Smishing & Phishing Explained: How to Identify Scam Texts

Author: eFraudPrevention

BankUnited

What is Smishing?

Smishing, or SMS phishing, is a type of fraud in which scammers use text messages to try and extract personally identifiable information (PII) from their targets.

They then use this stolen information for different types of identity theft-related crimes. The fraudsters often impersonate reputable organizations and ask recipients to click on a link or call a number.

While phishing scams are similar (but usually orchestrated via email), SMS texting scams take advantage of the immediacy of cell phone use. Let's see how these two types of fraud compare.

What's The Difference Between Smishing and Phishing?

A **phishing** email is one of the oldest scamming tactics borne out of the internet age.

These phishing attacks are legitimate-looking emails designed to trick recipients into giving up sensitive information or clicking on malicious links.

With the massive increase in cell phone use over the years, scammers attempt phishing scams through text messages and social media messenger apps, like WhatsApp, SnapChat and Facebook. As such, smishing is a type of phishing.

Perpetrators of both of these scam methods share the same goal — to illicitly obtain personal information from their targets.

Signs of Smishing:

- Scammers use SMS text messages to attempt to obtain information.
- Attackers usually impersonate reputable brands, like Microsoft or Amazon, to gain their victims' trust.
- Smishing messages are short, and usually include a malicious link.
- Since smishing messages are concise, they can be harder to recognize.

Signs of Phishing:

- Scammers use emails to gather information.
- Attackers may pretend to be someone from within a familiar organization or business.
- Phishing attempts can be longer emails that try to convince targets of their authenticity.
- Poor grammar or design flaws are common characteristics of scam emails.

Here are a few tips to prevent text message spam:

- **Delete text messages that ask you to confirm or provide personal information:** Legitimate companies don't ask for information like your account numbers or passwords by email or text.
- **Don't reply, and don't click on links provided in the message:** Links can install malware on your computer and take you to spoof sites that look real but whose purpose is to steal your information.
- **Treat your personal information like cash:** Your Social Security number, credit card numbers, and bank and utility account numbers can be used to steal your money or open new accounts in your name. Don't give them out in response to a text.

- **If you are an AT&T, T-Mobile, Verizon, Sprint, or Bell subscriber,** you can report spam texts to your carrier by copying the original message and forwarding it to the number 7726 (SPAM), free of charge.
- Review your cell phone bill for unauthorized charges and report them to your carrier.
- **To block spam messages** -- but not all incoming texts from friends and family -- call your carrier's customer service number (usually 611) and instruct them to "Block all text messages sent to you as email" and "Block all multimedia messages sent to you as email." You also might be able to log into your account online and activate these blocks there.
- **If dialing 611** or going into your phone settings online does not slow down spam, check with your mobile provider about other options to block future spam messages.
- **Set up and use a free email account** that's only for things like promotions, contests, and the like. This way, you can easily segregate those messages from your personal and work correspondence.
- **Don't fall for texts from your bank or credit union that ask for "confirmation details".** Your bank may well text you – for instance to confirm a transaction on PC – but bank texts will not, ever, ask you to confirm details, or for passwords. Banks also won't update their apps in this way. If you're suspicious, don't click links, and don't call any numbers in the text. Instead, call your bank on its "normal" number – Google it if you don't know – and check whether the text is from them.
- **Don't fall for warnings saying, "Your phone is infected"**. Recent SMS phishing scams use a bogus "security alert" to scare users into installing fake antivirus apps. Reputable security companies will not "push" products in this way.
- **Don't trust caller ID.** Just because your caller ID displays a phone number or name of a legitimate company you might recognize, it doesn't guarantee the call is really coming from that number or company.

Report Text Message Fraud

Federal Trade Commission (FTC) Complaint Assistant

This U.S Government service is designed to streamline the complaint process for every type of fraud. You can file a complaint online, print a copy, and get expert advice on what you need to do. Topics cover everything that falls within Rip-offs, Imposter Scams, Mobile Devices, Telephones, Internet Services, Online Shopping, Computers, Education, Jobs, Making Money, Credit, Debt, Robocalls, Unwanted Telemarketing, Text, and SPAM. or call FTC Hotline at **877-701-9595**.

Report incidents. Report fraud to reportfraud.ftc.gov or call **(888) 382-1222.** The FTC wants the number and name that appeared on the caller ID as well as the time of day and the information talked about or heard in a recorded message. If you think you've been a victim of a phishing attack you can also contact, the Internet Crime Complaint Center.

Register your number with the National Do Not Call registry at donotcall.gov. Even though criminals and unscrupulous telemarketers may ignore the list, if you are on the list and get a call from a supposed telemarketer, that could be a tip that the offer is bogus. Most legitimate telemarketers obey the rules and laws about contacting consumers. Also, the Website provides a place where complaints can be filed.

File a complaint with the FCC if you receive an unwanted commercial email message sent to your mobile phone, an autodialed/prerecorded telephone voice message, or an unwanted text message to your mobile phone. There is no charge for filing a complaint. Call **1-888-CALL-FCC (1-888-225-5322)**.

All content is for informational purposes only and does not constitute legal, tax, or accounting advice. You should consult your legal and tax or accounting advisors before making any financial decisions.