Be Aware of Smishing

607-433-2200 | directive.com

Phishing + SMS = Smishing

By sending a message that claims (and may even appear) to come from an authority figure or trusted contact, an attacker can bypass your security by convincing a user to undermine their protections.

Smishing is simply the application of these principles via a text message, rather than through the generally standard email.

Instead of an email or phone call, you could get a text message from a number that claims to be an institution that you do business with, be it a financial institution, a service provider, what have you.

Chances are, there will be a link included with the message, prompting you to log in. The problem is the link will direct you to a fraudulent login page which will collect your actual credentials. Some will prompt you to download a document, which (surprise, surprise) is hiding some variety of malware in it.

So, simple as that, an attacker suddenly has access to one of your accounts, or potentially your device itself. Just take a moment and consider how much sensitive data you likely keep on your phone, data that could then be extracted by the hacker.

To safeguard yourself against such scams, it is crucial to be vigilant and aware. This checklist will help you identify and avoid falling victim to text message scammers.

Who is the Sender? Scammers often use generic or unfamiliar numbers to mask their identities. If the message claims to be from a company or organization, verify the contact information independently before responding.

Watch for Threats or Urgency: Text messages containing phrases like "urgent response required" or "your account will be closed" are red flags. Legitimate organizations usually provide ample time to address issues and do not resort to threats.

How's the spelling and grammar? Scammers frequently make spelling and grammatical errors. A consistently poor quality of writing can indicate a fraudulent message.

What are they asking for? Beware of text messages asking for personal or sensitive information such as your Social Security number, bank account details, or passwords. Legitimate institutions seldom ask for such information via text messages.

Do they want you to click a link? Text messages may include shortened URLs or hyperlinks leading to malicious websites. Avoid clicking on these links without verifying their legitimacy.

Trust your instincts! If something feels off or too good to be true, it probably is. Listen to your gut feeling when assessing the authenticity of a text message. When in doubt, contact the organization directly to verify the message's legitimacy.

directive
Outsource IT

330 Pony Farm Road, Oneonta, NY 13820