TOP TIPS TO AVOID SOCIAL ENGINEERING SCAMS

KNOW THAT SPAM FILTERS ARE IMPERFECT

Just because an email makes it into your inbox doesn't mean that it's legitimate.

VERIFY ALL FINANCIAL TRANSACTIONS

Get verbal and/or written approval before making any sort of financial transfer.

USE A PASSWORD MANAGER PROGRAM

These help you create strong, unique passwords, and alert you of any that are compromised.

USE A VPN, ESPECIALLY WHEN ON PUBLIC WIFI

Hackers can exploit unsecured WiFi to gain access to your data. Unless you're using a VPN.

BACK. UP. EVERYTHING!

Your servers, your cloud data, your laptops. Restores are your last line of defense.

DON'T TAKE IDENTITIES AT FACE VALUE

It's easy for hackers to assume the identity of a person or entity you trust over email or phone.

DON'T OPEN UNEXPECTED ATTACHMENTS

Even Word documents can be malicious; if you weren't expecting it, don't click on it.

DON'T PLUG A FOREIGN USB INTO YOUR MACHINE

Bad actors will load USB drives with malicious programs. If it isn't yours, leave it alone.

USE MULTI-FACTOR AUTHENTICATION

This keeps your accounts secure even if your passwords get compromised.

IF YOU THINK YOU'VE BEEN HIT, SHUT DOWN.

If you suspect your machine is compromised, turn it off **immediately** and contact IT.