STUDY GUIDE FOR CYBER BINGO

PHISHING

DON’T' GET CAUGHT

WHAT IS PHISHING

Phishing scams are emails, texts, or phone calls that attempt to trick you into clicking a link, disclosing sensitive information, or downloading a virus. These scams are usually easy to detect for a variety of reasons, but they can also be extremely difficult to detect, leaving you vulnerable.

TYPES OF PHISHING ATTACKS

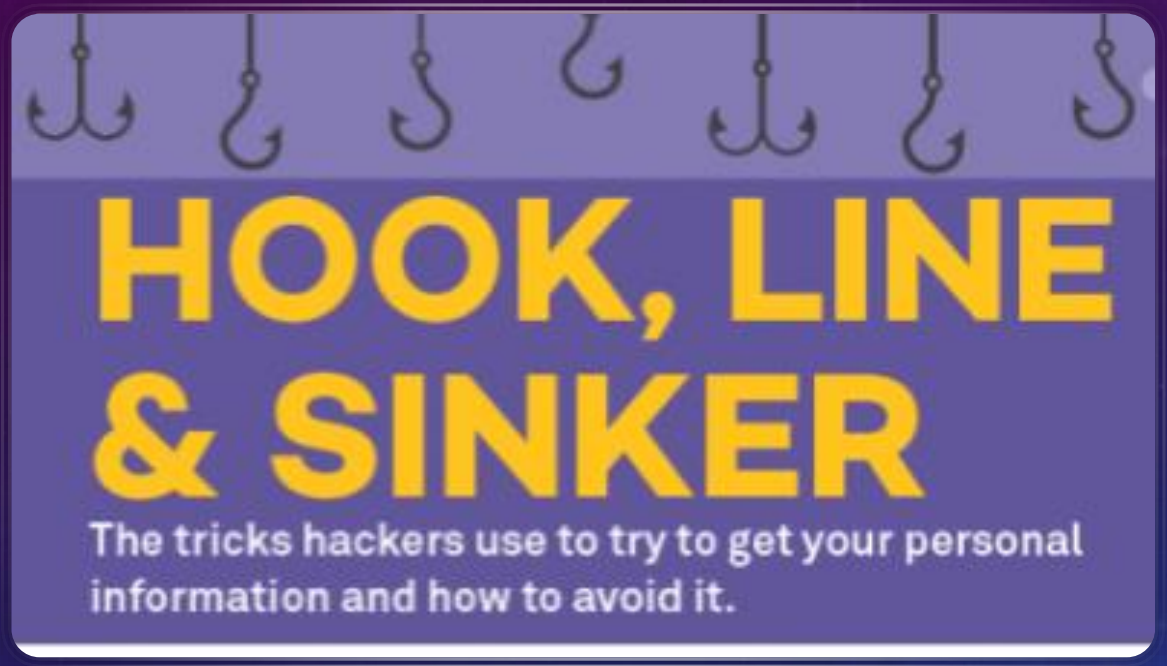
MASS-MARKET PHISHING	SPEAR PHISHING	WHALING
CLONE PHISHING	VISHING	SNOWSHOEING PHISHING

HOW DO I PROTECT MYSELF

•The best way to avoid phishing is to learn how to recognize it. You are less likely to fall victim to their tricks if you know what an untrustworthy email looks like.

•Look for four indicators of a phishing email:

- The email address
- A greeting or your name
- Syntax and grammar
- URL



MORE TIPS

- Before you click or enter sensitive information, always double-check the spelling of URLs in email links. Keep an eye out for URL redirects, which send you to a different website with the same design.
- If you receive an email from a known source that appears suspicious, send a new email to that source rather than simply replying.
- Don't share personal information on social media, such as your birthday, vacation plans, address, or phone number.
- If you believe you have received a phishing scam email, please contact your local IT Department; they are always eager to assist you and help prevent the spread of such email scams.

8 signs of a **Phishing Scam**

- Poor grammar, spelling mistakes & unprofessional language
- A generic greeting or no greeting at all
- Messages that push you to act urgently
- Requests for personal information e.g. PINs, passwords & login details
- Suspicious links - Hover over links to reveal misleading URLs
- Unsolicited attachments that often contain hidden malware
- Unofficial from address or phone number
- Promotional offers that sound too good to be true

REPORT PHISHING IMMEDIATELY.