STAYING AHEAD OF THE CURVE WITH MULTI-CHANNEL PHISHING

What is Multi-Channel Phishing?

Multi-channel phishing uses a variety of platforms like SMS, social media, voice calls, and QR codes to deceive targets and steal sensitive information. Just as a misleading pit stop sign can derail an F1 race, multi-channel phishing attempts can compromise your cybersecurity by luring you into a sophisticated trap.

Common Multi-Channel Phishing Techniques

Understanding the tactics cybercriminals use is the first step to staying safe. Here are some common multi-channel moves threat actors use:

Smishing (SMS Phishing): 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.

3 Ways to Stay Safe:

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

Social Media Scams: Social media phishing includes fake accounts impersonating people you know or brands you trust. They may send messages with links to “claim a prize” or ask for personal information.

3 Ways to Stay Safe:

1. Enable multi-factor authentication (MFA) on all accounts.
2. Report and block suspicious accounts immediately.
3. Stay alert for fake ads offering deals that seem too good to be true.

Vishing (Voice Phishing): Attackers prey on our inclination to trust someone who seems authoritative on the phone. From bogus IRS agents to fake IT technicians, these scammers use fear and urgency to manipulate victims.

3 Ways to Stay Safe:

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

QR Code Phishing: Cybercriminals use malicious QR codes that link directly to phishing websites to steal your personal information or infect your device with malware.

3 Ways to Stay Safe:

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