5-Step Plan for Employers to Defeat Text Message 'Smishing' Scams

Insights
5.05.22

Have you received a text from a random number in the last few days? Perhaps the text looks quite obviously suspicious, but it could pass as legitimate – especially if you are distracted or multitasking while scrolling through your device. The text contains a link asking you to confirm the delivery or receipt of a package. Or it tells you that you have just paid a bill. Or need to pay an outstanding bill. Or it could just be advertising a random product. These texts are actually scams that have been dubbed "smishing" – combining "SMS" and "phishing" – and your employees are no doubt receiving them, too. In a remote-work era where a multitude of attackers are attempting to gain access to your company network through digital vulnerabilities, the time is now for employers to guard yourself against this latest weapon in the cyberwar raging all around us. What are the five steps your organization can take today to best prepare?

What is Smishing?

"Smishing" is a version of phishing carried out over SMS (short message service, commonly known as texting) channels. The senders of these malicious texts are trying to get hold of personal information, passwords, and money.

Smishers start by sending a text impersonating a reputable company. Typical smishing attempts specifically involve using the name of common parcel carriers informing you that your package has been delivered, or fake texts seemingly coming from a bank, company vendor, or other common company name. The messages almost always have a link. Unfortunate recipients who click that link will often end up having unsuspecting malware downloaded to their devices, or will be lead to a legitimate-looking form to "log in" and voluntarily provide a trove of valuable data.

Smishing is the New Cyberattack

There is ample evidence indicating a rapid increase in smishing attempts. Smishing attacks increased 24% in the U.S. alone and 69% globally last year. According to data from the Federal Trade Commission, 21% of fraud reports that were filed in 2021 involved smishing. That's 377,840 out of the total 1,813,832 reports that identify a contact method. Of those hundreds of thousands of claims, a total of $131 million was lost, with an average of $900 per report.

Work-from-home and hybrid work arrangements have led your employees to use their mobile phones and company devices at an increasing rate. This has led many of these smishing attacks to have a workplace component.

What Can Employers Do? A 5-Step Plan to Combat Smishing

So what can you do to address this latest cyber-concern? Here are five steps your organization can take to put yourself in the best position.

1. **Develop Strong BYOD Policies**
   First, you should have – and enforce – strong BYOD policies. They should include employee obligations relating to data security on company devices, with a new emphasis on smishing scams.

   Among other things, the policy should advise employees that they must protect confidential, proprietary, and non-public information, and that they should not allow non-employees to copy or download such information. The policy should also require employees not to share remote access addresses, logins, or passwords with anyone, even if they believe that the individual requesting the information has already been approved for remote access.
2. **Stay Up to Date**
   Next, you should make sure you keep company issued phones' software and web browsers up to date to take advantage of build-in protection features. Ask your employees to do the same for personal devices being used for business purposes.
3. **Keep Things Need-to-Know**
   You should also take steps to make confidential or other sensitive information available only on a need-to-know basis. This will minimize the spread of the information and opportunities for cybercriminals to access company data if a device is compromised. You should advise employees who do have access to such information not to provide it in response to a request delivered through text message.
4. **Enable Multi-Factor Authentication**
   You should also consider requiring multi-factor authentication to access company systems. This will provide extra security in the event an employee has their password compromised.
5. **Train, Train, Train**
   Finally, and perhaps most importantly, you should instruct employees to be wary of unsolicited requests for information sent by text and phone call. Educate your employees on the typical hallmarks of smishing schemes, including the sense of urgency often embedded into the message, such as a "limited-time offer" or other call for immediate action. You should caution employees not to tap links in an unexpected text message.

   If employees are unsure if the text is legitimate, you should train them to contact the company associated with the text request through a separate source, such as a previously verified phone

associated with the text request through a separate source, such as a previously verified phone number. If they receive a text from an unknown number from someone indicating they are a co-worker, you should train the recipient to follow up with the purported sender via company email or phone to confirm the text message.

Conclusion

Fisher Phillips will continue to monitor further developments regarding smishing, so be sure to subscribe to Fisher Phillips' Insight system to stay up-to-date. If you have any questions regarding how your organization can mitigate the risk of smishing attempts, please consult your Fisher Phillips attorney, the author of this Insight, or a member of Fisher Phillips' Privacy and Cyber Practice Group.

Related People

Risa B. Boerner, CIPP/US, CIPM
Partner
610.230.2132
Email

Brett P. Owens

Partner
813.769.7512
Email

Service Focus

Privacy and Cyber