PHISHING VS SOCIAL ENGINEERING

WHAT IS A SOCIAL ENGINEERING ATTACK?

- THE ATTACKER USES HUMAN INTERACTION TO OBTAIN INFORMATION ABOUT AN ORGANIZATION OR ITS COMPUTER SYSTEMS
- THE ATTACKER MAY SEEM UNASSUMING AND RESPECTABLE, POSSIBLY CLAIMING TO BE A NEW EMPLOYEE OR A REPAIR PERSON, AND MAY EVEN OFFER CREDENTIALS TO SUPPORT THAT IDENTITY. THEY WILL OFTEN DO THIS MULTIPLE TIMES WITH MULTIPLE PEOPLE UNTIL THEY GAIN ENOUGH INFORMATION TO INFILTRATE AN ORGANIZATION'S NETWORK

WHAT IS A PHISHING ATTACK?

- PHISHING ATTACKS USE EMAIL OR MALICIOUS WEBSITES TO SOLICIT PERSONAL INFORMATION BY POSING AS A TRUSTWORTHY ORGANIZATION, SUCH AS A CREDIT CARD COMPANY OR FINANCIAL INSTITUTION
- THESE EMAILS AND SITES SUGGEST THERE IS A PROBLEM, PROMPTING A USER TO RESPOND WITH SENSITIVE INFORMATION SUCH AS USERNAMES AND PASSWORDS THAT THE ATTACKER CAN THEN USE TO GAIN ACCESS TO ACCOUNT INFORMATION

BE SUSPICIOUS! NEVER GIVE PERSONAL OR FINANCIAL INFORMATION TO AN UNVERIFIED REQUESTER

cybersafework.com

CYBER SAFE WORK

Creating A Culture Of Security