Bank of Botetourt

September 2023

What Is Smishing? Definition, Examples & Protection

Modern communication is largely dominated by mobile devices and cybercriminals have devised new ways to exploit unsuspecting users. One such method that has gained significant attention is smishing—a malicious practice that aims to deceive and defraud people through text messages. Short for "SMS phishing," smishing utilizes persuasive messages to trick recipients into revealing sensitive information or downloading harmful content.

Definition of Smishing (SMS Phishing)

Smishing, derived from "SMS" and "phishing," is a type of cybercrime that uses deceptive text messages to manipulate victims into divulging sensitive personal information such as bank account details, credit card numbers and login credentials.

Just as with phishing emails, the goal of smishing is to trick individuals into revealing private information that can be used for identity theft, financial theft or other fraudulent activities. Given the prevalence of text messaging as a form of communication, smishing has become a significant concern in cybersecurity.

Smishing vs. Phishing

Both smishing and phishing are forms of cyberattacks that trick individuals into providing personal, sensitive information. They primarily differ in their methods of delivery and the technologies they exploit.

Phishing

This is a broader term for a method of deceptive communication intending to trick recipients into revealing sensitive information, such as usernames, passwords, credit card numbers or Social Security numbers. Typically, phishing attacks occur via email. The attacker sends a seemingly legitimate email that encourages the recipient to click on a link. This link then leads to a fraudulent website that resembles a trusted site where the recipient is prompted to enter their sensitive information.

Smishing

This is a form of phishing that uses Short Message Service (SMS), commonly known as text messages, instead of email. Typically, the scammer poses as a legitimate institution, such as a bank, a service provider or a reputed company. The text message they send creates a sense of urgency or threatens consequences if the victim doesn't respond immediately. It downloads malware on the phone or includes a link to a fraudulent website designed to look like the legitimate organization's site. When victims reach that site they are tricked into entering their personal information.

What is Smishing vs. Vishing?

Smishing and vishing are both phishing tactics targeting mobile users. Smishing uses deceptive SMS

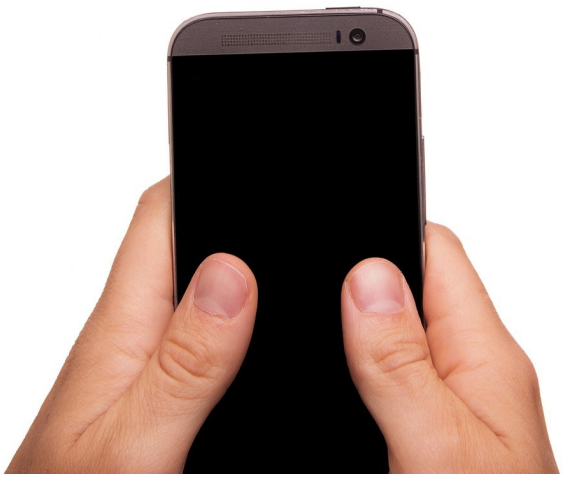
Continued on Page 2

Member FDIC

EQUAL HOUSING LENDER

Connect with us!

(540) 591-5000



text messages to trick victims into revealing sensitive information. Vishing, on the other hand, uses voice calls or voice mails for the same fraudulent purpose.

It's essential to never share personal information in response to unsolicited messages, whether received via email, phone, or text message, and to independently verify the request through known, trusted channels.

7 Types of Smishing

Smishing attacks can take several forms, each with its own approach but all ultimately aiming to trick victims into divulging sensitive information or performing actions beneficial to the attacker. Here are some of the most common types of smishing attacks:

1. ***Impersonation Scams***: The attacker pretends to be a known organization or individual. The attack could be via a message pretending to be from a bank, government agency or a reputable company.
2. ***Tech Support Scams***: Attackers pose as representatives from tech companies, claiming that the victim's device or account has been compromised and that they need sensitive data to fix the problem.
3. ***Account Suspension Scams***: These messages claim that an account (bank account, social media or any other service) has been suspended and prompt the victim to verify their identity by providing sensitive information.
4. ***Missed Delivery Scams***: Attackers send messages claiming that the victim has missed a package delivery, and they need to provide personal details or a fee to reschedule the delivery.
5. ***Prize or Lottery Scams***: Messages claiming that the victim has won a prize or a lottery, and they need to provide personal details or make a payment to claim the winnings.
6. ***Charity Scams***: In these attacks, scammers impersonate a charitable organization, asking for donations, usually following a large-scale disaster or during holiday seasons.
7. ***Malware Link Scams***: Messages containing a link, which when clicked, installs malware on the victim's device, allowing the attacker to steal information or gain control over the device.

Attackers are constantly innovating and finding new ways to exploit human trust, so it's crucial to be skeptical of any unsolicited or unexpected message that asks for sensitive information or prompts to click a link.

How To Protect Against Smishing

Protecting against smishing attacks involves a combination of awareness, vigilance and adopting certain precautionary measures. Here are some steps you can take:

1. ***Be Suspicious***: Always be wary of unsolicited messages that request personal information or urge you to take immediate action.
2. ***Don't Click on Links***: Avoid clicking on links in unexpected or unsolicited text messages. If you believe the message could be legitimate, independently look up the company's contact information and reach out to them directly for verification.
3. ***Verify the Sender***: Be cautious of messages from unknown numbers or numbers that don't look like phone numbers. Scammers often use email-to-text technologies to anonymize their true phone numbers.
4. ***Install Security Software***: Keep your mobile device secure by using trusted security software, and ensure that all your devices have the latest updates and patches.
5. ***Educate Yourself and Others***: Awareness is a powerful tool against smishing. Understand the tactics scammers use and share this knowledge with friends and family.
6. ***Use Two-Factor Authentication***: Implement two-factor authentication on your accounts when possible. This adds an extra layer of security, making it harder for scammers to access your accounts, even if they get your login details.
7. ***Don't Respond***: If you receive a smishing text, don't respond, even if the message gives you an option to "opt out" of future messages. Responding can confirm to the scammer that your number is active.
8. ***Report Smishing Attempts***: Forward smishing texts to 7726 (or "SPAM") on most carriers. This helps your carrier identify and block spammers. You can also report the scam to the Federal Trade Commission (FTC) in the United States.

Remember, the most important rule is to never share your personal information in response to an unsolicited message. If in doubt, contact the company or organization directly using contact details you know are legitimate.

You can prevent smishing by staying vigilant. You should avoid clicking links in unexpected texts, never share personal information in response to unsolicited messages, use security software, update devices regularly, implement two-factor authentication and report suspected smishing attempts to your service provider.

Sources/Credit:

Article:

Forbes Advisor, What Is Smishing? Definition, Examples & Protection, By Shweta, Kelly Main, Contributor, Editor, August 1, 2023

Images:

Telephone, Mobile, Call image. Free for use., By: niekverlaan,

Smartphone, Phone, Typing image. Free for use.: By: niekverlaan; Attribution: Pixabay; Pixabay Content License Summary

2023 Business Email Compromise Statistics

BEC attacks are more common than ever

In 2023, the volume of nefarious emails impersonating enterprises reached a staggering crescendo, with attacks such as BEC making up 99% of reported threats. Historically, most of the threats reported in user inboxes have been BEC attacks, but 99% represents by far the highest share since Fortra began tracking this data point.

Considering this intelligence, organizations must implement a security awareness training program to ensure their staff are well placed to identify and flag potential BEC attacks. The unprecedented prevalence of BEC attacks means that, essentially, they are not a risk but an inevitability. Organizations must provide their employees with the necessary skills and information to recognize and alert security teams to the warning signs of a potential BEC scam.

Cybercriminals are innovating BEC tactics

Traditionally, BEC scams impersonate an organization's CEO or high-level executive to fool victims into facilitating a major financial transaction. However, threat actors have begun to change their tactics, expanding their target list to include vendors associated with the intended victim. By compromising a third-party or business partner, cybercriminals can target larger organizations with realistic emails containing key insider information, significantly increasing the legitimacy of an attack and the likelihood of success. Similarly, cybercriminals have begun to utilize generative AI to craft well-written, mistake-free emails that are more likely to fool victims.

Interestingly, while wire transfers made up only 4% of the preferred cash-out methods, in Q1, cybercriminals moved away from asking for a specific payment. Instead, attackers ask the victim to provide "the outstanding balance" or "owed amount", attempting to redirect payment of an unpaid invoice that has been partially or fully approved by internal stakeholders.

These developments are yet another example of how important regular security awareness training is. It is not enough to provide security awareness training upon hiring an employee or once a year; organizations must administer training regularly to reflect the current threat landscape.

Hybrid vishing is on the rise

Hybrid vishing attacks, which use phone numbers and the stolen intellectual property of trusted brands to evade gateways and convince users of their legitimacy, make up for 45% of all reported Response-Based threat types. These attacks primarily impersonated online financial services brands such as PayPal and digital security software such as Norton or McAfee products. If the victim calls the phone number, the criminal will attempt to monetize the attack through identity theft, credit card fraud, or a malware implant.

Again, organizations must empower their employees to identify and thwart hybrid vishing attacks with cybersecurity awareness training. Hybrid vishing is a relatively new attack technique, and it is likely that an organization's staff will be neither aware of it nor how to thwart it.

Credential theft is making a comeback

Despite falling in the second half of 2022, credential theft led all email impersonation threat types in Q1 2023. The Microsoft O365 phish drove this increase, experiencing the largest quarter-over-quarter jump in share (10%) since Fortra began reporting this datapoint, making up nearly 41% of all credential theft phishes. Most modern organizations use the Microsoft Suite in some capacity, meaning users are pre-conditioned to trust emails from Microsoft, helping cybercriminals obfuscate their attacks.

Although it's difficult to convey, organizations must impress upon their staff that the brands they trust the most are inherently the least trustworthy. Again, this can only be achieved through effective security awareness training.

Fortra's 2023 BEC Trends, Targets, and Changes in Techniques Report reveals the alarming surge in Business Email Compromise (BEC) attacks, constituting 99% of reported threats. Cybercriminals are innovating tactics by targeting vendors and utilizing generative AI. Hybrid vishing and credential theft are also on the rise. Organizations must prioritize regular security awareness training to empower their staff to identify and thwart these evolving threats. The report serves as a crucial reminder that knowledge and proactive measures are paramount in safeguarding against cybersecurity risks in today's increasingly perilous digital landscape.

Sources/Credit:
Article:
2023 Business Email Compromise Statistics, Josh Breaker-Rolfe, August 15, 2023
Image:
Scam Phishing Fraud royalty-free stock illustration. Free for use & download, Image by Mohamed_hassan; Attribution: Pixabay; Pixabay Content License Summary