ITS CORNER

ISSUE 01: BEWARE OF PHISHING ATTEMPTS!

In this first edition of our OCCC cybersecurity newsletter, we'll delve into one of the most prevalent and persistent threats in the digital realm: **phishing attempts**. Despite advancements in cybersecurity technology, phishing remains a top concern for individuals and organizations.

Phishing is a malicious tactic used by cybercriminals to deceive individuals into divulging sensitive information such as passwords, credit card numbers, or personal data. These attacks often come in the form of emails, text messages, or phone calls impersonating reputable entities like banks, government agencies, or familiar companies.

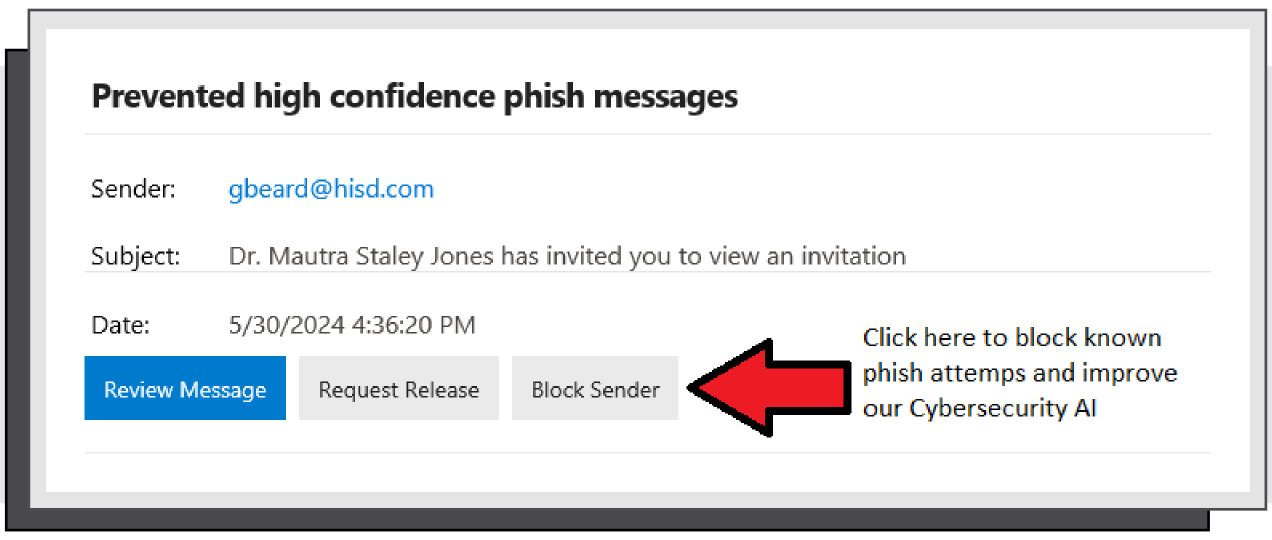
Types of Phishing Attacks

- **Spear Phishing** - This *highly-targeted* form of phishing involves tailoring messages to specific individuals or organizations, often using information gleaned from social media or data breaches to increase credibility and effectiveness
- **Impersonation Attacks** - Cybercriminals are increasingly impersonating trusted entities such as colleagues, vendors, or even friends in their phishing attempts, making it more challenging to discern the authenticity of messages.

> **Phishing is a malicious tactic used by cybercriminals to deceive individuals into divulging sensitive information.**

How Can You Protect Yourself Against Phishing?

1. **Think Before You Click:** Exercise caution when clicking on links or downloading attachments, especially if the sender is unfamiliar or the message seems suspicious.
2. **Verify the Source:** Before divulging any sensitive information, verify the legitimacy of the sender by contacting them directly through a trusted means of communication.
3. **Stay Informed:** Stay updated about the latest phishing trends and tactics by regularly educating yourself and your team through cybersecurity awareness training programs.
4. **Use Multi-Factor Authentication (MFA):** Implementing MFA adds an extra layer of security by requiring users to provide multiple forms of verification before accessing accounts or sensitive data.
5. **Keep Software Updated:** Ensure that your operating system, antivirus software, and applications are regularly updated with the latest security patches to mitigate vulnerabilities.



Prevented high confidence phish messages

Sender: gbeard@hisd.com

Subject: Dr. Mautra Staley Jones has invited you to view an invitation

Date: 5/30/2024 4:36:20 PM

Click here to block known phish attemps and improve our Cybersecurity AI

Though our ITS team blocks thousands of phishing attempts each day, the reality is that some sophisticated emails may still evade detection.

In such instances, it's **imperative** that every team member utilizes the block and reporting functions promptly.

Connect Your Issued Computer to the OCCC Network for Updates at Least Every 30 Days

Refresh your computer by plugging into the OCCC domain every 30 days. Refreshing your computer by restarting or updating its software helps clear temporary files, reset system processes, and install crucial updates. This enhances the overall speed and responsiveness of the system and ensures that it remains up-to-date with the latest security patches, protecting against potential cyber threats.

30

Got an IT Problem?

Your first stop is **The Helpdesk,** located on the first floor across from the Bursar's Office. Mr. Brian W. Fugett, the Director of Technology Support Services, leads a team of trained, on-demand IT professionals who can handle your IT needs.

Oklahoma City Community College