OUCH! | September 2020

SANS SECURITY AWARENESS

OUCH!

The Monthly Security Awareness Newsletter for Everyone

Stop That Phish

Overview

Email and messaging services (such as Skype, Twitter, or Snapchat) are one of the primary ways we communicate. We not only use these technologies every day for work, but also to stay in touch with friends and family. Since so many people around the world depend on these technologies, they have become one of the primary attack methods used by cyber attackers. This attack method is called phishing. Learn what phishing is and how you can spot and stop these attacks, regardless if you are at work or at home.

What Is Phishing

Phishing is a type of attack that uses email or a messaging service to fool you into taking an action you should not take, such as clicking on a malicious link, sharing your password, or opening an infected email attachment. Attackers work hard to make these messages convincing and tap your emotional triggers, such as urgency or curiosity. They can make them look like they came from someone or something you know, such as a friend or a trusted company you frequently use. They could even add logos of your bank or forge the email address so the message appears more legitimate. Attackers then send these messages to millions of people. They do not know who will take the bait, all they know is the more they send, the more people will fall victim.

Protecting Yourself

In almost all cases, opening and reading an email or message is fine. For a phishing attack to work, the bad guys need to trick you into doing something. Fortunately, there are clues that a message is an attack. Here are the most common ones:

- A tremendous sense of urgency that demands “immediate action” before something bad happens, like threatening to close an account or send you to jail. The attacker wants to rush you into making a mistake.
- Pressuring you to bypass or ignore your policies or procedures at work.
- A strong sense of curiosity or something that is too good to be true. (No, you did not win the lottery.)

- A generic salutation like “Dear Customer.” Most companies or friends contacting you know your name.
- Requesting highly sensitive information, such as your credit card number, password, or any other information that a legitimate sender should already know.
- The message says it comes from an official organization, but has poor grammar or spelling or uses a personal email address like @gmail.com.
- The message comes from an official email (such as your boss) but has a Reply-To address going to someone’s personal email account.
- You receive a message from someone you know, but the tone or wording just does not sound like him or her. If you are suspicious, call the sender to verify they sent it. It is easy for a cyber attacker to create a message that appears to be from a friend or coworker.

Ultimately, common sense is your best defense. If an email or message seems odd, suspicious, or too good to be true, it may be a phishing attack. Subscribe to OUCH! and receive the latest security tips in your email every month - www.sans.org/security-awareness/ouch-newsletter.

Guest Editor

Tonia Dudley has been developing and running Security Awareness programs since 2011, which includes building an award-winning phishing training program. You can find her at www.linkedin.com/in/toniadudley.

Resources

Social Engineering:	https://www.sans.org/u/Cb1
Helping Others Secure Themselves:	https://www.sans.org/u/Cb6
Email Do’s and Don’ts:	https://www.sans.org/u/Cbg
CEO Fraud:	https://www.sans.org/u/Cbl
OUCH! Translations and Archives:	https://www.sans.org/u/Cbq

License