Jessi Frenzel
CS 373
Final Presentation
8/13/25

Phishing Attacks [Transcript]

Intro

This is Jessi Frenzel, for CS 373 and today I'll be talking about phishing attacks.

Phishing

Despite being around for decades, phishing attacks persist as a surefire way to get people to fall prey to cyber attacks.

What's Phishing?

Phishing is a deceptive process whereby an attacker manipulates someone into giving up personal information or login credentials by appearing to be legitimate [1, 2]. Palo Alto Networks describe phishing as the "most pervasive initial access vector in modern cyber attacks, often serving as the entry point for credential theft, account compromise, ransomware deployment, and supply chain infiltration. [1]"

As the image illustrates, first the attacker sends a link via email, text, or social media posting [1, 2]. The victim clicks on the link and is taken to a phishing website. It's a fake website that looks like the website for the actual company they think they've been contacted by.

The victim enters their information (such as login credentials, credit card details) into the phishing website. The attacker then uses the credentials on the legitimate website.

How is it Done?

Phishing links can be sent by email or text. They can also be posted to collaboration platforms like Slack and Teams, or social media sites like Facebook and LinkedIn.

They can even be done via voice calls or something as simple as distributing a flyer with a QR code.

Here are some examples of phishing.

Phishing Example

This is a message my son received this year, in June 2025. He had just gotten the newly-released Nintendo Switch 2 after waiting months for its release, and was eagerly awaiting a new case that I ordered as a gift for him for his birthday. We were about to travel by plane the next day, so it was urgent for him to receive the case and protect his new Switch 2 while flying.

He received this text message, claiming to be from USPS and requiring a payment in order to deliver his item. He assumed it must be about his Switch case. Since he needed the case so badly, he clicked the link to see what was delaying the delivery. All they are asking for is 28 cents, easy! Thankfully he reported it to me and I was able to catch him in time before he entered his debit card info.

I pointed out to him the bad grammar and the suspicious URL. The ‘L’ on lump should be capitalized and the website *should* include “usps.gov” but it doesn’t. Plus, the original text message is coming from an international number. USPS would never.

But here’s how this attack *could* have succeeded:

First, the likelihood that an American customer is waiting on a package delivery of some sort in 2025 is high. Sure, Amazon typically delivers with their own trucks and shipping, but they have been known to use USPS for a hand off as well.

Second, they were only asking for a small amount. Just 28 cents to receive your urgent item! That’s a small request. Someone may think, “What’s the harm?” But all they need is for you to enter your credit card information and then they have it. They can use it to purchase anything.

Lastly, overall, the phishing website looks authentic! It uses the website and branding colors of the real USPS and it renders well on a mobile device. This is called “brand impersonation” and it makes users trust what they are seeing and stops them from investigating further [3].

Luckily, in the case of my son, he was using a debit card, not credit, and his account was low at the time, with a balance of only 26 cents. If they would have tried to run his card for the mere 28 cents they would have been rejected for insufficient funds. However, that won't be the outcome for everyone. In fact, they would likely store the card information instead of using it right away.

Spear Phishing

Unlike general phishing, which casts a wide net, spear phishing targets a specific individual or organization. The attacker researches the target, conducting reconnaissance, looking for information about them on their website, Facebook, or LinkedIn, so the attack can be crafted in a personalized way [4].

Spear Phishing Example

Here's one real-world example of spear phishing, and actually this one can be considered whaling due to the high-value target. In 2015, Ubiquiti CEO Robert Pera was alerted by the FBI that Ubiquiti's Hong Kong unit had made 14 wire transfers over 17 days to countries like Russia, China, Hungary, and Poland. The total amounted to $46.7 million, or roughly 10% of Ubiquiti's cash position. Pera was unaware of the transfers until the FBI reached out to him [5].

How did this happen?

Phony emails were sent to Ubiquiti's chief accounting officer, Rohit Chakravarthy from a bogus Pera and bogus lawyer Tom Evans claiming Ubiquiti would be making some acquisitions that would require several wire transfers.

Normally, large wire transfers done by publicly-traded companies in the US require at least two people to sign off on them. Accounting and disbursing should be two separate roles, done by people of different levels in the corporate hierarchy or of different departments. That did not happen in this case.

According to Forbes, if the FBI hadn't notified Ubiquiti that they had been watching their Hong Kong account, the transfers would have continued undetected. As a result of the attack, Chakravarthy resigned from Ubiquiti and moved on to another company.

Quishing (QR codes)

Quishing refers to using QR codes to catch users in phishing schemes [6].

Some examples of quishing:
Handing out flyers at conferences: Attackers print QR codes with links to malicious websites in flyers and hand them out at conferences. They have QR code stickers printed and lay them over restaurant QR codes, parking meter codes, or charity event donation boxes so when a patron scans to pay they end up on a malicious website prompting them to enter their payment info.

Attackers have also covered QR codes in hotel rooms that help guests connect to wifi. Instead, the malicious QR codes lead to phony sites which ask for personal information.

The same tactic is used on social media, where followers are asked to scan a QR code to enter a contest, and then their personal information is captured.

People could also scan a QR code thinking they were signing up for a COVID-vaccine appointment or making a payment for one, however the attackers capture their personal information or credit card info.

Defenses Against Phishing

First, know the signs. Check the sender. Check the URL where you're being sent. If there are spelling errors, strange domain names, or grammar mistakes, it's likely a phony message.

Don't download files or attachments from unknown senders. Use antivirus software.

Verify requests for payment or personal information. If a bank texts or emails you asking you to log in, open a new browser page and log in, or call them at the number on the back of your card. If someone calls claiming to be the CEO, hang up and call them back on a trusted number.

Require 2 or more people for sensitive or high-value transactions. The second person needs to be a superior or someone from a different department. That would have helped stop the Ubiquiti attack [5].

Security Awareness Training - teach employees to identify and respond to phishing attacks of all kinds [6].

Take a Zero-Trust stance. Understand that nothing should be implicitly trusted [7]. Be suspicious of everything.

This ends my presentation. Now I'll allow time for the review of my Resources slides. Thank you.

Resources

[1] Palo Alto Networks, "What Is Phishing?," *Palo Alto Networks*. https://www.paloaltonetworks.com/cyberpedia/what-is-phishing (accessed Aug. 13, 2025).

[2] CloudFlare, "What is a Phishing Attack?," *Cloudflare*. Accessed: Aug. 13, 2025. [Online]. Available: https://www.cloudflare.com/learning/access-management/phishing-attack/

[3] Palo Alto Networks, "What Is Spear Phishing?," *Palo Alto Networks*, 2015. https://www.paloaltonetworks.com/cyberpedia/what-is-spear-phishing#types (accessed Aug. 14, 2025).

[4] SentinelOne, "What is Spear Phishing? Types & Examples," *SentinelOne*, Jun. 14, 2025. https://www.sentinelone.com/cybersecurity-101/threat-intelligence/spear-phishing (accessed Aug. 13, 2025).

[5] N. Vardi, "How A Tech Billionaire's Company Misplaced $46.7 Million And Didn't Know It," *Forbes*, Feb. 08, 2016. https://www.forbes.com/sites/nathanvardi/2016/02/08/how-a-tech-billionaires-company-misplaced-46-7-million-and-didnt-know-it (accessed Aug. 13, 2025).

[6] Keepnet Labs, "10 Real-Life Quishing Attack Examples to Strengthen Your Cybersecurity," *Keepnet Labs*, Nov. 15, 2024. https://keepnetlabs.com/blog/10-real-life-quishing-attack-examples-to-strengthen-your-cybersecurity (accessed Aug. 13, 2025).

[7] Palo Alto Networks, "What Is Smishing?," *Palo Alto Networks*, 2015. https://www.paloaltonetworks.com/cyberpedia/what-is-smishing#spot-smishing-attempt (accessed Aug. 14, 2025).