PHISHING ATTACKS AND SOCIAL ENGINEERING

BY LOGAN FERGUSON

WHAT IS A PHISHING ATTACK?

- Phishing is the technique of attempting to acquire sensitive user information through a fraudulent solicitation (NIST, 2021)
- The perpetrator disguises themself as a legitimate business or reputable person and makes a convincing offer
- Tricking individuals to reveal sensitive data such as bank accounts, social media login, social security, and IP addresses
- Phishing is a form of social engineering

TYPES OF PHISHING ATTACKS

- There are six common types of phishing attacks (Bisson, 2021)
  - Deceptive Phishing
  - Spear Phishing
  - Whaling
  - Vishing
  - Smishing
  - Pharming

DECEPTIVE PHISHING

- Email from a recognized sender containing malicious content
- Tricks humans by impersonating a legitimate corporation and uses a fake emergency to steal personal information (Bisson, 2021)
- Mass emails are sent out attempting to catch as much personal information as possible
- Hackers use many different techniques to evade the detection of their malicious content in emails

SPEAR PHISHING

- Hackers target one specific person at a time
- Email from a recognized sender containing personalized information to lure user into a trap (Bisson, 2021)
- Tends to be more successful than deceptive phishing
- Hackers will find information on their targets first using other social engineering techniques
- This kind of attack is most common on social media sites since they contain the most personalized information

WHALING

- Specifically targets business executives
- Used to steal login credentials and authorize falsified financial transactions and obtain W-2 information on the targeted businesses' employees
- Difficult to carry out, but the financial gains are vast
- Hackers can use a business email compromise (BEC) of the CEO's email account to authorize huge financial transfers and request employee W-2's to file fake tax returns for employees (Bisson, 2021)

VISHING

- All the previous attacks rely heavily on emails while vishing relies on phone calls
- Very effective because it gives the target a sense of ease being able to hear someone's voice
- Attackers will sometimes use a VoIP
- Usually to impersonate a known company and to collect bank and other sensitive information from targets (Bisson, 2021)

SMISHING

- Very similar to Vishing except it is done through SMS (text messages)
- Utilizes text messaging to trick targets into clicking on malicious links
- Attackers will include links in texts that trigger downloads of a trojan or virus, take the user to a credential-stealing form, or impersonate a customer service representative and ask the user to contact them (Bisson, 2021)
- Smart phones are very vulnerable to this kind of attack

PHARMING

- A very advanced form of a phishing attack
- Leverages DNS poisoning to redirect the target to a malicious site (Bisson, 2021)
- Antivirus software and many email filters are too advanced for hackers to use normal phishing attacks
- Changes (or poisons) a DNS's IP address, which will then locate and take a user to different website

HOW TO DEFEND AGAINST PHISHING ATTACKS

- Best way to defend a phishing attack is to be well educated on these attacks and how they are carried out (Albladi & Weir, 2020)
- Never open an unknown link, whether it's from an email, text, or sometimes even someone you know
- Never give your personal information to someone you do not know especially over the phone or through text messages
- Enable two-factor authentication on all your online accounts (Bisson, 2021)
- Use reputable antivirus software and keep it updated to help prevent all kinds of phishing scams (Touhid, 2019)

REFERENCES

- Albladi, S., & Weir, G. (2020, March 05). Predicting individuals' vulnerability to social engineering in social networks - cybersecurity. Retrieved February 28, 2022, from https://cybersecurity.springeropen.com/articles/10.1186/s42400-020-00047-5

- Bisson, D. (2021, October 13). 6 common phishing attacks and how to protect against them. Retrieved February 28, 2022, from https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and- how-to-protect-against-them/

- NIST. (2021). Phishing - glossary. Retrieved February 28, 2022, from https://csrc.nist.gov/glossary/term/phishing

- Touhid. (2019, August 25). What is the best defense against phishing attacks? Retrieved February 28, 2022, from https://cyberthreatportal.com/what-is-the-best-defense-against-phishing/