Phishing: The Most Common Form of Cybercrime

By: Carter Wakefield

Executive Summary

- What is Phishing?
- Why's Phishing the Biggest Cybercrime?
- How and Why Phishing Works?
- Effects of Phishing
- Most Common Types of Phishing
- How to Defend Against Phishing
- Summary

Phishing: The Most Common Form of Cybercrime

With the rise of the digital era, cybercrime plagues the World Wide Web, but there is one crime that tops them all as the most used and abused cybercrime: phishing. Phishing has solidified its name as the most common cyberattack in the world, with an “estimated 3.4 billion phishing emails sent every day”(Griffiths, 2025). Phishing is a type of cybercrime in which an attacker pretends to be someone to manipulate victims into giving out information. They often pretend to be companies, businesses, and actual people, so it can be really hard to determine who is real or fake. Phishing is so common because there are so many different types of phishing, and they target all different types of people. The types of phishing include various forms such as email phishing, spear phishing, whaling, smishing, vishing, clone phishing, quishing, and many more. Phishing works because of deception and manipulation; by masking their true intent and identity, they are easily able to compromise even the most secure businesses and companies. Attackers are usually after things such as financial information, personal information, accounts/passwords, and access to restricted areas/systems.

A basic phishing attack occurs in the following sequence. First, an attacker will select a target to go after, then they develop a convincing fake message to manipulate their target. Then the victim will receive the decoy message. The victim is typically then required to complete some task, like pay a toll, click a link, or provide some sort of information. The victim does what the fake messages say, and the attacker now has access to stolen information/unauthorized systems.

Phishing is effective because, attackers like to use trusted and familiar companies, because people are more likely to fall into their trap. The attackers also tend to create a sense of urgency to throw off their victims. The messages that these attackers use are also very convincing. Some of the more clever attacks also use information about the victims to deceive them. All these factors combined, it can be hard to determine the fake from the real.

Phishing attacks are the most common type of attack because of the variety and ease of the attack. Billions of phishing attacks are sent out daily, and with the rise of AI, these numbers are only rising. It was stated that, “3.4 billion phishing emails sent daily; 82.6% are AI-generated” (Keepnet/VIPRE). Almost every organization is targeted by various phishing attacks. Organizations and businesses such as Google, Facebook, the Colonial Pipeline, Elara Caring Health Care, Levitas Capital, USPS, Spectrum Health, the U.S. Interior Department, and Crelan Bank are among some of the many big names that have suffered massive losses due to phishing attacks. In the early days of phishing attacks, it started as poorly made mass spam mail, messages, and calls, and over time it has evolved and automated into AI-backed operations that pump out countless attacks a day. As technology keeps advancing, so do phishing attacks, and it's becoming harder and harder to defend against.

Phishing has remained so popular because of its ease of use and because it has proven to be quite profitable. It was stated that one whaling attack focused on high-profile targets can cost a business over 40 million USD in damages. It was reported that, ”phishing still causes an average of $4.88 million in breach costs per incident” (IBM 2025). This doesn’t even include the damages from fraud as a result of phishing. A successful phishing attack can give an attacker access to bank accounts, payments, personal information, and more. With every breach, damages are costly; millions are needed to recover from phishing attacks.

Phishing attacks are so common because literally anyone can be targeted. Individuals are targeted because they are easier and faster to pump out attacks, allowing for quick and fast results. Businesses are targeted more carefully because they contain sensitive intel, employee info, and essential company data; targeting larger businesses are essential for obtaining huge payouts. The elderly and young people are primary targets for attackers because they are less tech-savvy and are easier to manipulate, making them easy targets. Lastly, the military and government are targeted because they contain valuable classified intelligence, critical infrastructure systems, and serve as the highest payout and can be used for espionage and

disruption of services. A lot of state-sponsored phishing attacks often target military and government agencies.

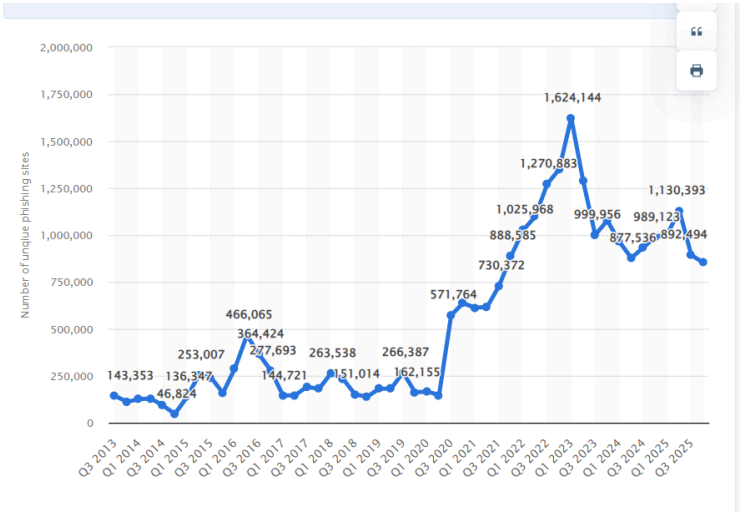
As we know, phishing is a deceptive attack that seeks to trick its victims, but it can come in many forms. The most common are email phishing, spear phishing, smishing, and vishing. Email phishing is one of the simplest and most common forms of phishing; it's a fake email that appears to trick the victims. For example, a fake Amazon email demanding you change your password (giving them your account access). Spear phishing is a type of phishing that targets a specific organization or person who is of high value/profile. Smishing is a common attack that most people have probably seen as a phishing attack through text. This can be a text requesting to change your address or a text telling you to pay a toll. Vishing is a phishing attack that is executed through phone calls. This can be a call about your car's extended warranty or a crazy loan approval. This is what makes phishing so dangerous: it disguises itself in every aspect of technology.

Phishing started off as a simple, easy-to-spot email scam; then throughout time evolved into websites, then with the evolution of social media, then text, then mobile devices, and lastly AI. It has come so far and has plagued every part of the World Wide Web, making it increasingly harder to determine what is real and what is a phishing scam.

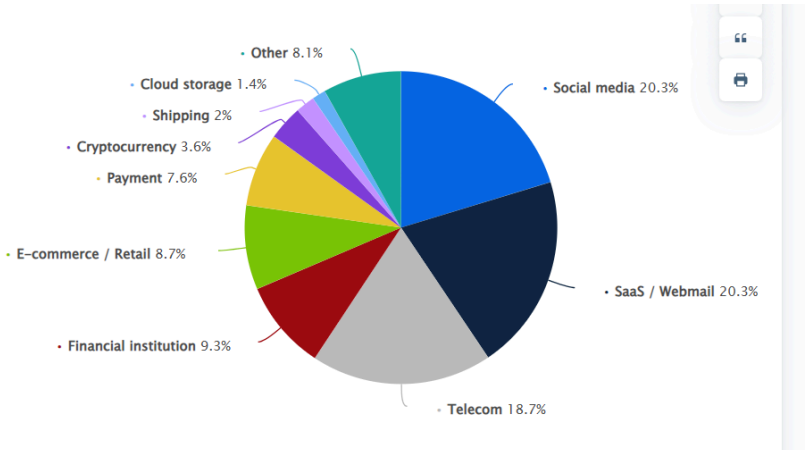
Phishing is one of those attacks that you can't seem to get rid of. Professionals struggle to find counters because methods are always changing and evolving. The hardest aspect of protecting against phishing is the human factor; humans are the leading cause of cyberattacks. We can do all the cyberawareness training and keep bringing attention to phishing, but it won't put a stop to the attacks. Attackers have always been hard to detect because they mimic websites and organizations, so it can be almost impossible to tell the difference. With the advancement of AI, phishing scams have and will continue to get harder and harder to detect.

However, Organizations are still providing a solid fighting effort in attempts to decrease the effectiveness of phishing. Employee cyber awareness training is the biggest and most

effective counter to phishing, because it helps educate employees on all kinds of attacks and how to spot the early signs of an attack before it escalates. This awareness training should be done at least annually to ensure readiness and awareness for all employees. Increased security measures such as 2FA, email filtering, security systems, and more are also making moves at fending off against the ever growing threat of phishing. In all, the best way to fight phishing is to stay up to date on all updates, training, and readily updating credentials.



The following chart showcases the Number of phishing attacks detected worldwide from the 3rd quarter of 2013 to the 4th quarter of 2025. This graph only showcases "detected" attacks, so the true number of attacks is likely much higher. On average in recent years, every 3 months there are at least 800k reported phishing attacks, thus resulting in around 3,200,000 reported phishing attacks a year. This statistic really showcases the sheer size of phishing attacks.



The following chart showcases the distribution of industries most targeted by phishing attacks worldwide in the 4th quarter of 2025. It breaks down the most targeted industries, allowing us to identify the industries that require more attention when it comes to protecting against phishing. Given the information provided, we can better prevent future phishing attacks.

With the information stated previously, it is clear that phishing is no joke and is an ever-evolving threat that targets anyone and everyone. There are things you can do to counter it. To start, individuals such as you and I can counter phishing threats in a few ways. First and most importantly, be paranoid; don't trust unknown messengers. Be careful when clicking links, emails, and text messages. Secondly, strengthen credentials; this starts with developing strong passwords, and changing passwords regularly can help counter phishing. Using 2FA is also essential because it acts as a secondary defense if your credentials get compromised. Lastly, trust your gut, and if something feels wrong, don’t interact with it. You need to be able to weed out what's real and fake. Don't be scared to report suspicious activity because the only way phishing will be stopped is if you do your part and report it. For example, using these methods, I was able to stop a phishing attack back in 2023. I was talking to a buddy of mine in 29 Palms, California, and he was on his phone and got a text stating there was a problem with his package that was “urgent”. I had gotten the same text previously and could tell it was a scam. He started clicking the link, and I had to frantically stop him before he entered his information into the fake

website. In the end, it was a good lesson, and I was able to educate him on how to identify a phishing scam and the importance of looking twice before acting.

Businesses have their own actions they must take to prevent phishing. First and most importantly, they must mandate annual cyber awareness training. As stated before, humans are the primary cause of all cyberattacks, so it's important to understand phishing and how to counter it. Secondly, businesses need to establish a solid security policy that includes a firm guidance for use of services, as well as a solid report system to ensure the safety of the company and its assets. These security policies also need to implement an incident response plan to assist employees with resolving and mitigating company losses. Lastly, businesses need to regulate emails consistently and establish filters to prevent any attacks from targeting employees.

The government also has its own role in ending phishing. The government is responsible for providing public cyber awareness aid to ensure the everyday Joe is kept up to date on all the knowledge they need to protect themselves. They are also responsible for assisting in disaster recovery through forensic cyber investigations; this ensures we understand our enemy and are better able to prevent future phishing attacks. The government needs to evaluate the World Wide Web and develop guidelines for defenses to assist private and public sectors in the war against phishing.

The future of phishing is unknown; it is constantly advancing and changing. The fear of the unknown haunts professionals daily. With the advancement of AI, phishing becomes more and more convincing by the day. Whether it's deepfakes, fake calls, or personal chatter phishing scams, it just keeps becoming more and more convincing, tricking the smartest of people. The only way to combat the ever-growing threat is for society to institutionalize cyber awareness training in the workplace, education, and personal life.

Overall, phishing is a type of cybercrime in which an attacker pretends to be someone to manipulate people into giving out information. Social engineering is a technical term for how

criminals manipulate people into carrying out tasks. As a collective whole, things such as filtering spam, enabling 2FA, and blocking suspicious messages will prevent phishing but won't end it. In order to combat the ever-growing and advancing threat of phishing, we must, as a collective society, actively educate ourselves on cyber awareness and react to all situations with readiness and care in order to reduce the chance of making mistakes. If we as a society can develop better security, better cyber awareness, and faster reporting, we can put a halt to the threat of phishing.

Glossary

Phishing - a type of cybercrime in which an attacker pretends to be someone(uses deception) in order to manipulate people into giving out information.

Social engineering - how criminals manipulate people into carrying out tasks.

2FA - a security method that requires an individual to provide 2 or more forms of authentication to grant access to said account/system.

Email phishing - fake emails that appear to trick the victims.

Spear phishing - a type of cybercrime that targets a specific organization or person who is of high value/profile

Smishing - phishing attack executed through text.

Vishing - phishing attack that is executed through phone calls/voice

Clone phishing - phishing attack in which an attacker poses as a legitimate trusted website, company, business, etc.

Quishing - phishing attack executed through QR codes

Citations

8 devastating phishing attack examples and prevention tips. (n.d.). *BlueVoyant*. https://www.bluevoyant.com/knowledge-center/8-devastating-phishing-attack-examples-and-prevention-tips

Global cybersecurity incidents consequences. (n.d.). *Statista*. https://www.statista.com/statistics/1622365/global-cybersecurity-incidents-consequences/

Number of phishing attacks worldwide. (n.d.). *Statista*. https://www.statista.com/statistics/266155/number-of-phishing-attacks-worldwide/

Phishing statistics. (n.d.). *StationX*. https://app.stationx.net/articles/phishing-statistics

Phishing statistics 2026. (n.d.). *CNIC Solutions*. https://cnicsolutions.com/statistics/phishing/phishing-statistics-2026/

The latest phishing statistics. (n.d.). *AAG IT Services*. https://aag-it.com/the-latest-phishing-statistics/

The true cost of phishing attacks. (n.d.). *Kaseya*. https://www.kaseya.com/blog/the-true-cost-of-phishing-attacks/

Websites most affected by phishing. (n.d.). *Statista*. https://www.statista.com/statistics/266161/websites-most-affected-by-phishing/

Why governments and agencies are targeted by cyber attacks: A deep dive into the motives. (n.d.). *SentinelOne*. https://www.sentinelone.com/blog/why-governments-and-agencies-are-targeted-by-cyber-attacks-a-deep-dive-into-the-motives/