SOCIAL ENGINEERING

The use of deception to manipulate people into divulging confidential and personal information that may be used for fraud, scams, and hacking

TYPES OF SOCIAL ENGINEERING

PHISHING

Hackers pretend to be trusted names using familiar email addresses to obtain your personal information

PIGGYBACKING/TAILGATING

A hacker physically follows an employee into a restricted area or logs onto their computer to access a private network

PRETEXTING

Hackers impersonate other trusted figures within an organization, such as supervisors or coworkers, to gain your trust so that you'll provide them with data

PHARMING

Hackers re-create websites that look identical to the original, but instead contain malware that accesses your personal information

SOCIAL MEDIA

Similar to phishing, hackers will act like someone you know and try to obtain information through messages, or get you to click malicious links

HOW DOES IT AFFECT YOU?

If criminals get your credentials, they can impersonate you in crimes, hack your company, access your private network, or steal your identity

Hackers can access devices and files at your company, sending out confidential data and spam through your email account

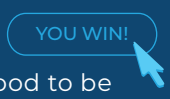
Once hackers gain entry to your accounts, they can manage, transfer, and steal your or your company's assets – and you may not realize until it's too late

BE SUSPICIOUS OF EMAILS, TEXTS, AND CALLS ASKING FOR PERSONAL INFORMATION

Watch for any communications that create a false sense of urgency and check links before opening them

CONFRIM A PERSON'S CREDENTIALS BEFORE LETTING THEM INTO RESTRICTED AREAS

WATCH FOR CLICKBAIT ON SOCIAL MEDIA



If it sounds too good to be true, it probably is

ASK QUESTIONS!

REPORT SUSPICIOUS BEHAVIOR

DON'T LET OTHERS USE YOUR LOGIN CREDENTIALS OR SHARE ANSWERS TO YOUR SECURITY QUESTIONS