WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Phishing Attacks and Their Prevention Techniques

PATEL KRUTARTH BHAVANBHAI [1], PATEL JANKI NILESHBHAI[2], PATEL RONAK BIPINBHAI [3] , PROF. VIJAYSINH JADEJA[4]

[1] SAL COLLEGE OF ENGINEERING
[2] DEPARTMENT OF ENGINEERING
[3] AHMEDABAD,GUJARAT,INDIA

ABSTRACT :

Phishing is one of the oldest and most dangerous types of online crime. It is a way to fool people into giving up personal information like their usernames, passwords, and credit card numbers. This paper talks about how phishing attacks work and how they have changed over time, as well as the most common ways attackers use them and how to stop them. It talks more about how AI can help find phishing attacks and the problems that will come up in the future when trying to stop them.

Phishing attacks have come a long way since they were easy-to-spot scams. Now they use fake websites, emails that look like they came from a professional, and even content made by AI. These people target people, businesses, big companies, government agencies, and even famous business leaders. This can cause them to lose money, have their identity stolen, damage their reputation, and have private information leaked.

This paper talks about the different types of phishing attacks, such as email phishing, spear phishing, whaling, smishing, and vishing. It also talks about how hackers trick people into falling for phishing attacks. It also talks about the mental things that make phishing work and what happens when someone falls for it.

1. Introduction

Since the digital age began, people have come to depend on email, social media, and online banking a lot. Unfortunately, the internet has made cybercrime a real threat. Phishing is one of the most common and profitable ways to commit cybercrime.

Phishing is when a hacker pretends to be a trusted group, like a bank, business, or government agency, to get people to give them private information. Phishing can result in identity theft, monetary loss, and a breach of privacy. Phishing is one of the biggest problems with cybersecurity in the world because it keeps changing as technology gets better. Attackers use social engineering to make messages and websites look real. For example, they might play on people's emotions, like fear, urgency, curiosity, or greed. This means that even someone who knows a little about cybersecurity can fall for phishing if they're not careful.

Phishing attacks can be very bad for you. People can have their identity stolen, have their bank accounts accessed without their permission, lose money, or have their private information made public. Data breaches, fines, and damage to an institution's reputation are all possible, and these things can have effects that last for a long time. Today, attackers use sophisticated techniques like professionally designed email templates, fake websites that look like real ones, automated phishing, and even AI-based messages that are almost impossible to tell apart from real messages. The threat is always there and getting worse because phishing is always getting better.

2. Evolution of Phishing Attacks

In the middle of the 1990s, bad people started phishing by making fake AOL log-in pages to get people's login information. It was easy to see the attacks back then, and they weren't very hard to figure out. But the ways that people do phishing have changed over time.

Phishers today have well-designed websites, believable messages, and even AI-powered tools that make the messages sound completely real. Phishing isn't just done through email, text messages, social media, and phone calls anymore. They use AI, big data, and automation to find and choose targets more quickly and easily.

3. Common Techniques Used by Attackers

Phishing attacks can take many forms, so the first step in stopping them is to know what they look like.

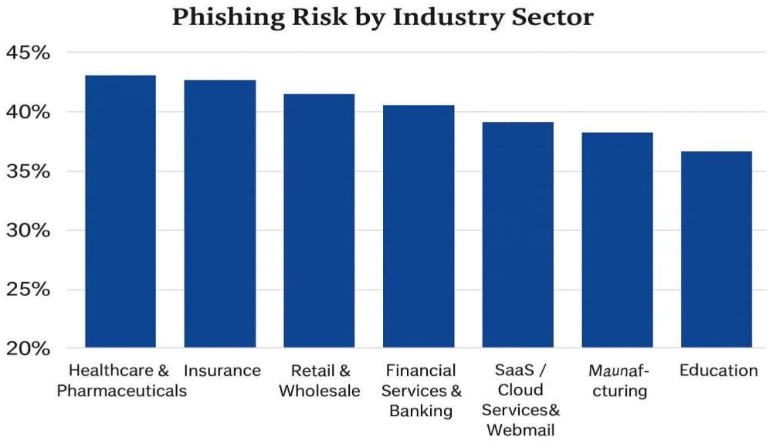
1. Email phishing: Fake emails that seem to come from a bank, an online store, or the government.
2. Spear phishing: This type of phishing tries to look more trustworthy by using personal information to target specific people or groups.
3. Whaling: Attacks on famous people or groups, like CEOs or high-ranking government officials.
4. Smishing and vishing: Phishing through text messages (smishing) or phone calls (vishing).
5. Clone Phishing: They take a real message and change the links to bad ones.

4. Phishing activities trends report :

Phishing activity went up again. There were 1,003,924 phishing attacks in the first quarter of 2024. This is a big jump from the 963,994 attacks in the first quarter of 2023. Since the fourth quarter of 2023, this was the highest level for a quarter. The number of attacks went up again, reaching 1,130,393. This is a 13% increase from the first quarter of 2025 and the highest level in a quarter since the second quarter of 2023.

	August	**September**	**October**
Number of unique phishing web site (attack) detected	361,578	376,071	383424
Unique Phishing email campaigns	59037	28509	48550
Number of brands targeted by phishing campaigns	331	349	324

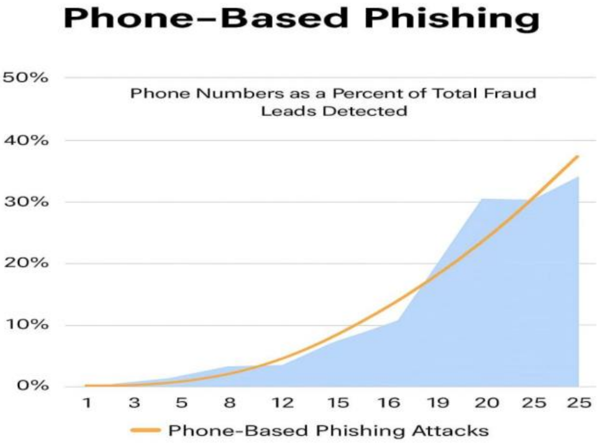
Most-Targeted Industry Sectors:-



The Anti-Phishing Working Group (APWG) Phishing Activity Trends Reports for the first and second quarters of 2025 say that phishing attacks still targeted most industries, with the financial sectors being the most affected. Banks and payment services were the most common targets for phishing in the first quarter of 2025, making up 30.9% of all phishing activity. That number went down a little to 18.3% in the second quarter of 2025, but the financial sector was still the most targeted. SaaS and webmail services were also the targets of a lot of phishing. They were responsible for 17.6% of all phishing activity in Q1 and 18.2% in Q2. In the second quarter, 14.8% of attacks were on retail and e-commerce sites, and 12.1% were on payment services. 11.3% of attacks were on social networking sites, making them the most common target. Next were telecom companies with 4%, shipping and logistics with 3.9%, and the cryptocurrency market with 2.7%.

There were some important patterns in the APWG reports. Attacks on banks and other financial institutions rose a lot, from 11.9% in the fourth quarter of 2024 to 18.3% in the second quarter of 2025. This shows that attackers are now going after things that have to do with money. Attackers are going after more things, like parking meters, public utilities, and automated collection booths. QR-code phishing is getting more and more risky. In the second quarter of 2025, 1,642 brands were attacked, with DHL and Microsoft being the most common. There were also a lot more attacks that compromised business email (BEC). In the first quarter of 2025, wire transfer attacks rose by 33% compared to the previous quarter. The average request amount in the second quarter of 2025 was $83,099, which is a huge 97% increase from the previous quarter. These show that attackers are getting better at what they do, and all businesses need strong cybersecurity, such as multi-layered defense, user education, and constant monitoring, to stop this threat from becoming real.

Phone-Based Phishing :



Phone phishing, which is also called "smishing" when done through text messages and "vishing" when done through voice calls, is a type of social engineering attack that is growing quickly. It uses people's trust in mobile phones to get them to share private information, install harmful software, or send money. Thieves send fake texts with links to fake login pages or harmful apps, or they call people and pretend to be from banks, the government, or job sites to scare them and steal their personal information. They also use QR codes, which are sometimes called "quishing," to get people to visit phishing sites on their phones. The Anti-Phishing Working Group (APWG) and security researchers have put out reports that show a big rise in phishing over the phone and on mobile devices. APWG's trend reports from 2025 say that millions of people are being phished through QR codes and mobile communication channels. Other studies and reports from the industry back this up by showing that both smishing and vishing are getting much worse every year. ([docs.apwg.org] [1]

5. Psychological Factors Behind Phishing

Phishing works because it plays on people's feelings, not because of any technical problems. People who write messages make them sound scary, important, greedy, or interested.

An email that says your bank account will be closed unless you respond right away makes you respond too soon without checking where it came from. People get curious and greedy when they get reward/refund emails that promise something for free. By learning these psychological tricks, people can be more careful and stay away from scams.

6. Prevention Techniques

Technology and people can both help stop phishing. Here are some general ways to stop it:

User Education: Regular training and awareness campaigns to help people spot links and messages that could be harmful.

Two-Factor Authentication (2FA) makes your account even safer, even if someone gets your password.

Email gateways that are safe: Look for any signs of bad behavior in the messages and attachments.

Anti-Phishing Toolbars: These are add-ons that show up when someone goes to a phishing site.

Routine software patching protects the system from known problems.

Look at the URL: Before giving a site any personal information, always check its address.

Role of Artificial Intelligence in Phishing Detection

AI and ML are advanced tools that help you spot phishing attempts. AI programs can look at a lot of websites and emails to find strange patterns and automatically find phishing material.

For instance, machine learning systems can find the tone, structure, or links in phishing messages and warn people before they happen. AI systems can also find new bad websites, which stops people from going to ones that are dangerous. These technologies are very important for modern cybersecurity solutions because they keep getting better as they handle more data.

Future Trends and Challenges

Phishing gets smarter as technology gets better. In the future, phishers might try to trick people with deepfake videos, AI-generated voices, and text messages that are very personalized.

Another threat is social engineering. When attackers watch what their victims do online to come up with believable messages, this is what happens. To fight these kinds of threats, cybersecurity experts are making tools to watch people's behavior, better AI filters, and programs to raise awareness around the world. Governments and businesses that make laws need to work together to make cybersecurity laws and rules stronger.

Conclusion

PPhishing attacks are still one of the most common and newest types of cyberattacks. They go after people, businesses, and important areas like banking, e-commerce, SaaS platforms, and social media. The attacks trick people into giving up sensitive information, credentials, or money by making them feel like they need to act quickly or pretending to be someone else. Smishing, vishing, QR code phishing, and BEC are all growing, which shows that attackers are getting better at getting past traditional defenses. Using a mix of technical, organizational, and behavioral controls is the best way to stop something from happening. Companies can use email and web filtering, anti-phishing tools, and multi-factor authentication that can't be hacked as part of their multi-layered security systems. Workers need regular training and awareness programs to help them recognize emails, calls, and messages that seem fishy. Independent checks of financial transactions and alerts when phishing is suspected can help lower the risk even more. You need a mix of technology, education, and being careful to keep sensitive information safe from being misused and to lessen the effects of phishing attacks.

REFERENCES

1. Jagatic, T. N., et al. (2007). Social Phishing. Communications of the ACM.
2. APWG Phishing Activity Trends Report (2023). Anti-Phishing Working Group.
3. Hong, J. (2012). The State of Phishing Attacks. Communications of the ACM.

4. Symantec Internet Security Threat Report (2024).

5. Kumar, A., & Singh, R. (2022). AI Techniques for Phishing Detection. Journal of Cybersecurity Studies.

6. Fortra. (2025). Recapping APWG Phishing Activity Trends Report Q1 2025. [https://www.fortra.com]

7. Yubico. (2025). Phishing Email Recognition and Human Interaction Survey. [https://www.yubico.com]

8. Kaspersky. (2025). AI-Powered Phishing Attacks Are on the Rise. [https://www.kaspersky.com]

9. Check Point Research. (2025). Credential Theft and Phishing Trends Report. [https://www.checkpoint.com]

10. Microsoft Security Blog. (2025). Disruption of Phishing Subscription Services in 2025. [https://www.microsoft.com/security/blog]