Types of phishing

Phishing is one of the most common types of **social engineering**, which are manipulation techniques that exploit human error to gain private information, access, or valuables. Previously, you learned how **phishing** is the use of digital communications to trick people into revealing sensitive data or deploying malicious software.

Sometimes, phishing attacks appear to come from a trusted person or business. This can lead unsuspecting recipients into acting against their better judgment, causing them to break security procedures. In this reading, you'll learn about common phishing tactics used by attackers today.

Des ressources sensibles sont extraites d'un ordinateur à l'aide de divers hameçons.

The origins of phishing

Phishing has been around since the early days of the internet. It can be traced back to the 1990s. At the time, people across the world were coming online for the first time. As the internet became more accessible it began to attract the attention of malicious actors. These malicious actors realized that the internet gave them a level of anonymity to commit their crimes.

Early persuasion tactics

One of the earliest instances of phishing was aimed at a popular chat service called AOL Instant Messenger (AIM). Users of the service began receiving emails asking them to verify their accounts or provide personal billing information. The users were unaware that these messages were sent by malicious actors pretending to be service providers.

This was one of the first examples of mass phishing, which describes attacks that send malicious emails out to a large number of people, increasing the likelihood of baiting someone into the trap.

During the AIM attacks, malicious actors carefully crafted emails that appeared to come directly from AOL. The messages used official logos, colors, and fonts to trick unsuspecting users into sharing their information and account details.

Attackers used the stolen information to create fraudulent AOL accounts they could use to carry out other crimes anonymously. AOL was forced to adapt their security policies to address these threats. The chat service began including messages on their platforms to warn users about phishing attacks.

How phishing has evolved

Phishing continued evolving at the turn of the century as businesses and newer technologies began entering the digital landscape. In the early 2000s, e-commerce and online payment systems started to become popular alternatives to traditional marketplaces. The introduction of online transactions presented new opportunities for attackers to commit crimes.

A number of techniques began to appear around this time period, many of which are still used today. There are five common types of phishing that every security analyst should know:

- **Email phishing** is a type of attack sent via email in which threat actors send messages pretending to be a trusted person or entity.
- **Smishing** is a type of phishing that uses Short Message Service (SMS), a technology that powers text messaging. Smishing covers all forms of text messaging services, including Apple's iMessages, WhatsApp, and other chat mediums on phones.
- **Vishing** refers to the use of voice calls or voice messages to trick targets into providing personal information over the phone.
- **Spear phishing** is a subset of email phishing in which specific people are purposefully targeted, such as the accountants of a small business.
- **Whaling** refers to a category of spear phishing attempts that are aimed at high-ranking executives in an organization.

Since the early days of phishing, email attacks remain the most common types that are used. While they were originally used to trick people into sharing access credentials and credit card information, email phishing became a popular method to infect computer systems and networks with malicious software.

In late 2003, attackers around the world created fraudulent websites that resembled businesses like eBay and PayPal™. Mass phishing campaigns to distribute malicious programs were also launched against e-commerce and banking sites.

Profils de réseaux sociaux extraits d'un ordinateur.

Recent trends

Starting in the 2010s, attackers began to shift away from mass phishing attempts that relied on baiting unsuspecting people into a trap. Leveraging new technologies, criminals began carrying out what's known as targeted phishing attempts. Targeted phishing describes attacks that are sent to specific targets using highly customized methods to create a strong sense of familiarity.

A type of targeted phishing that evolved in the 2010s is angler phishing. **Angler phishing** is a technique where attackers impersonate customer service representatives on social media. This tactic evolved from people's tendency to complain about businesses online. Threat actors intercept

complaints from places like message boards or comment sections and contact the angry customer via social media. Like the AIM attacks of the 1990s, they use fraudulent accounts that appear similar to those of actual businesses. They then trick the angry customers into sharing sensitive information with the promise of fixing their problem.

Key takeaways

Phishing tactics have become very sophisticated over the years. Unfortunately, there isn't a perfect solution that prevents these attacks from happening. Tactics, like email phishing that started in the last century, remain an effective and profitable method of attack for criminals online today.

There isn’t a technological solution to prevent phishing entirely. However, there are many ways to reduce the damage from these attacks when they happen. One way is to spread awareness and inform others. As a security professional, you may be responsible for helping others identify forms of social engineering, like phishing. For example, you might create training programs that educate employees about topics like phishing. Sharing your knowledge with others is an important responsibility that helps build a culture of security.

Resources for more information

Staying up-to-date on phishing threats is one of the best things you can do to educate yourself and help your organization make smarter security decisions.

- Google’s phishing quiz is a tool that you can use or share that illustrates just how difficult it can be to identify these attacks.
- Phishing.org reports on the latest phishing trends and shares free resources that can help reduce phishing attacks.
- The Anti-Phishing Working Group (APWG) is a non-profit group of multidisciplinary security experts that publishes a quarterly report on phishing trends.

Revision #1
Created 26 August 2023 13:21:05 by naruzkurai
Updated 26 August 2023 13:21:24 by naruzkurai