IT'S CYBERSECURITY AWARENESS MONTH!

Updates from the Office of Internal Controls, Audit Compliance & Information Security (IAC/S)

Welcome to week 2 in Cybersecurity Awareness Month! This week we are focusing on Social Engineering.

WHAT IS SOCIAL ENGINEERING?

Social engineering is any manipulation technique that exploits human behavior and error in order to gain access to sensitive or confidential information. Where some scammers would steal someone's personal information, social engineers convince their victims to willingly hand over the requested information like usernames and passwords.

Social engineering attacks are generally not quick. Instead of a smash-and-grab robbery, social engineers tend to take a prolonged approach that starts with research.

How can you recognize it?

These are a few indicators that should raise a red flag:

- A message arrives unexpectedly either via email, text message, or phone call (robocall).
- The sender asks for something out of the ordinary such as an offer of money, or a request to do the following: send money, open a document, run an executable, or send information.
- The request is usually something that the (pretended) sender has never asked for before.
- The requested action is potentially harmful.
- The sender attaches an unusual file or url.

How can you protect yourself?

Check the validity of the source.
Pay close attention to the email header and check that it matches with previous emails from the same sender. Look out for spelling and grammar mistakes, as this is a common sign of a scam.

Regularly update and patch your operating system and applications to reduce the risk of known vulnerabilities.

Remain vigilant when contacted by third parties.
Keep in mind that reputable organizations will never ask users to share passwords or login credentials. Every conversation should begin with the agent asking you to verify your identity through a security question that you selected in the past.

Log in via your account or official website.
Accessing sites this way, rather than through embedded links or pop-up ads, is one way to ensure legitimacy.

What not to do

Do not respond to urgent requests.
Scammers will often instill a sense of immediacy to prompt action. Always say you need more time to get the information and then verify the request via another contact method.

Do not insert an unknown USB or other device into your computer.
If you find an unattended USB or other endpoint, hand it over to an IT professional or member of an information security team.

Do not allow another user to access your personal device or accounts.
Malware can be installed in a matter of seconds. Never share your devices with other users or allow friends or coworkers to use your device unsupervised.

Hopefully you now have a better understanding of Social Engineering. Remember, if you are in doubt whether something is legitimate don't be afraid to ask someone for help. It is always better to be cautious than to rush and make a mistake. We depend on you to make good decisions in helping us remain safe and secure.