Servis 1st Bank

Cybersecurity Awareness Month

Cybercriminals are effective at getting what they want. They've learned that the easiest way around your organization's defenses isn't hacking and cracking, it's tricking you into letting them in.

Digital Attacks

Phishing: Email-based social engineering targeting an organization.
Spear Phishing: Email-based social engineering targeting a specific person or role.

This is the method most often used by hackers. They use emails disguised as contacts or organizations you trust so that you react without thinking first. Their goal is to trick you into giving out sensitive information (your username and password), or taking a potentially dangerous action (clicking on a link or downloading/opening an infected attachment).

Phone Attacks

Smishing: Text-based social engineering.
Vishing: Over-the-phone-based social engineering.

Hackers sometimes use a made-up scenario to gain your trust so they can get the information they want. For example, they'll call and pretend to be on your IT team, mentioning the names of individuals they found while researching your organization. Then, they might say some updates just rolled out, and they need to validate a few things on your workstation.

In-Person Attacks

USB Attacks: An attack that uses a thumb drive to install malware on your computer.
Tailgating: When a hacker bypasses physical access controls by following an authorized person inside.

Hackers might try to steal information using physical access. They might "tailgate" you or one of your co-workers, which is when they will act like they work there and follow you into the office. They might also use a uniform or stolen key card to get access to unlocked workstations or valuable information left out on desks.

Red Flags

Red flags are a sign of danger or a problem. They can be as subtle as an uneasy feeling or as obvious as an email about "suspicious charges" from a bank with which you don't even have an account.

Pay attention to these warning signs as they can alert you to a cybersecurity attack!

What to Do If You Suspect Fraud

If you suspect fraud, immediately notify your ServisFirst Bank account officer.
The sooner you contact the bank, the higher the chances of getting your funds returned.

Servis 1st Bank®

For more information on how to protect your organization, please visit www.servisfirstbank.com/fraud-prevention-education/.

Please contact Cash Management with any questions at 866.922.5794 or contact your local banker.