Texas Council Risk Management Fund

Short Messaging Service (SMS) Attacks

SMS Phishing or Smishing is a social engineering attack that uses fake mobile text messages to trick people into downloading malware, sharing sensitive information, or sending money to criminals. The term “smishing” is a combination of “SMS”—or “short message service,” the technology behind text messages—and “phishing.” In many cases, the cybercriminal poses as someone you know or authorized to ask you for sensitive information, such as tech support staff, government workers, a bank, or another financial institution.

So, how does a cybercriminal use smishing? A smishing text is a text message sent to your phone worded in a way that makes you feel comfortable sharing personal information. Often, these “texts” are actually emails sent to your phone. The attacker never has your phone number in the first place. A smishing text may also contain a link to a site that looks legitimate. However, once you enter your personal information, it is captured by a cybercriminal and either used by them or sold to someone who seeks to abuse your credentials.

Smishing attacks often work by combining two or more steps, with the end objective of stealing your information. The first step is to get you to feel obligated to take action. This can be for legal reasons, to make money, or to “save” money that you do not want stolen. The second step is to get you to a legitimate-looking site designed to look nearly identical to the kind of site you expect to see. For example, if it is a government site, it will have the appropriate crest or insignia that corresponds with the agency you expect the site to belong to. If it is a financial institution, the site may have fonts, logos, and color schemes you will normally see on a site run by that institution.

The final step is to get you to enter your personal information. The request can be something as straightforward as asking you to enter your account name and password. Once you provide the information and submit it, the attack succeeds. Smishing can also be executed using fewer steps. For example, the original text may contain a link that, once tapped, downloads malware that can be used to steal your information.

One of the most effective tools to help people in an organization avoid smishing attacks is education. Attackers may use several methods to trick their targets, but many of the attacks have similar signatures. Making sure all employees and executives know what the different kinds of smishing attacks look like can equip them to spot and stop them.

Here are some ways users help to prevent smishing attacks:

1. Anything that demands you act quickly or with a sense of urgency should be questioned.
2. Never click on links embedded inside text messages.
3. Check the number that sends a message asking for information or to click a link inside it. If it looks suspicious, it is possibly a smishing attack.

4. Never keep your banking or credit card information on your phone. Malware can be used to access it.
5. If you do not know who is texting you, do not reply to the message or click anything inside it.
6. Report smishing attempts to the Federal Communications Commission (FCC) to help other potential victims.
7. Do not respond to requests to change or update account information via text message.

Security Awareness Training helps your organization fight smishing and other social-engineering attacks by providing users with continuous simulation and training to understand the latest attack techniques, recognize subtle clues and help stop email fraud, data loss, and organizational damage.

The TCRMF Cyber Risk Services Advisor is ready to schedule Cyber Risk Assessments, Incident Response Plan Tabletop Testing visits, and Cyber Presentations for members. To get on the schedule, contact Lee Cain, Cyber Risk Services Advisor, at (512) 619-1437 or Lee.Cain@sedgwick.com.