CLICK THINKING

Quick insights for protecting yourself and your company from online threats.

spotlight

Vishing and SMiShing

When it comes to scams, a phone call or a text can be as effective to a cybercriminal as an email.

When you have a phone, you're just a call or text away from anyone, including cybercriminals.

To avoid being victimized, it pays to know their tricks.

WHAT YOU NEED TO KNOW TO PROTECT YOURSELF

- Voice phishing by phone—or vishing—is the deceptive practice cybercriminals use to trick individuals into giving up valuable information.
- To avoid being vished, verify the caller's name, company, title and phone number. If the information isn't forthcoming, politely end the call.
- Listen for mumbled responses to security questions. Scammers that don't know the answers will do this hoping you'll accept a garbled response and move on.
- Some voice phishers will pretend to represent a deaf or special needs person, using this as an excuse for being confused about answers to security questions.
- Poor audio and unfamiliar dialects may indicate vishing.
- SMiShing—phishing by text—is another way scammers target individuals and businesses.
- Be wary of texts that ask you to respond immediately or threaten dire consequences for not doing so.
- Distinguish between legitimate texts asking for verification codes and malicious texts that demand immediate action.
- Be on the lookout for SMiShing attempts that ask for email resets or request sensitive account information.