Cyber Liability

MSV MEDICAL SOCIETY OF VIRGINIA INSURANCE AGENCY

Smishing Explained

Most businesses and individuals are familiar with phishing, a cyberattack technique that entails cybercriminals leveraging fraudulent emails to manipulate recipients into sharing sensitive information, clicking malicious links or opening harmful attachments. While these email-based scams remain a pressing concern, a new form of phishing—known as smishing—has emerged over the years, creating additional cyber exposures for businesses and individuals alike.

Smishing relies on the same tactics as phishing. The sole difference between these two cyberattack techniques is that smishing targets victims through text messages rather than emails. As a growing number of individuals utilize their smartphones for both personal and work-related purposes (e.g., interacting with colleagues and clients on mobile applications), smishing has become a rising threat. In fact, recent research found that nearly three-quarters (74%) of organizations experienced smishing incidents in the past year, while just 23% of the workforce recognizes this term.

With these numbers in mind, it's evident that businesses need to address smishing exposures within their operations. The following article provides an overview of smishing and offers best practices for businesses to protect against this emerging cyberattack technique.

What Is Smishing?

Smishing follows the same format as phishing, using deceiving messages to manipulate recipients. These messages are generally sent via text, but can also be delivered through mobile instant messaging applications (e.g., WhatsApp). In these messages, cybercriminals may implement a wide range of strategies to get their targets to share information or infect their devices with malware. Specifically, they will likely impersonate a trusted or reputable source and urge the recipient to respond with confidential details, download a harmful application or click a malicious link. Here are some examples of common smishing messages:

- A message claiming to be from a financial institution, saying the recipient's bank account is locked or experiencing suspicious activity and asking them to click a harmful link to remedy the issue
- A message impersonating a well-known retailer (e.g., Amazon, Target or Walmart), encouraging the recipient to download a malware-ridden application to receive a gift card or similar prize
- A message claiming to be from an attorney or law enforcement, saying the recipient is facing legal trouble or criminal charges and urging them to call an unknown number for more information
- A message impersonating the government, asking the recipient to click a suspicious link for details on their taxes or participation in a federal loan program
- A message claiming to be a research organization, requesting the recipient download a malicious application to complete an informational survey
- A message impersonating a delivery service, informing the recipient that they are receiving a package and providing them with a fraudulent link for tracking the item

If a recipient is tricked into doing what a smishing message asks, they could end up unknowingly downloading malware or exposing sensitive information, such as login credentials, debit and credit card numbers or Social Security numbers. From there,

cybercriminals may use the information they obtained from smishing for several reasons, such as hacking accounts, opening new accounts, stealing money or retrieving additional data. Since individuals may use their smartphones for work-related tasks, smishing has the potential to impact businesses as well. For example, an individual who falls for a smishing scam could inadvertently give a cybercriminal access to their workplace credentials, allowing the criminal to collect confidential data from the victim's employer and even steal business funds.

The nature of smishing has made this cyberattack technique a significant threat. This is because individuals are typically not as careful when communicating on their smartphones compared to their computers, often engaging in multiple text conversations at a time (sometimes while distracted or in a rush). After all, research from Experian found that individuals between ages 18-24 exchange around 4,000 texts each month. Considering these findings, individuals may be less wary or observant of a text message from an unknown number than an email, making them more likely to interact with a malicious text.

Furthermore, many individuals falsely assume that their smartphones possess more advanced security features than computers, thus protecting them from harmful messages. However, smartphone security has its limits. Currently, these devices are unable to directly safeguard individuals from smishing attempts, leaving all smartphone users vulnerable. That's why it's important for businesses to take steps to protect against smishing.

How to Protect Against Smishing

To effectively minimize smishing exposures and prevent related cyberattacks, businesses should:

- **Conduct employee training**—First, businesses should educate employees on what smishing is and how it could affect them. Additionally, employees should be required to participate in routine training regarding smishing detection and prevention. This training should instruct employees to:
  - Watch for signs of smishing within their text messages (e.g., lack of personalization, generic phrasing and urgent requests)
  - Refrain from interacting with or responding to messages from unknown numbers or suspicious senders
  - Avoid clicking links or downloading applications provided within messages
  - Never share sensitive information via text
  - Utilize trusted contact methods (e.g., calling a company's official phone number) to verify the validity of any request sent over text
  - Report any suspicious messages to the appropriate parties, such as a supervisor or the IT department
- **Ensure adequate bring-your-own-device (BYOD) procedures**—Apart from providing smishing training, businesses should establish solid BYOD procedures to ensure employees act accordingly when utilizing their personal smartphones for work-related purposes. Such procedures may include using a private Wi-Fi network, implementing multifactor authentication capabilities, conducting routine device updates and logging out of work accounts after each use. These procedures can help deter smishing attempts and decrease the damages that may ensue from smishing incidents.
- **Implement access controls**—Another method for limiting smishing exposures is the use of access controls. By only allowing employees access to information they need to complete their job duties, businesses can reduce the risk of cybercriminals compromising excess data or securing unsolicited funds amid smishing incidents. To further protect their information, businesses should consider leveraging encryption services and establishing secure locations for backing up critical data.
- **Utilize proper security software**—Businesses should also make sure company-owned smartphones are equipped with adequate security software. In some cases, this software can halt cybercriminals in their tracks, stopping smishing messages from reaching recipients' devices and rendering harmful links or malicious applications ineffective. In particular, smartphones should possess antivirus programs, spam-detection systems and message-blocking tools. Security software should be updated as needed to ensure effectiveness.
- **Purchase sufficient coverage**—Finally, it's vital for businesses to secure proper cyber insurance to protect against potential losses stemming from smishing incidents. Businesses should reach out to their trusted insurance professionals to discuss specific coverage needs.

Conclusion

In summary, smishing is a serious cyber threat that both individuals and businesses can't afford to ignore. By staying aware of smishing tactics and implementing solid mitigation measures, businesses can successfully protect against this rising cyberattack technique, deterring cybercriminals and minimizing associated losses. For more risk management guidance, contact us today.