Phishing is a technique widely used by cyber threat actors to lure potential victims into unknowingly taking harmful actions. This popular attack vector is undoubtedly the most common form of social engineering—the art of manipulating people to give up confidential information— because phishing is simple and effective. Scammers launch thousands of phishing attacks every day, and they're often successful.

In this guide

What is phishing?

In the 1990s, it was common for hackers to be called Phreaks. What passed for hacking in those days was referred to as phreaking. So, the act of using a lure—a more or less authentic-looking email —to catch or trick an unsuspecting computer user adopted the "ph" from phreaking to replace the "f"

Phishing scams are often the “tip of the spear” or the first part of an attack to hit a target. The attack may be aimed at stealing login credentials or be designed to trick a user into clicking a link that leads to deploying a payload of malware on the victim’s network. Once one or more users within an organization fall prey to an orchestrated phishing campaign, the attackers will have culled credentials or delivered a malware payload needed to launch their full-scale attack.

There is a wide variety of attack types that begin with a phishing campaign. The hacker’s objective may be to steal credentials and other personally identifiable information (PII) that they can then sell on the dark web, download the malware for a ransomware attack, or steal valuable information as part of an industrial or military espionage campaign.

Nation-states and state-sponsored advanced persistent threat (APT) actors use phishing to gain a presence on the victim’s network to begin privilege escalation that can eventually severely compromise our nation’s critical infrastructure or financial institutions.

type.

In addition to what we might think of as common phishing that is focused on everyday computer and network users, there is spear phishing, whale phishing, and smishing.

Spear Phishing

Unlike common phishing scams where hackers use a wide-reaching net to reel in the largest possible number of potential victims, spear phishing attacks are more focused. Spear phishing thieves generally target members of a particular group. It could be employees of an aerospace company on which the attackers have set their sights or students, staff, or the faculty of a targeted university.

The success rate of spear phishing is much higher than that of common broadcast phishing but also requires the hackers to invest time and resources into doing some pre-attack research. The more they can learn about their target, the more likely they are to be successful.

Whale phishing is similar to spear phishing, with a few notable differences. While spear phishing is generally aimed at members of a group, whale phishing is focused on a specific individual—usually the “biggest phish” at the target organization or an individual with significant wealth or power that the attackers wish to leverage.

Whale phishing also requires an extraordinary amount of pre-attack research. Attackers can spend months, if not years, learning about and grooming a whale. The ne’er-do-wells will learn everything they can from social media and other public sources about their target. Sometimes criminals spear phish lesser marks to gain additional intelligence about their whale target.

Smishing

The term smishing derives from SMS phishing. It is phishing that involves a text message rather than email. Victims typically receive a deceptive text message to lure the recipient into providing their personal or financial information. Scammers attempt to disguise themselves as a government

Ukraine power grid cyberattack

In what is considered to be the first successful cyberattack against an electrical power grid, the Ukrainian power grid was knocked offline in a 2015 attack that began with phishing.

That attack, thought to have been launched by a Russian advanced persistent threat group known as Sandworm, was initiated with a spear phishing ruse that dumped a payload of BlackEnergy malware onto the SCADA system that controls Ukraine's power grid. The resulting distributed denial of service (DDoS) attack left large parts of Ukraine without power for about six hours. More than two months after the attack, power grid control centers were still not fully operational.

Facebook and Google

In one of the most expensive phishing attacks ever, a Lithuanian hacker sent a series of fake invoices designed to look like they came from Quanta Computer—a Taiwanese electronics manufacturer—to Facebook and Google between 2013 and 2015. Both companies regularly did business with Quanta, Reported in 2016, this whale phishing attack targeted a high-level executive at Belgium-based Crelan Bank with instructions to immediately send approximately $75.8 million to an account controlled by the attacker. Details are scarce, but the victim complied with the fraudulent request, and the money was lost.

This flavor of whale phishing or business email compromise (BEC) scam is sometimes called CEO Fraud and is often targeted toward small to mid-sized companies that may not have adequate controls in place to prevent this type of fraud. An Austrian manufacturing company called FACC was hit with a similar attack, losing nearly $60 million.

UC San Diego Health

In July 2021, UC San Diego Health disclosed a data breach after attackers hijacked employee email accounts in a spear phishing attack. The school's data breach notification page says that unauthorized access is likely to have occurred between December 2, 2020, and April 8, 2021.

a major bank or other institution then send the email to hundreds of thousands of email addresses. Only a percentage of the recipients will be customers of the spoofed company, but it cost the hackers nothing to play the numbers game. They know that even if only a small percentage of the recipients are customers and only a tiny fraction of those people fall for the scam, they still come out on top.

Common phishing ploys include stating in an email that they have noticed some suspicious activity or login attempts—telling the potential victim to follow a link in the email to remedy the situation. Most of these low-budget scams are easy to detect. There will be misspellings or language that is not consistent with a business email. The address from which the email is sent can often be identified as not belonging to the company that purports to have sent it.

Low-budget mass email scams are often targeted toward senior citizens who may not know how to detect obvious clues indicating a phishing scam. An example of an easy to detect sender email address is BankofAmerica@gmail.com. To anyone familiar with email address formats and business email practices, it should be evident that Bank of America does not use a Gmail account for customer email. If a company asks you to interact with them on their website, type the company's known URL directly into your browser rather than use a link from an email.

Email spam filters are an effective—but not foolproof—tool for protecting against low-budget phishing attacks.

A spam filtering solution integrated with your email platform uses a set of rules to determine which of your incoming messages are spam and which are legitimate. The several types of spam filters include content filters, header filters, blacklist filters, permission filters, and challenge-response filters. Each applies a different set of rules to your incoming emails and can be beneficial in detecting phishing scams.

Cyber threat actors are always finding new and innovative ways to bypass spam filters to trick email or SMS users, enabling them to steal sensitive information or deliver destructive payloads. Beyond spam filters, there are steps that users should take to avoid becoming a victim of a phishing attack.

Conclusion

Phishing is but a modern twist to any number of age-old ploys to trick people into giving up information that can be used against them. From eavesdropping to mail tampering, criminals have always sought to steal information as a precursor to launching other exploits.

As it has always been, each individual must shoulder the responsibility to protect themselves from trickery and deception. There are software tools, such as spam filters and antivirus software, that can help, but in the end, we must all be ever-diligent and even a little suspicious of email and SMS communications.

PROGRAMS BY STATE CERTIFICATIONS DEGREES ONLINE PROGRAMS CAREER GUIDES

EXPERTS RESOURCE CENTER INDUSTRIES

Security Engineer
Chief Information Security Officer
Security Analyst
Computer Forensics
Security Consultant
Digital Forensics
Cryptographer
Security Administrator
Penetration Tester
Security Software Developer
Security Specialist
Security Code Auditor
Security Architect
Malware Analyst
Data Protection Officer
Cybercrime Investigator

Internship Guide
Security Clearance Guide
Ethical Hacker Guide
Coding for Cybersecurity Guide
Cybersecurity 101
Student Guide to Internet Safety
Scholarship Guide
Cybersecurity Math Guide
Small Business Guide
COVID-19 Guide
Cybersecurity for K-12 Students
Career Networking Guide
What is a Cyber Range?
Code Like a Hacker
Reacting to a Cyber Incident
Introduction to Cyber Defense

Healthcare Sector
Environmental Sector
Energy Sector
Government Sector
Transportation Sector
Food and Agriculture Sector