ATTACK SPOTLIGHT

SHINING A LIGHT ON THE LATEST SECURITY THREATS

CONVERSATIONAL SMISHING SCAMS

As organizations educate users about phishing, cybercriminals look for other ways to engage potential targets. One way is to make contact through SMS messages—known as “SMS phishing” or “smishing.”

These messages usually start with a friendly conversation. Cybercriminals will spend weeks or months interacting with targets to build a relationship. Then try to trick them into sending money or investing via malicious investment platforms.

Fortunately, you can protect yourself from these attacks:

- Be suspicious of any unsolicited messages.
- Remember that cybercriminals attempt to trick people via SMS.
- Be wary of any request for money sent solely through SMS.
- Always verify communications from unknown numbers claiming to be known contacts. Use another, trusted means of communication, such as an email address.