HOW HACKERS TRY TO TRICK YOU

As cyber attacks continue to get more sophisticated, employees need to be vigilant and aware of the multitude of ways hackers can gain access to sensitive information. From phishing schemes to deepfakes, cybercriminals are constantly evolving their methods.

HERE ARE SOME OF THE WAYS YOU MIGHT BE AT RISK FOR CYBERCRIME:

SCANNING A QR CODE

QR codes are everywhere from restaurants to advertisements and even business cards. While they're very convenient, they also pose a significant risk. Cybercriminals use malicious QR codes that link directly to phishing websites to steal your personal information or infect your device with malware.

Three ways to stay safe:

- Verify the source of the QR code.
- Avoid scanning QR codes from unknown or suspicious sources.
- Use QR code scanners that can check URLs before opening them.

VIA TEXT MESSAGE

Hackers send deceptive text messages to trick people into sharing private data or clicking on a malicious link. These messages often appear to come from a trusted source, like a bank or government agency.

Three ways to stay safe:

- Be cautious of unsolicited text messages, especially those asking for personal information.
- Do not click on links or download attachments from unknown senders.
- Verify the legitimacy of the text by contacting the organization directly.

OVER THE PHONE

Scammers often call people and pose as legitimate entities to extract sensitive information. These callers often use manipulative language to create a sense of urgency or fear.

Three ways to stay safe:

- Do not provide personal information over the phone unless you are certain of the caller's identity.
- Verify the caller's credentials by contacting the organization directly.
- Be skeptical of unsolicited calls requesting sensitive information.

OVER YOUR SHOULDER

Attackers look over your shoulder to observe your screen or keyboard to steal sensitive information, such as passwords and PINs. This tactic, called "shoulder surfing," can happen in public places like cafes, airports, or even within your office.

Three ways to stay safe:

- Be aware of your surroundings when entering sensitive information.
- Use privacy screens on your devices and always lock them when unattended.
- Shield your keyboard when typing passwords or PINs.

BY IMPERSONATING SOMEONE YOU TRUST

Deepfakes use artificial intelligence to create hyper-realistic, but fake videos or audio recordings. Cybercriminals can use deepfakes to impersonate company executives or other trusted individuals, leading to significant security breaches.

Three ways to stay safe:

- Be cautious of unexpected or unusual requests, even if they appear to come from known individuals.
- Verify the identity of the person making the request through multiple channels.
- Stay informed about the latest developments in deepfake technology.