SOCIAL ENGINEERING

How to recognize and respond to threats

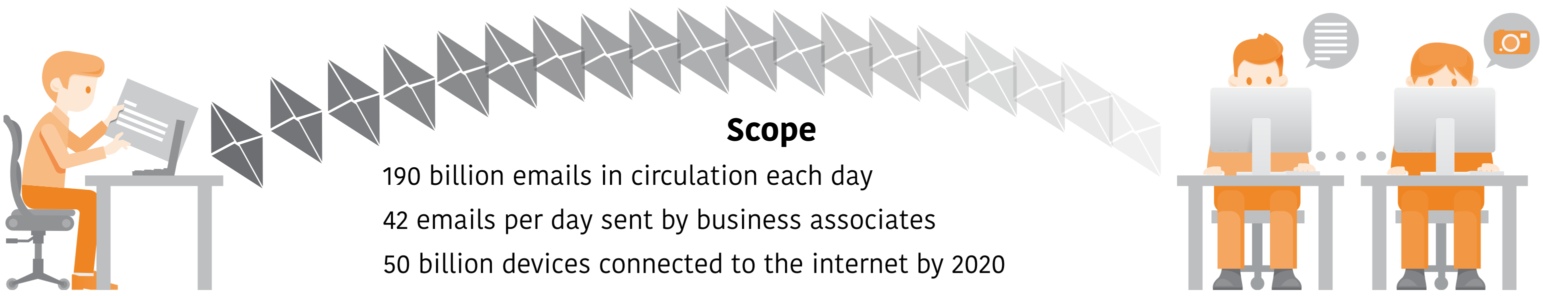
Social engineering: Hacking tricks to get users to share account or login information.

Phishing
Email-based hacking

Vishing
Phone-based phishing

Smishing
Text-based phishing

Impersonation
In-person deception



Scope
190 billion emails in circulation each day

42 emails per day sent by business associates

50 billion devices connected to the internet by 2020

Risk Factors

28% chance a business will experience a data breach within 2 years

55% increase in employee-focused phishing attacks

36% of phishing attacks use executable files

The weakest link is human

90% share names and email addresses without question

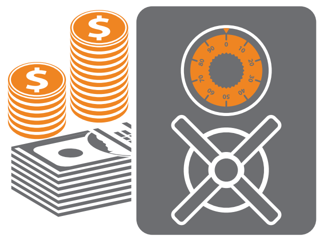
67% supply social security numbers, birth dates and employee numbers

The Costs

$3.8 million cost of average data breach

$80 billion spent on cybersecurity in 2016

$6 trillion amount per year spent on cybercrime damages by 2021



The Facts

97% of attacks employ social engineering tactics.

91% of data breaches come from phishing.

90% of data attacks could have been prevented.

How to prevent attacks

Train associates on latest schemes and proper protocols.

Use a reputable **antivirus software**.

Perform **regular backups** to an external hard drive or cloud.

Disconnect your drive after data backup to prevent ransomware attacks.

DO NOT pay the ransom. Recover data without paying.

Employ spam and virus email filters to block exploits.

Detect attacks using an endpoint protection system and IDS/IPS.