10 Tips for Spotting SMiShing and Vishing

Look out for social engineering

The attacker's goal is often to convince you to talk to them so they can trick you into sharing sensitive information.

Be aware that urgency is a red flag

Attackers want you to react fast, without thinking about the consequences. Their phone calls and texts are made to provoke — claiming importance, danger or disaster.

Don't use their contact methods

If you suspect SMS phishing or voice phishing, don't contact them back using the methods they provide. Use an official phone number or website.

Remember that your phone can get malware

Getting malware onto your phone is one way attackers may breach a network. Always have antivirus on your mobile device!

Don't assume automated calls are legitimate

Some attackers will use text-to-speech devices or voice filters to sound like the automated calls used by legitimate organizations. Never assume a call is legitimate because it sounds automated.

Remember that caller ID is not foolproof

Attackers are capable of spoofing caller ID to fool their targets. Never rely on caller ID alone to prove identity.

If you suspect SMiShing or vishing, report it immediately

SMiShing and vishing can lead to holes in the overall security network and result in major breaches or losses. Always report suspected attacks to your supervisor.

Look out for common attacks

Fake security notifications and messages from government agencies are two common forms of SMiShing attacks. Vishers may impersonate government agencies, bill collectors, banks and others.

Don't click on links or download any software updates or apps from texts

Updates will never arrive via text message! Never click on a link in a text. Use a search engine or a bookmark to navigate to the site instead.

Don't show your hand

Keep your cards close to your chest. Never reveal sensitive information to someone who has called you. Call the organization back via an official number in order to fulfill information requests.