

What Is Phishing in Cyber Security, and How Can Businesses Combat It?

ARTICLE 03.24.22 DEAN DORTON

It's a common occurrence that most — if not all of us — have experienced at some point: an email lands in your inbox with an urgent request for immediate action. Perhaps it appears to be from your bank or credit card company. And if you don't click to respond **now**? Your account could be frozen. Or worse, you could face financial ruin.

What the cyber criminals behind phishing attacks like this and others have known for years is that people can be susceptible to emotional motivators ... such as curiosity or even fear. When people act emotionally, they're more likely to make mistakes. They take the bait. They click. And they inadvertently surrender information that can endanger their identity, their finances, or their organization, with potentially devastating results.

Preying on that human element, cyber criminals continue to hone their phishing attacks on individuals as their gateway to businesses across every industry, improving in sophistication, stealth, and deception every day.

They also continue to explore fresh waters for their phishing expeditions as well — such as those surrounding COVID-19. In fact, as confusion about vaccinations, booster shots, and the new Delta variant swept across the world this past June, [pandemic-related phishing attempts jumped 33%](#) over the spring.

Couple the emotional motivators with the prevalence of remote workers connecting more devices to servers with subpar cyber security measures in place, and cyber criminals are knee-deep in highly attractive targets to phish.

So what exactly is phishing in cyber security, how can you recognize it and, more importantly, what can you do to prevent it?

What Is Phishing?

Phishing is a type of [social engineering](#) attack that attempts to lure unsuspecting victims into divulging sensitive personal or organizational information.

Posing as a trusted source, cyber attackers use **email**, **phone**, or **text messages** to dangle the bait and acquire things like credit card information, social security numbers, passwords, and other login credentials. Once the victim clicks a link, they can be directed to what appears to be a legitimate site where sensitive information can be compromised — or malware can be installed.

Originating some time in the mid-1990s, phishing remains one of the cheapest and easiest methods of cyber attack today. Why? Because people are much more vulnerable than technology. While organizations can put early warning security systems in place to cut down on some of the attacks, people still make mistakes.

Once characterized by poorly written and even laughable emails easily identified as a scam, phishing attacks have evolved into sophisticated click bait. So much so that more than [25% of workers](#) still fall for phishing scams. And smaller organizations with fewer than 250 employees see a higher rate of phishing attack, with [approximately one in every 323 emails being malicious](#).

Common Types of Phishing Attacks

As technologies advance, this type of attack continues to exploit vulnerabilities. Here are 10 types of the most common phishing attacks every organization should be aware of:

- **Email phishing:** Perhaps the most widely known type of phishing attack, emails appear to come from a reliable source or reputable organization. Some of the more sophisticated email phishing scams (also called Clone Phishing) even use recognized addresses that are easier to trust and open, along with some urgent language. The spoofed email will contain one or more links that lead to false websites where the damage can be done.

- **Vishing (Voice phishing):** The combination of Voice over IP ([VoIP](#)) with phishing, this attack involves a call from a bad actor enticing the victim to divulge sensitive information.
- **Smishing (SMS phishing):** With smartphone users in their sites, smishing attackers can deliver malicious short links. With the popularity of SMS from legitimate sources like banks, retailers, and political parties, cyber criminals understand that [about 98% of SMS messages](#) are read within seconds of being received.
- **Spear phishing:** Rather than cast a wide net to hit on random targets, spear fishing targets a specific person or organization with something in common. It's a rising, more involved cyber attack that allows the attacker to create a more customized scam with insider information of that individual or the company, and can come in the form of an email, phone call, or SMS.
- **Session hijacking:** Also known as TCP session hijacking, this method involves taking over a web user session by disguising the cyber criminal as the authorized user. Once accessed, the attacker can masquerade as that user and gain access to a server without having to provide authentication.
- **Malvertising (Malicious Advertising):** A relatively new type of phishing attack where a third-party server is breached by the criminal, malvertising injects a malicious code inside digital advertising. It's difficult to detect by users and hosts of sites, and because the digital ads are displayed to every visitor, virtually every page viewer is at risk of infection.
- **Content injection:** Also known as Content Spoofing, attackers target unsuspecting website users via a "text injection" in the web application. Unbeknownst to the user, this provides a modified page disguised as the trusted domain they intended to visit. Most often, content injection goes hand in hand with social engineering because it relies on the trust of the user.
- **MitM attack:** Here, cyber criminals insert themselves in between two legitimately communicating hosts to distribute malware that gives the cyber criminal access to a user's browser and the data it sends. Once in control, the attacker can redirect users to a fake site that looks like the intended site where they can steal or modify information.
- **Pharming:** Victims of this attack are rerouted from the legitimate site they intended to visit to a fake page that closely resembles the real site. Also known as DNS poisoning, pharming is a two-step process where an attacker first installs malicious code on a victim's computer or server. Once on the spoofed website, they may be tricked into offering personal data or credentials. This technique does not require a user to open a website themselves: they're automatically redirected to the fake site.
- **Whaling:** Aimed at the "big fish" in the executive suite of an organization with access to significantly sensitive corporate info, whaling is a highly-targeted attack that involves more sophisticated social engineering tactics. Often launched via emails, they can contain personal information, detailed business verbiage, and a compelling reason for the victim to act. While many organizations train all levels of employees on how to recognize phishing emails, C-suite execs can occasionally be a softer target when inundated with emails and other priorities that allow the whaling email to land.

10 Ways to Spot a Phishing Attempt

The first line of defense against a phishing attack is knowing and heeding the warning signs. While the technologies cyber criminals use to launch these attacks continue to evolve, there are still tell-tale clues that can help your organization avoid the dangers, including:

1. **There's an unusual sense of urgency or attempt to invoke fear.** A legitimate communication from any reputable organization does not display an air of desperation to entice you to act. Undue urgency in a communication is quite possibly the reddest of all red flags.
2. **The source of the email is a Gmail or non-corporate email account.** Cyber criminals also often use an email address that closely resembles one from a reputable company by altering or omitting a few characters.
3. **You're addressed generically and not by name.** Anything that leads with "Dear Valued Customer" or "Sir/Ma'am" along with a lack of contact information in the signature block are strong indicators of a phishing email.
4. **You're requested to confirm credentials or personal information.** Businesses rarely (if ever) make this request without confirming your identity. Regardless, be sure to double check the URL, and look for the green lock in the browser to see if it's a secure site before entering information.
5. **The email or website is poorly written.** If it's riddled with grammatical mistakes and poor sentence structure, it's probably a hoax.

6. **The website is poorly designed.** Legitimate companies invest heavily in the branding and display of their communications and their site. Spoofed sites only appear to be put together well, and often hit you with a **pop-up window** asking for details the minute you land on them.
7. **You discover spoofed hyperlinks.** These can be found by hovering over any links in the body of the email. If the links don't match the text that appears when hovering over them, the link may be spoofed.
8. **Pop-ups appear.** If it's a site you visit regularly and you're suddenly prompted for a login is highly suspicious. Legitimate login requests will have a security certificate that matches the URL of the site.
9. **The message comes with suspicious attachments.** An unsolicited email requesting a user download and open an attachment is a common malware delivery mechanism. Best to delete it and move on.
10. **The message seems too good to be true.** The thing to keep in mind is this: phishing — and social engineering in general — simply works. It has for decades. Virtually everyone today has an email address where they send and receive significant numbers of emails, access business servers from **unsecured networks**, or surf social media sites that can all make them susceptible to manipulative phishing attacks.

Protecting yourself and your organization from these cyberattacks is a group effort that requires vigilance and constant communication.

Steps to Prevent Phishing Attacks

Because phishing attacks target human negligence, indifference, or error, there's no way to guarantee 100% protection from a scam. But there are steps you can take to make your organization a more difficult target.

In our recent [cyber security FAQ post](#) we cover several best practices that can give your company a solid cyber security posture to mitigate risk and be prepared to act in the event of an attack. Some of these include:

- **Performing company-wide education and ongoing training:** A crucial step for everyone from the C-suite down to interns who have access to your network. Help identify signs of an attack, spoof websites, and conduct mock phishing scenarios multiple times a year. Develop security measures that include elements like password expiration and complexity, with a “think before you click” policy.
- **Installing antivirus software, email, and spam filters:** Reduce vulnerabilities with key technologies and software that can catch many phishing attacks before they happen.
- **Incorporating phishing filters:** Together with antivirus software, phishing software can help prevent malicious attacks on your computers and computer networks that anti-virus software alone could miss.
- **Updating software apps:** Staying current on software is key. Updates will add new features, fix known bugs, and upgrade security.
- **Implementing two-factor authentication:** One of the most effective tools to counter a phishing attack. Many platforms today allow for this extra layer of protection to require a second piece of information beyond username and password to verify who is accessing accounts.
- **Installing a firewall:** A necessary part of any cyber security architecture. On its most basic level, a firewall is the barrier between a private internal network and the public Internet. It's main purpose is to focus on blocking malware and application-layer attacks, allowing non-threatening traffic in and to keep dangerous traffic out.
- **Staying informed:** New phishing attacks are being developed every day. [In 2020, nearly 7 million new phishing and scam pages were created](#), with 206,310 new phishing scam sites created in one month alone. Stay in the loop about recent attacks, test your people often, and encourage them to think critically of what they're being asked to do.

Don't Take the Phishing Bait

Phishing attacks are one of the most common security challenges that individuals and companies alike face today. Cyber criminals continue to enhance their methods, probing for new opportunities to exploit world events, emotional triggers, and uninformed users to wreak havoc on bottom lines and — perhaps even more damaging — business reputation.

Despite best efforts and top technologies and software that organizations can put in place, true mitigation of phishing attacks relies heavily on the people behind the devices. So it stands to reason that, along with other available precautions, an excellent policy to help minimize those vulnerabilities is helping others operate with a healthy measure

of skepticism.

While we've touched on some of the basics about phishing threats out there today and a few steps you can take to safeguard against them, phishing attacks require ongoing vigilance and attention. Safeguard your critical information — and your reputation. Connect with Dean Dorton for a cyber security risk assessment today.

And for more insights and analysis on trends and cyber security solutions, be sure to subscribe to our blog.