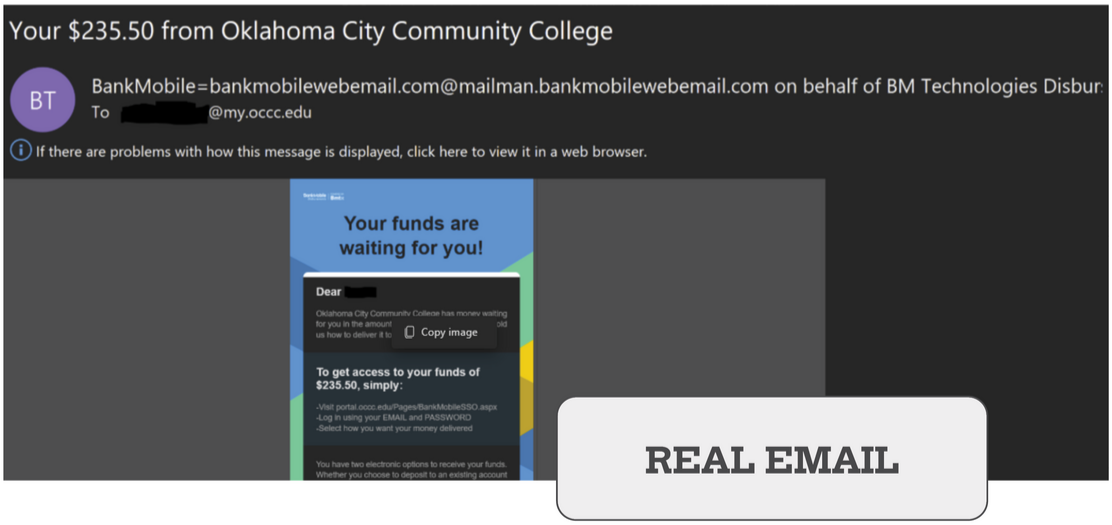
Below is a **REAL** phishing attempt sent to OCCC students. These cybercriminals were pretending to be from BankMobile. Review the photo below to see what they did!

Do NOT assume a suspect email is safe just because it is not listed here. There are many variants, and new ones are being sent out each day!

Remember to check the email! The gmail email address gives this scammer away.

The legitimate email BankMobile uses is **BankMobile@bankmobilewebemail.com**. Ensure to check the sender carefully!





NEVER reply or interact with the body of a phishing email. Instead, immediately report the email as phishing. Finally, if you accidentally click on anything in a suspected phishing email - reach out to the Help Desk immediately by submitting a Freshservice ticket or calling 405-682-7777!

WHY IT MATTERS

Ransomware Threats Are Increasing: Educational institutions have seen ransomware attempts rise 23% in 2025. Even a single encrypted system can halt operations.

Phishing Is the Leading Cyber Threat: Over 75% of targeted attacks start with email. Everyone is a potential target, including students, staff, and faculty.

Credential Theft Is Surging: Incidents have increased 160% this year, accounting for 20% of breaches.

AI-Driven Phishing: Up to 80% of phishing emails may be AI-generated in 2025. These are harder to detect and require extra vigilance.

New Campus Members Are Most Vulnerable: Individuals in their first three months on campus are 71% more likely to fall for scams. Early awareness is critical.

Training Reduces Risk: Regular password updates and cybersecurity awareness training can reduce phishing risks by up to 70%.

Example: A new student received an email appearing to be from the Bursar's office. By verifying it with ITS, they avoided sharing credentials and protected the campus community!

WHAT ITS IS DOING TO PROTECT YOU

1. Cisco Endpoint Security: Runs in the background on OCCC devices, blocking malware, ransomware, and fileless attacks in real time.

2. Cisco IronPort (Secure Email Gateway): Filters phishing, spam, and unsafe attachments before they ever reach your inbox.

3. Microsoft Entra Security: Protects OCCC accounts, including privileged ones, with multi-factor authentication (MFA) and password policies. Entra P2 adds intelligent risk monitoring and conditional access, automatically blocking suspicious sign-ins to keep your account and the campus safe.

4. Proactive Monitoring: ITS reviews alerts, investigates suspicious activity, and adjusts defenses to stay ahead of evolving threats.

Together, these layers form a defense-in-depth strategy that protects devices, email, and identities.

BEST PRACTICES WHEN CHANGING YOUR PASSWORD

- Use a passphrase at least 12-15 characters long with a mix of letters, numbers, and special characters. (E.g., C@mpus$unset2563!). (*Do not use this example password.)
- Don't reuse passwords across accounts.
- Never share your password with anyone.

Visit the ITS Help Desk in the Main Building (behind the coffee shop), call 405-682-7777 (Ext. 7777), or submit a Freshservice ticket. You can also find more resources and past ITS Corners at occc.edu/information-technology.

STAY ALERT. STAY SECURE. PROTECT OCCC.