Huntington
Welcome.®

HUNTINGTON CYBER SMARTS

WHAT IS SOCIAL ENGINEERING?

Social Engineering is a popular and effective way for fraudsters to get your personal information. They use different forms of communication to get you to respond quickly, without considering that their intentions are malicious. Stay safer from social engineering with these tips below.

1 DON'T BE QUICK TO CLICK

Do you know 94% of malware is delivered by email?[†]

Fraudsters want you to open links in an email, text, or push notification. It may even be delivered like it was sent from a reliable source. Always read before you proceed.

SAFETY TIP

Check the email address against valid email addresses typically sent from that sender. If they don't match the text, the link may be a hoax.

2 CONSIDER THE SOURCE

Hackers attack every 39 seconds, on average 2,244 times a day.[‡]

Social Engineering relies on human nature to have you reveal personal information by trying to instill trust. Be suspicious if you don't know who is calling or emailing you.

SAFETY TIP

Find the customer service number of the organization the fraudster mentions and call to verify the source or their identity.

3 DON'T BE PHISHING BAIT

Phishing attacks account for more than 80% of reported security incidents.[§]

Be extra cautious. A new approach called 'spear phishing' is when an email is directed to one individual pretending to be another person – like your boss or IT professional.

SAFETY TIP

Use a good spam filter that can help detect suspicious files or links. It may already have a list of IP addresses or sender IDs that are fraudulent.

4 SAY NO TO QUID PRO QUO

In a recent study, participants were more likely to give their passwords to total strangers if they were given candy first.[¶]

Fraudsters will try to get your personal data by offering an incentive or using 'scareware.' They often say there's a security issue with your smartphone or device and to take immediate action.

SAFETY TIP

Social Engineering often uses urgency to catch you off guard. You can stop the threat by taking a moment to stop and think.

5 HAVE AN EYE FOR DETAILS

47% of employees who work from home cited distraction as the reason for falling for a phishing scam.[≠]

More than half of all emails are spam.[#] Social engineering attackers hope you're not looking for red flags in all those messages.

SAFETY TIP

Bad grammar, spelling errors, and an unfamiliar tone or greeting usually mean an email could be a phishing attack.

[†] Forbes, https://www.forbes.com/sites/joegray/2019/09/11/phishing-not-just-for-criminals/?sh=20e6345e24b3
[‡] Varonis, https://www.varonis.com/blog/cybersecurity-statistics/
[§] Varonis, https://www.varonis.com/blog/cybersecurity-statistics/
[¶] Science Daily, https://www.sciencedaily.com/releases/2016/05/160512085123.htm
[#] Symantec, https://docs.broadcom.com/doc/istr-23-2018-en
[≠] Tessian, https://ai4.io/wp-content/uploads/2020/07/Tessian-Research-The-Psychology-of-Human-Error.pdf