ARTISANS' BANK
SAFETY + SECURITY
SHARED MONTHLY NEWSLETTER

NOT TODAY, SMISHER

APRIL 2024

Today, we receive texts constantly. Everything from confirming your online food order to your doctor scheduling an appointment generates a text. According to a study by RedEye, the average text message open rate is at 99%. And that's an opportunity for hackers who send scam messages.

With hackers knowing their malicious text will mostly likely be opened, and with about 24% of people who respond or interact with messages (email or SMS) from somebody they don't know, the odds that hackers will get your sensitive information are high. SMS phishing, or smishing, is becoming more common and dangerous.

WHAT IS SMISHING?

Smishing (SMS phishing) is essentially a phishing text message. It has become a popular cyberattack, tricking recipients into providing personal and sensitive information such as login credentials and credit card information.

During a smishing attack, a hacker creates a message that seems very real. It could be from a bank, a delivery service, or a friend or family member. The message is usually laced with urgency or danger.

The message often comes from a spoofed number. It may include attachments containing malware, or it may include links to phony sites.

These sites are intended to copy any information you enter. Once the hacker has the information you shared, they can use it in your real accounts, which can lead to identity theft or fraud.

Smishing attacks may also come through social media messaging apps. Hackers send direct messages on Facebook, Instagram, TikTok, X, and other popular services.

Examples of SMS attacks — *Which ones have you received?*

DELIVERY NOTIFICATION
"Your delivery is stuck at the warehouse!" The message states your package is undeliverable, and you need to urgently update your information to receive it.
Slow down and think about if you even have a package out for delivery. If you do, go to the retailer's official website to check the status of your package.

BANK FRAUD ALERT
"Suspicious activity!" The message states that there has been suspicious activity in your account, and you should click the link to confirm your identity and provide account information.
Banks will never ask for your personal or confidential information via text. If you receive a request asking for your bank credentials, ignore the message and report it. In the US or UK, you can forward the message to 7726 (SPAM).

THE "NO LINK" SCAM
"Hey there, how have you been?" Scammers will send out hundreds of these generic messages, just baiting someone to engage with them. If you answer, they lead you down a slippery and dangerous slope.
Do not engage with these types of messages — not even to tell them they have the wrong number! These conversations could lead to you being scammed.