tmasf™ connects
Commute • Career • Community

SUSPICIOUS CALLS, EMAILS, MESSAGES

Click Here to see our video interview with Centarus on the Suspicious Calls, Emails, and Messages.

Phishing has become the most common cybersecurity crime in the 21st century. General housekeeping rules to consider when you receive a suspicious call, email or message include:

- **Ask yourself:** Was this something I was expecting?
- **Analyze the message:** Is the email address/phone number legitimate? What is the context of the message? Is the grammar correct?
- **Stay extra cautious** about messages regarding password resets, or that include large attachments and external links

EMAIL MANAGEMENT

Email spam can be irritating, especially when you may have multiple email accounts. The *CAN-SPAM Act of 2003* was passed to enforce rules in commercial emails. The law gives all recipients the opportunity to unsubscribe and stop email spam. In addition to the law, there are anti-spam solutions to implement and diminish the number of emails being received.

EXFILTRATION PROTECTION

Your Managed Service Provider (MSP) or IT Service Provider can assist in determining system parameters in the form of *SPF* and *DKIM* records. These security tools prevent phishers from sending emails on your behalf.

Other ways to protect yourself include setting up a *Mobile Device Management* software and implementing *multi-factor authentication* on your accounts, to be covered in future topics.

DATA EXFILTRATION

Data exfiltration is the theft of data from any device, including personal and corporate computers and mobile devices, through cyberattacks. Common types of data exfiltration include:

- **Social engineering/phishing attacks:** This tactic uses deception and manipulation to trick victims into downloading malware and give up sensitive personal or account information. For more information on phishing, please refer to our *Phishing with Michael* series, where we interview a local jobseeker on his own experiences with suspicious employers and phishing scams.
- **Outbound Emails:** Cybercriminals use outbound email systems to infiltrate emails, databases, and attachments (calendars, images, and planning documents).
- **Downloads/Uploads:** This method involves data transfers from trusted, secure devices to insecure devices (like a communal, public device or a thumb drive)
- **Human Error:** When authorized users access services and systems without following proper procedures and procedural failures given that proper procedures were not in place