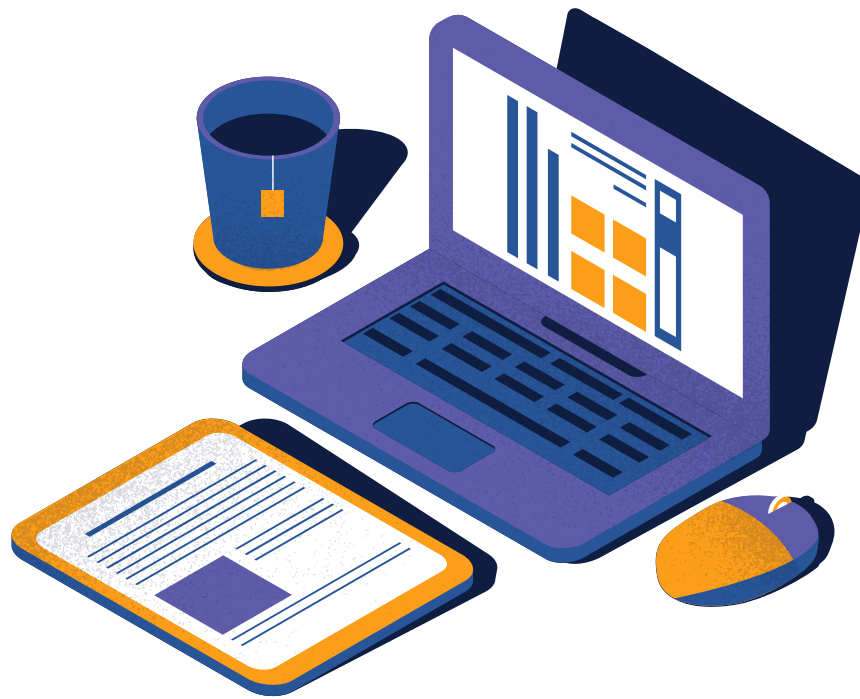




SOCIAL ENGINEERING

Social engineering refers to the tactic or way of manipulating or deceiving an internet user to gain access or control over a computer system, or to steal personal and financial information.



Common targets include ;

High-worth individuals, high-profile employees, and high-level leaders. Cyber criminals target people with high levels of access.

Popular online personalities. People who share more personal information online are more likely to be targets. If your spouse has 50k Instagram followers, they could be targets.

Younger generations and employees who are uninformed about cybersecurity threats. One study revealed that 45% of millennial employees don't know what phishing is.

Techniques used include;

Impersonation; This refers to an act of someone pretending to be another person for the purpose of entertainment or fraud.

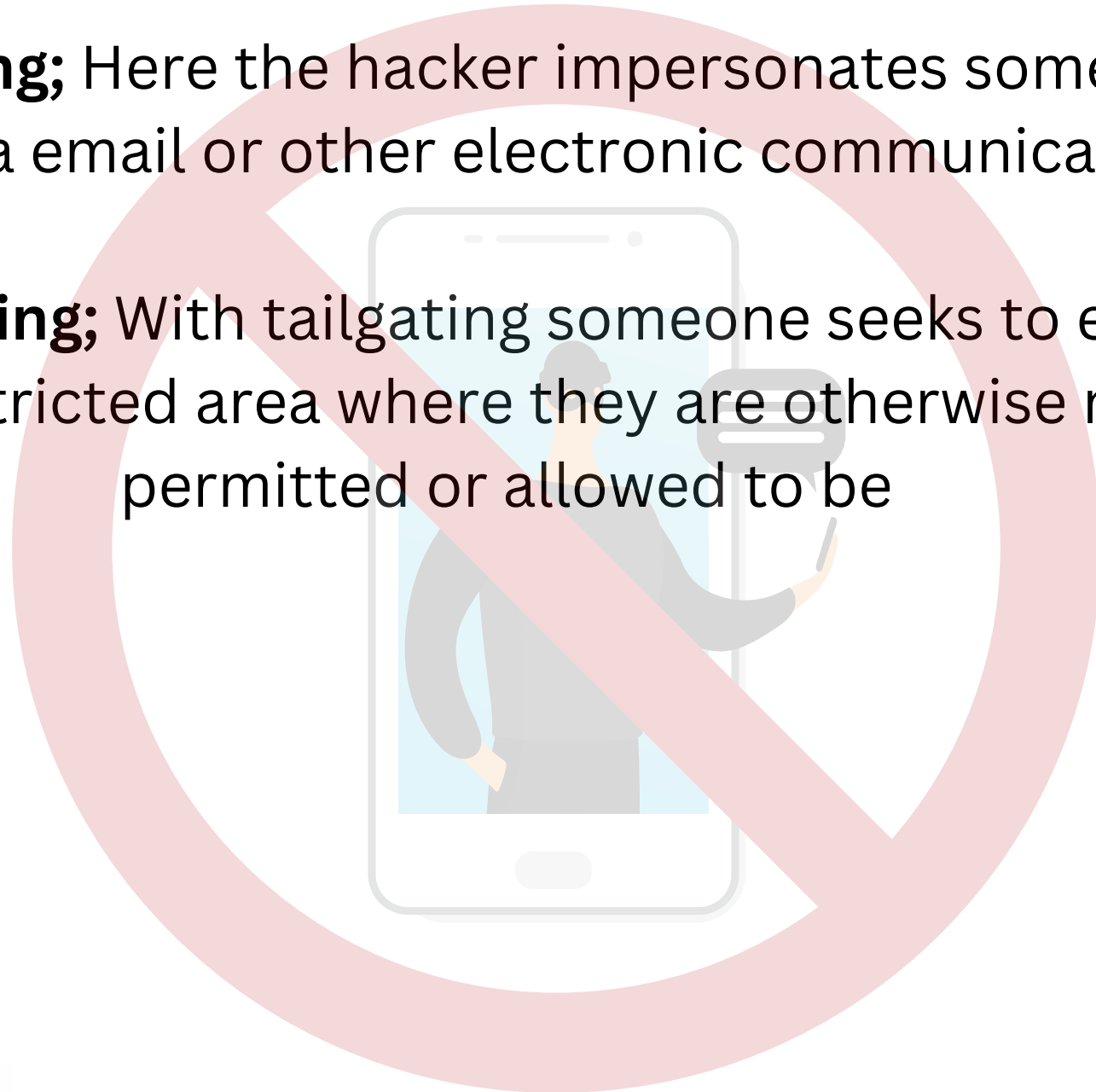
Pretexting; This refers to giving a specified reason as one's justification into sharing sensitive information.

Baiting; Here, the scammer uses false promise to lure a victim into a trap which may steal financial information or inflict the system with malware.

Techniques used include;

Phishing; Here the hacker impersonates someone else via email or other electronic communication.

Tailgating; With tailgating someone seeks to enter a restricted area where they are otherwise not permitted or allowed to be



How to protect yourself from social engineering attacks?

Shrink your online footprint. The less you share online and on social media, the harder it is for hackers to target you. Avoid posting personal information.

Install antivirus software. Ransomware, malware, and spyware exist at unprecedented levels today. Don't let these harmful applications wreak havoc on your privacy.

Regularly check your credit report and bank statements. Scammers are almost always after your financial accounts. Check for the warning signs of identity theft — such as strange charges on your bank statement or accounts you don't recognize.

Use a VPN when browsing and shopping online. VPN scrambles the data you send and makes your location untraceable.

Monitor the Dark Web for your exposed data. Hackers will often sell your personal data on the Dark Web.





Always use Two Factor Authentication (2FA). This is a second-layer of security on all your accounts.

So if a hacker tricks you into sending your password, they still need a special code that only you have to gain access to your accounts.

Consider signing up for identity theft protection.

top-rated identity theft protection monitors all of your most sensitive personal information, online accounts, and finances for signs of fraud.


THANK
you



PASSWORDS

Password Managers / Two
Factor Authentication





Password is a string of characters used to authenticate or verify the identity of a user.

It's used to protect sensitive information and prevent unauthorized access to person's digital accounts



STRONG PASSWORDS

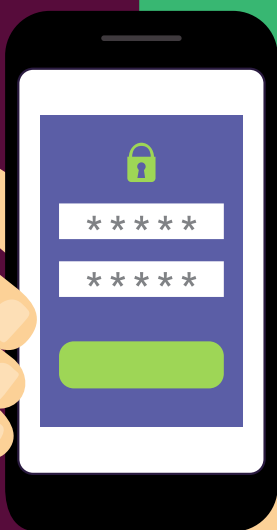
Quick tips for creating and saving
your online passwords



ADD VARIETY

Use uppercase, lowercase, characters, and numbers.

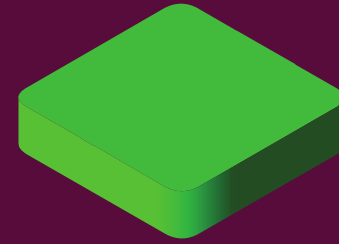
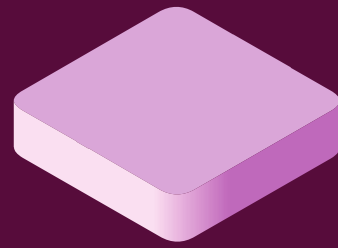
58isMypet58\$





DON'T RECYCLE

Don't use the same password for all of your accounts.



STEER CLEAR OF PERSONAL INFORMATION

Avoid using birthdates or
names from your loved
ones.





MAKE IT LONG

Use passwords longer than
six characters when
possible.

58isMypet58\$

8-12charaters



HER
Internet





CHANGE IS GOOD

Make sure to review your passwords and change them frequently.

Atleast every after 90days



USE A PASSWORD MANAGER

Password management apps and sites can help keep track e.g. Lastpass, Key chain, Nordpass, 1password.



For more tips, visit
www.herinternet.org



HOW TO SEE SAVED PASSWORDS

Android/tablets

1. open chrome
2. At the top right, tap more settings
3. Tap password managers under "password check" tap check passwords.

**For more tips visit
www.herinternet.org**



TWO-FACTOR AUTHENTICATION 2FA

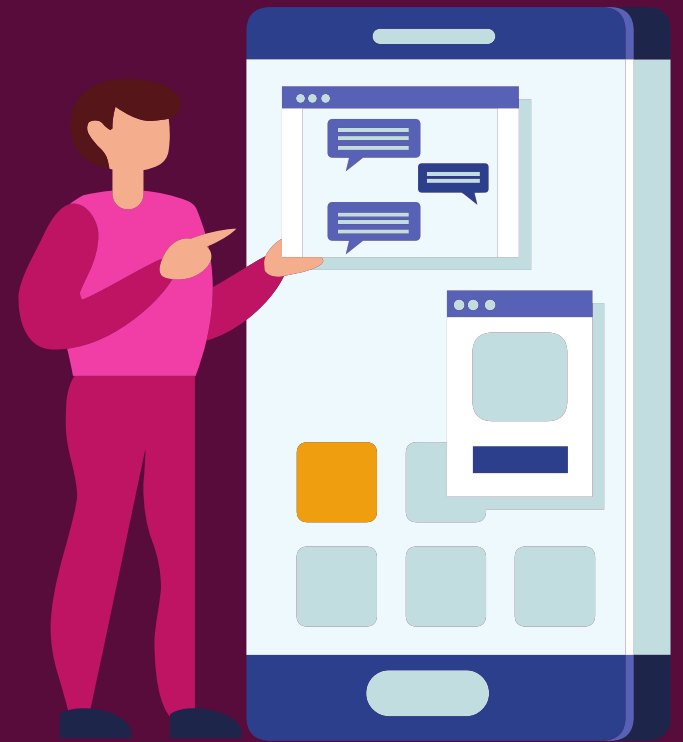
This is a verification method that provides two different types of verification to prove their identity.

For example a password
and pin
58isMypet58\$
565758



TYPES

1. One time passwords(OTP)
2. Biometric authentication
3. Hardware tokens
4. Push notifications



CONSIDERATIONS

1. Users should select strong, unique passwords
2. Back up methods for authentication





For more tips visit www.herinternet.org

