PHISHING SCAMS

TIPS

DEFINITION

The practice of tricking Internet users (as through the use of deceptive email messages or websites) into revealing personal or confidential information which can then be used illicitly (Merriam-Webster).

THE BAIT

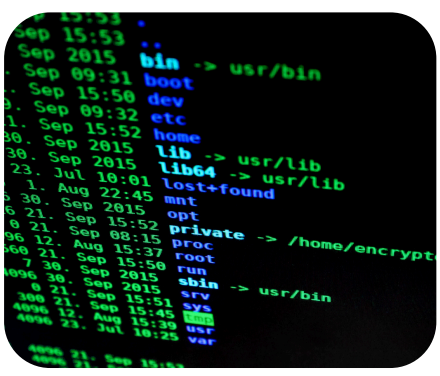
- Common tactics are things like fake emails, fictitious urgent messages, and “to good to be true” enticing offers.
- “Urgent Action Required: Account Suspension Notice”, “Claim Your Unclaimed Funds”, “Congratulations! You've Won a Prize!” from suspicious email address or with simple grammar and spelling errors are a tail-tell sign the email is a fake.

THE HOOK

- After taking the bait, the victims are met with legitimate looking login pages such as a Google sign in or a copy of their banks website.
- The fake login screens capture the victims log in credentials and are saved for future use by the phisherman.

THE CATCH

- After the login credentials are obtained the phisherman is then able to login and do whatever they please with your account.
- Phishing results in multiple different outcomes such as identity theft, financial loss, and malware infection.



FACTS

- 1 in 3 people are likely to click on a phishing email.
- There are other types like vishing (voice call phishing) and spear phishing (targeting a specific individual).
- The first phishing attack occurred in 1990's, targeting AOL users.