Staysafeonline.org

CYBERSECURITY AWARENESS MONTH

OCTOBER 2023

Dear Campus Community,

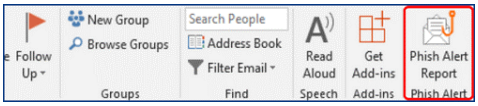
October marks the beginning of Cybersecurity Awareness Month, and as your Chief Information Officer, I want to share some crucial information to keep you safe online.

In today's digital world, threats to our personal and institutional information are ever-present. Cybercriminals use various tactics to deceive, manipulate, and exploit unsuspecting users. One of the most common techniques is phishing, where attackers send deceptive messages in an attempt to steal sensitive information.

Here are some tips to help you spot and avoid these phishing attempts:

- **Hover Before You Click:** Before clicking on any link in an email, hover over it with your mouse to see the actual URL. If it looks suspicious or doesn't match the sender's domain, it's best not to click.
- **Watch Out for Lookalike Domains**: Cybercriminals often use domains similar to genuine ones by missing a letter or changing characters, such as replacing an "I" with a "1". Always double-check the domain for subtle discrepancies.
- **Beware of Out-of-Character Messages:** If you receive an email asking you to perform actions that seem unusual or out of character for the sender, think twice before acting.
- **Sense of Urgency:** Be cautious of messages that create a sense of urgency or threaten negative consequences, like account expirations, lost access, or undelivered packages. Attackers use these tactics to induce hasty actions.
- **Know the Sender:** Even if an email appears to come from someone you know, it might not be genuine. Attackers often compromise accounts to target their connections or fake messages to seem like they're from a trusted source. This tactic, known as spoofing, can be particularly deceptive. Always verify any unusual requests, even if they seem to come from a familiar name.
- **Change of Venue:** Watch out for messages that ask you to change the mode of communication to text messages. These are almost always a scam. They often start with “are you free” and claim to be someone you know and ask to text them. Once they have you in text messages, its much easier to evade our technical defenses.

Should you encounter a suspicious link or suspect you've received a phishing email, please report it using Phish Alert Report button immediately.



You are both the first line of defense and the last. IT security isn't just a role for our department; it's a shared responsibility. Everyone plays a vital part in protecting GSU’s mission. Together, we can ensure our digital environments remain safe and secure.

Stay vigilant, stay informed, and remember - knowledge is our strongest asset in this fight.

Warm regards,
Jay Ellis
CIO

Grambling State University
Information Technology Center
Jacob T Stewart Hall |Room 139
403 Main Street |Box 4220 |Grambling, LA 71245
itc@gram.edu