# SMS Phishing Explained: Identify threats and protect your financial security

*Provided by MAI Capital's technology department*

Hackers continue to find stealthy new ways to gain access to people's financial lives and endanger their wealth. Experts warn it has become more commonplace for even casual hackers to exploit security vulnerabilities and trick unsuspecting victims into revealing personal or financial information.

Given the prevalence of mobile devices in our lives, learning how to spot a potentially harmful threat carried out over text messaging is essential for your personal cybersecurity. SMS phishing, or smishing, occurs when cybercriminals attempt to dupe the recipient of a phony text message. These messages may include a malicious link that appears legitimate but is designed to download malware or steal credentials.

Malware, or malicious software, installs itself on your phone and may impersonate a real app and prompt you to enter confidential details before sending the information to hackers, which they can then use to commit fraud or additional cybercrimes. Malicious links lead to fake sites which request your sensitive information. These fake sites closely resemble legitimate ones, which often leads to trusting users inadvertently sharing their personal details.

A primary reason smishing has become more prevalent is due to the difference in how users interact with text messages compared with email. According to manychat.com, the average open rate for SMS messages is 98% while, on average, email recipients open about 20% of their messages[1]. Due to this, big brands now routinely use text communication to reach consumers. Additionally, users have tended to have false confidence in the safety of text messages and assume their smartphones are more secure than other devices.

However, as people have become savvier to the threat of the seemingly innocuous links described above, phishers are increasingly shifting to newer forms of smishing, which are designed to trigger a response because they purport to require necessary actions by the recipient. The following are three common types of smishing schemes.

**Financial Services Smishing.** These attacks generally consist of link-free text messages about suspicious bank transfers or other payments. These are designed to elicit a "Yes" or "No" reply about a transaction or perhaps a "1" to decline future alerts. A "No" response often results in a phone call seconds later from someone impersonating the fraud department at the financial institution.

These impostors ask for personal information to "secure your account" or "verify suspicious activity." Fraudsters will typically use the information you provide to set up new accounts in your name, which are then used to process wire transfers of stolen funds.

[1] *https://manychat.com/blog/sms-vs-email-marketing-2021/*

continued

**Free Product/Service Smishing.** An enticing offer for a free product or service, particularly from what appears to be a credible retailer, can also elicit a quick reply and open up a clear pathway for phishers to manipulate your curiosity. Once again, these types of smishing scams lure victims into providing financial information that can be used for additional - and detrimental - foul play.

**Customer Service Smishing.** Attackers may impersonate representatives from a trusted company who are helping you to resolve an issue, typically with your online account. More specifically, these schemes tend to focus on issues with billing, account access, unusual activity, or a complaint. You may be led to a fake login page where you are induced to enter your credentials or you may be asked for your actual account details so you can reset a password.

## Recent Examples

Widely circulated reports about fake messages from seemingly trustworthy sources have brought smishing scams to the forefront of cybersecurity discussions. Below are some recent examples.

**USPS & FedEx Fake Deliveries.** In the fall of 2020, reports of fake package delivery scams increased significantly. Messages alerted users to missed or incorrect deliveries and provided a link to a USPS or FedEx survey, which promised a giveaway in exchange for answering a few questions. These sham sites helped phishers steal account details, credit card information, or login credentials for services like Google.

**COVID-19 Scams.** Preying on COVID-related fears is yet another angle scammers have exploited to fool unsuspecting users into revealing personal information. Early in the pandemic, the Better Business Bureau noticed a spike in reports about text messages urging people to take mandatory COVID-19 tests via a linked website. These smishing attempts aimed to win trust by claiming to be from government agencies, the Red Cross, or even the World Health Organization.

More broadly, experts attribute the uptick in overall smishing reports to people staying home and working remotely. The corresponding rise in online shopping likely contributed to this increase and encouraged criminals to use text messages to impersonate organizations.

## How to Protect Yourself

Defense against these attacks is critical. In 2020, the FTC reported that US consumers lost $86 million as a result of scam texts.

Kaspersky, a global cybersecurity company, offers the following guidance on protecting yourself against these threats and how to respond if you are a victim of smishing[2].

**Prevent Smishing:**

- Do not respond.
- Slow down if a message is urgent.
- Call your bank or merchant directly if doubtful.
- Avoid using any links or contact info in the message.
- Check the phone number.
- Never keep credit card numbers on your phone.
- Use multi-factor authentication (MFA).
- Never provide a password or account recovery code via text.
- Download an anti-malware app.
- Report all SMS phishing attempts to designated authorities.

[2] *https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it*

continued ➦

### Respond to a Smishing Attack:

- Report the suspected attack to any institutions that could assist.
- Freeze your credit to prevent any future or ongoing identity fraud.
- Change all passwords and account PINs where possible.
- Monitor finances, credit, and various online accounts for strange login locations and other activities.

As always, please reach out to your MAI Advisor with any questions or for additional information about protecting your personal and financial information.

References:

Chickowski, E. (n.d.). What is Smishing? SMS Phishing explained. Retrieved November 17, 2021, *from AT&T Cybersecurity: https://cybersecurity.att.com/blogs/security-essentials/sms-phishing-explained-what-is-smishing*

Kaspersky. (2021, February 5). Kaspersky. Retrieved November 16, 2021, *from www.kaspersky.com: https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it*

Krebs, B. (2021, November 10). Krebs on Security. Retrieved November 17, 2021, *from www.krebsonsecurity.com: https://krebsonsecurity.com/2021/11/sms-about-bank-fraud-as-a-pretext-for-voice-phishing/*

Sadan, T. (2021, January 29). SMS vs. Email Marketing: Which Channel Wins in 2021? Retrieved November 17, 2021, *from Manychat: https://manychat.com/blog/sms-vs-email-marketing-2021/*

*Information updated as of 12.01.21*

*Past performance is no guarantee of future results. This is not a recommendation to buy or sell any security. Any statistics mentioned have been obtained from sources we believed to be reliable, but the accuracy and completeness of the information cannot be guaranteed. Any statement non-factual in nature constitutes only current opinion of this author which is subject to change without notice.*