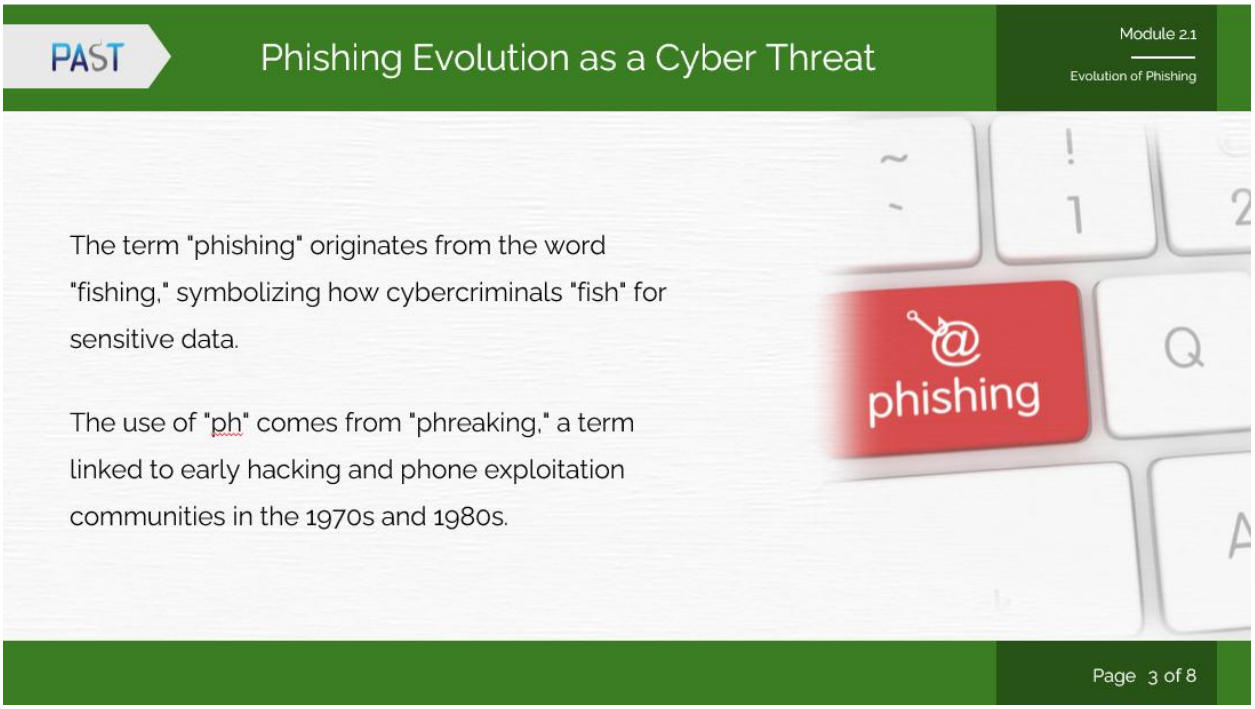
Phishing Assessment

Module 2.1: Evolution of Phishing

Table of Contents

1. Phishing evolution as a cyber threat



Phishing Evolution as a Cyber Threat

Module 2.1

Evolution of Phishing

The term "phishing" originates from the word "fishing," symbolizing how cybercriminals "fish" for sensitive data.

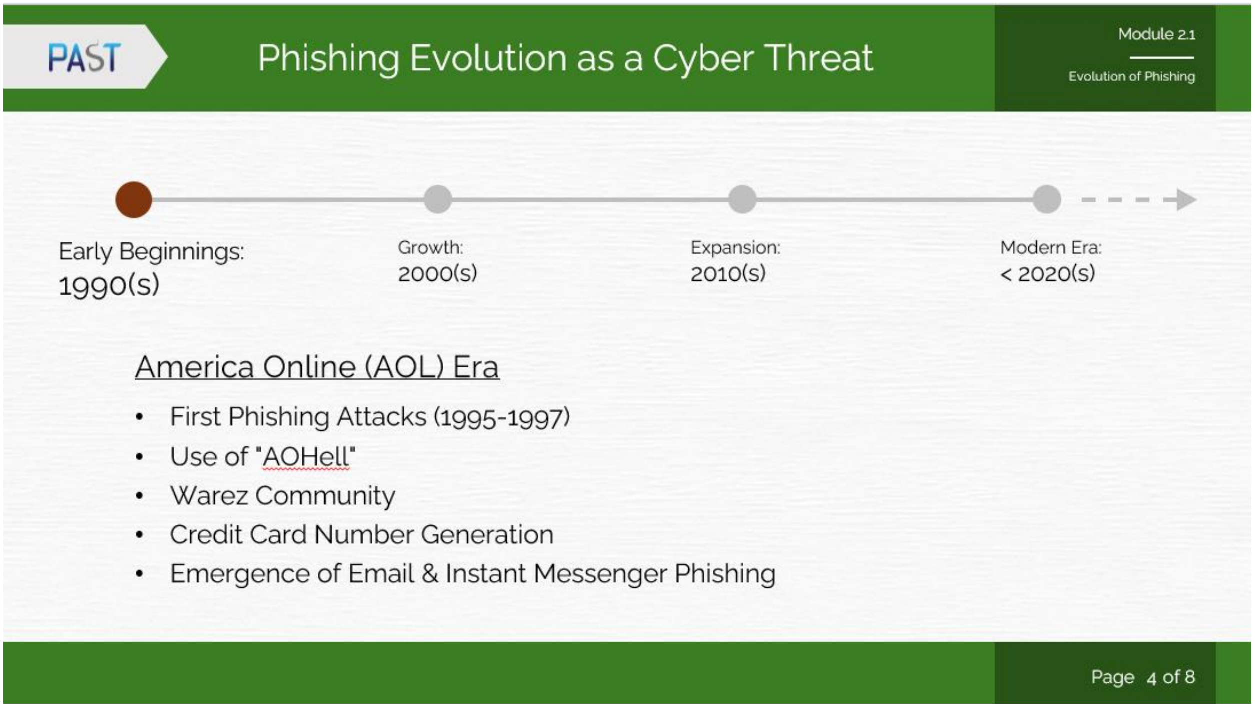
The use of "ph" comes from "phreaking," a term linked to early hacking and phone exploitation communities in the 1970s and 1980s.

Page 3 of 8

Phishing scams rely on fake emails and websites to trick people into willingly giving up sensitive information. It isn’t surprising, then, that the term “phishing” originates from the word "fishing," symbolizing how cybercriminals "fish" for sensitive data.

But there’s an interesting reason behind the unusual spelling with a “ph” instead of an “f.” It goes back to some of the earliest hackers, who were known as "phreaks"—a term that comes from "phone freaks." Phreaking was all about exploring and experimenting with telecommunication systems, and there’s always been a close connection between phreaks and hackers. So, using “ph” in phishing was used to link phishing scams with these underground communities.

Early Beginnings: The 1990s



PAST

Phishing Evolution as a Cyber Threat

Module 2.1

Evolution of Phishing

Early Beginnings:
1990(s)
Growth:
2000(s)
Expansion:
2010(s)
Modern Era:
< 2020(s)

America Online (AOL) Era

- First Phishing Attacks (1995-1997)
- Use of "AOHell"
- Warez Community
- Credit Card Number Generation
- Emergence of Email & Instant Messenger Phishing

Page 4 of 8

The **first phishing attacks** targeted America Online (AOL) users. Hackers posed as AOL staff, sending messages asking for login credentials.

Software like "**AOHell**" was used to automate the creation of fake messages to harvest credentials.

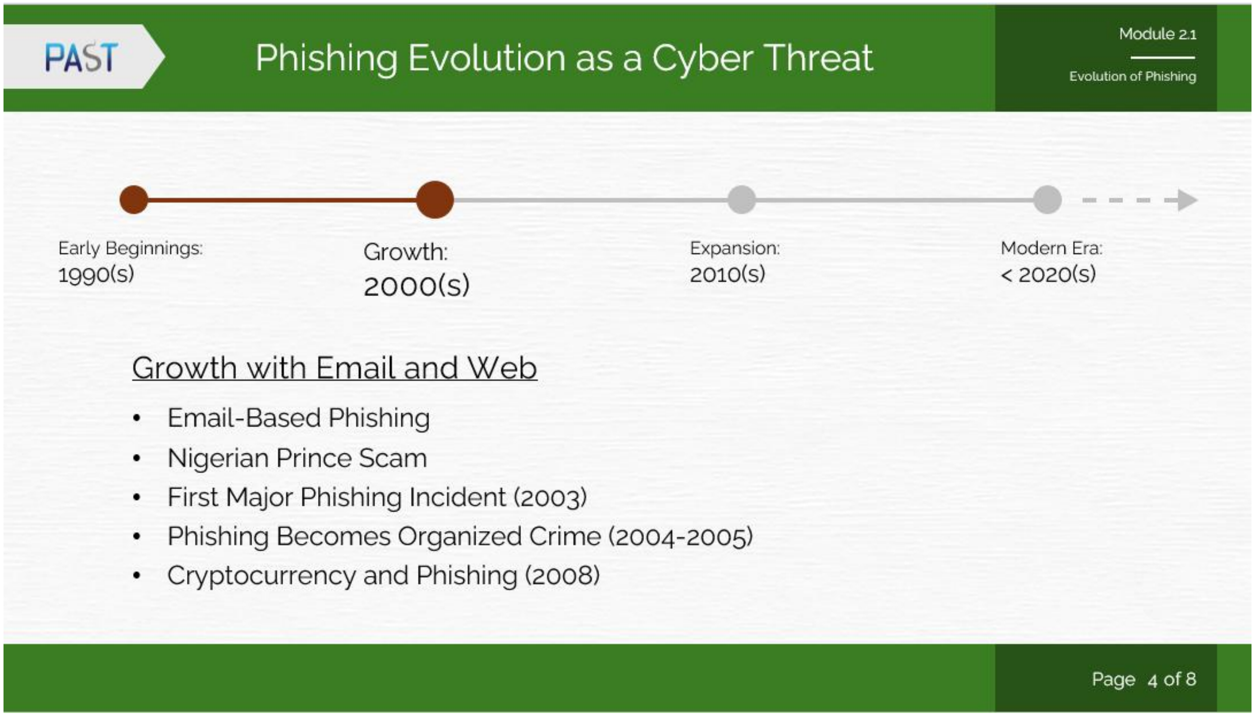
Back when America Online (AOL) was the number one provider of Internet access, millions of people logged on to the service each day. From the beginning, hackers and those who traded pirated software used the service to communicate with one another. This community was referred to as **the warez community**. It was this community that eventually made the first moves to conduct phishing attacks.

The first way in which phishers conducted attacks was by stealing users' passwords and using algorithms to **create randomized credit card numbers**. While lucky hits were few and far between, they struck the jackpot often enough to cause a lot of damage. The random credit card numbers were used to open AOL accounts. Those accounts were then used to spam other users and for a wide range of other things. Special programs like **AOHell** were used to simplify the process. This practice was put to an end by AOL in 1995, when the company created security measures to prevent the successful use of randomly generated credit card numbers.

With their random credit card number generating racket shut down, phishers created what would become a very common and enduring set of techniques. Through the **AOL instant messenger and email systems**, they would send messages to users while posing as AOL employees.

Those messages would request users to verify their accounts or to confirm their billing information. Often, people fall for the scam; after all, nothing like it had ever been done before. The problem intensified when phishers set up AIM accounts through the Internet; such accounts could not be "punished" by the AOL TOS department. Eventually, AOL was forced to include warnings on its email and instant messenger clients to keep people from providing sensitive information through such methods.

Growth with Email and Web (2000s)



PAST

Phishing Evolution as a Cyber Threat

Module 2.1

Evolution of Phishing

Early Beginnings: 1990(s)

Growth: 2000(s)

Expansion: 2010(s)

Modern Era: < 2020(s)

Growth with Email and Web

- Email-Based Phishing
- Nigerian Prince Scam
- First Major Phishing Incident (2003)
- Phishing Becomes Organized Crime (2004-2005)
- Cryptocurrency and Phishing (2008)

Page 4 of 8

Phishing expanded with the **growing popularity of email**. Scammers sent fake emails mimicking trusted institutions like banks or e-commerce platforms to steal passwords and credit card information.

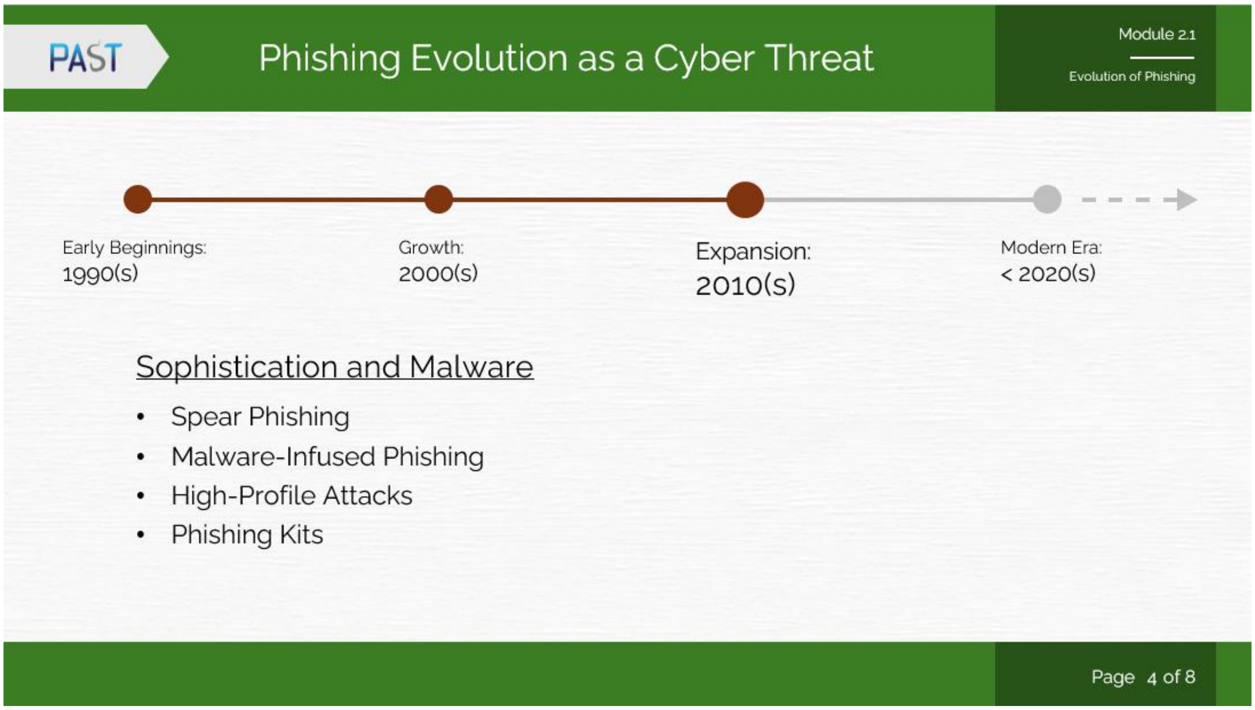
The **Nigerian Prince Scam** (advance-fee fraud) became a common email-based scam during this time.

First Major Phishing Incident (2003): attackers began registering fake domains that closely resembled legitimate websites like PayPal and eBay. Users would receive emails warning them of suspicious activity on their accounts and urging them to log in through a provided link. The link, of course, led to a fake website designed to steal their credentials.

By 2004, phishing was no longer just an occasional scam—it had become an **organized criminal operation**. Phishing software was developed and sold on the black market, enabling even less-skilled criminals to launch attacks. Meanwhile, companies scrambled to keep up, developing anti-phishing tools and email filters to detect fraudulent messages.

In late 2008, Bitcoin and other **cryptocurrencies are launched**. This allows transactions using malicious software to be secure and anonymous, changing the game for cybercriminals.

Sophistication and Malware (2010s)



PAST

Phishing Evolution as a Cyber Threat

Module 2.1

Evolution of Phishing

Early Beginnings: 1990(s)

Growth: 2000(s)

Expansion: 2010(s)

Modern Era: < 2020(s)

Sophistication and Malware

- Spear Phishing
- Malware-Infused Phishing
- High-Profile Attacks
- Phishing Kits

Page 4 of 8

Spear Phishing: More targeted phishing emerged, known as "spear phishing," aimed at specific individuals or organizations using personalized information.

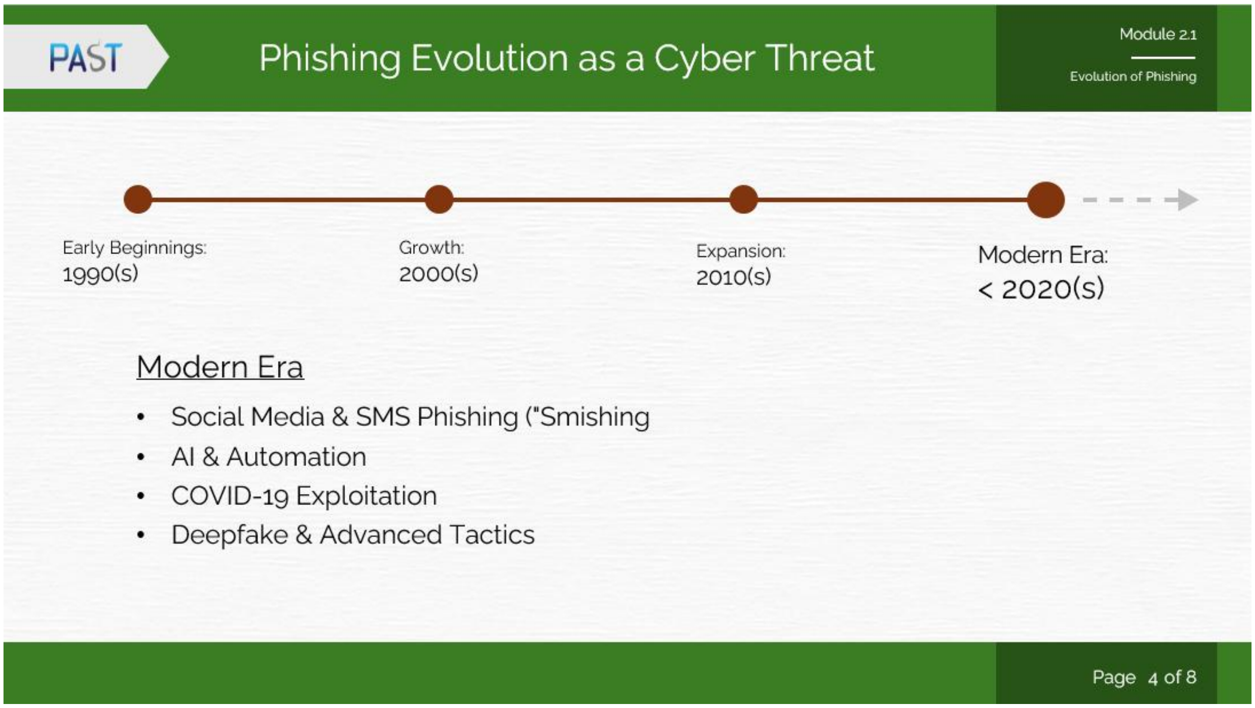
Rise of Malware Phishing: Phishing emails started carrying malicious attachments or links that installed ransomware, spyware, or keyloggers on victim devices.

In September of 2013, Cryptolocker ransomware infected 250,000 personal computers, making it the first cryptographic malware spread by downloads from a compromised website and/or sent to victims in the form of two different phishing emails. Cryptolocker scrambles and locks files on the computer and demands the owner make a payment in exchange for the key to unlock and decrypt the files.

High-profile Attacks incidents like the 2016 Democratic National Committee (DNC) email hack highlighted how phishing could influence politics and global events. Hackers used simple phishing emails to compromise high-profile political figures, leaking sensitive emails and impacting the U.S. election.

Phishing Kits and Tools: Cybercriminals developed ready-made phishing kits, enabling even non-technical individuals to launch attacks.

Modern Era (2020s)



Phishing Evolution as a Cyber Threat

Module 2.1
Evolution of Phishing

Early Beginnings:
1990(s)

Growth:
2000(s)

Expansion:
2010(s)

Modern Era:
< 2020(s)

Modern Era

- Social Media & SMS Phishing ("Smishing
- AI & Automation
- COVID-19 Exploitation
- Deepfake & Advanced Tactics

Page 4 of 8

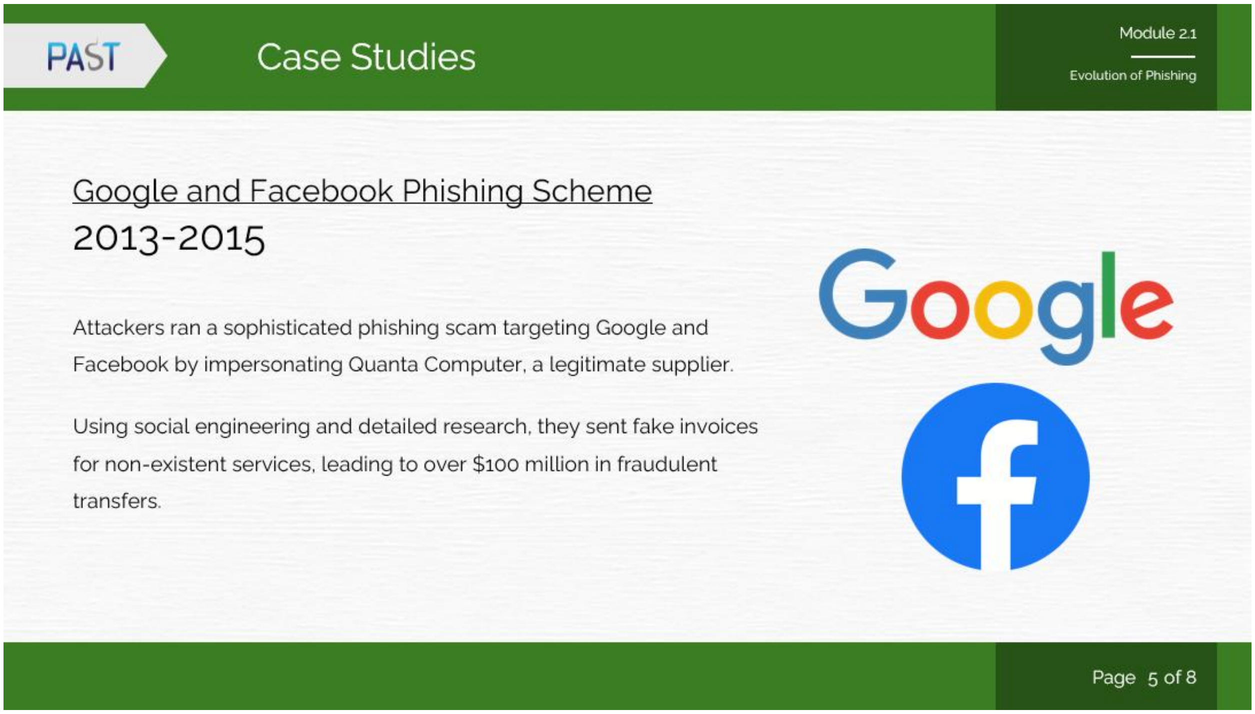
Social media and SMS Phishing (Smishing): Social media platforms and messaging apps became popular phishing grounds. Cybercriminals leveraged platforms like Facebook, Instagram, and WhatsApp for scams. Smishing, phishing via SMS, became a significant threat with the rise of mobile banking and personal data stored on smartphones.

AI and Automation: AI tools allowed for crafting more convincing and personalized phishing emails, bypassing traditional security filters.

COVID-19 Exploitation: Phishers exploited the COVID-19 pandemic, sending fake messages about vaccines, health updates, or stimulus payments.

Deepfakes and Advanced Tactics: The use of deepfake technology for phishing (e.g., mimicking voices or videos of trusted individuals) is an emerging trend.

2. Case studies



PAST

Case Studies

Module 2.1

Evolution of Phishing

Google and Facebook Phishing Scheme

2013-2015

Attackers ran a sophisticated phishing scam targeting Google and Facebook by impersonating Quanta Computer, a legitimate supplier.

Using social engineering and detailed research, they sent fake invoices for non-existent services, leading to over $100 million in fraudulent transfers.

Page 5 of 8

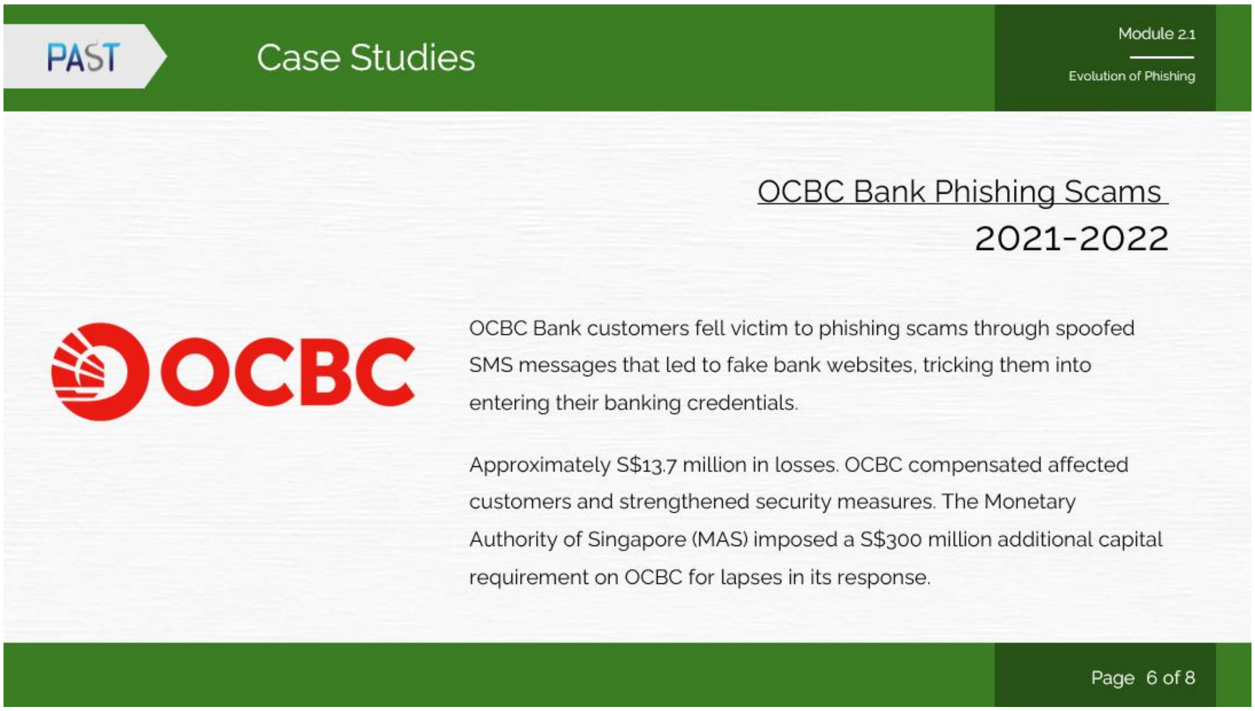
Google and Facebook Phishing Scheme (2013-2015)

Attackers executed a sophisticated phishing scam by impersonating Quanta Computer, a legitimate supplier. They sent fake invoices to Google and Facebook, requesting payment for non-existent services.

Impact: Financial Loss: Over $100 million in fraudulent transfers.

Methods: Social engineering and detailed research allowed the attackers to create convincing fraudulent requests.

Resolution: Some of the stolen funds were recovered after legal actions against the perpetrators, including the extradition of a primary suspect.



Case Studies

Module 2.1
Evolution of Phishing

OCBC Bank Phishing Scams
2021-2022

OCBC Bank customers fell victim to phishing scams through spoofed SMS messages that led to fake bank websites, tricking them into entering their banking credentials.

Approximately S$13.7 million in losses. OCBC compensated affected customers and strengthened security measures. The Monetary Authority of Singapore (MAS) imposed a S$300 million additional capital requirement on OCBC for lapses in its response.

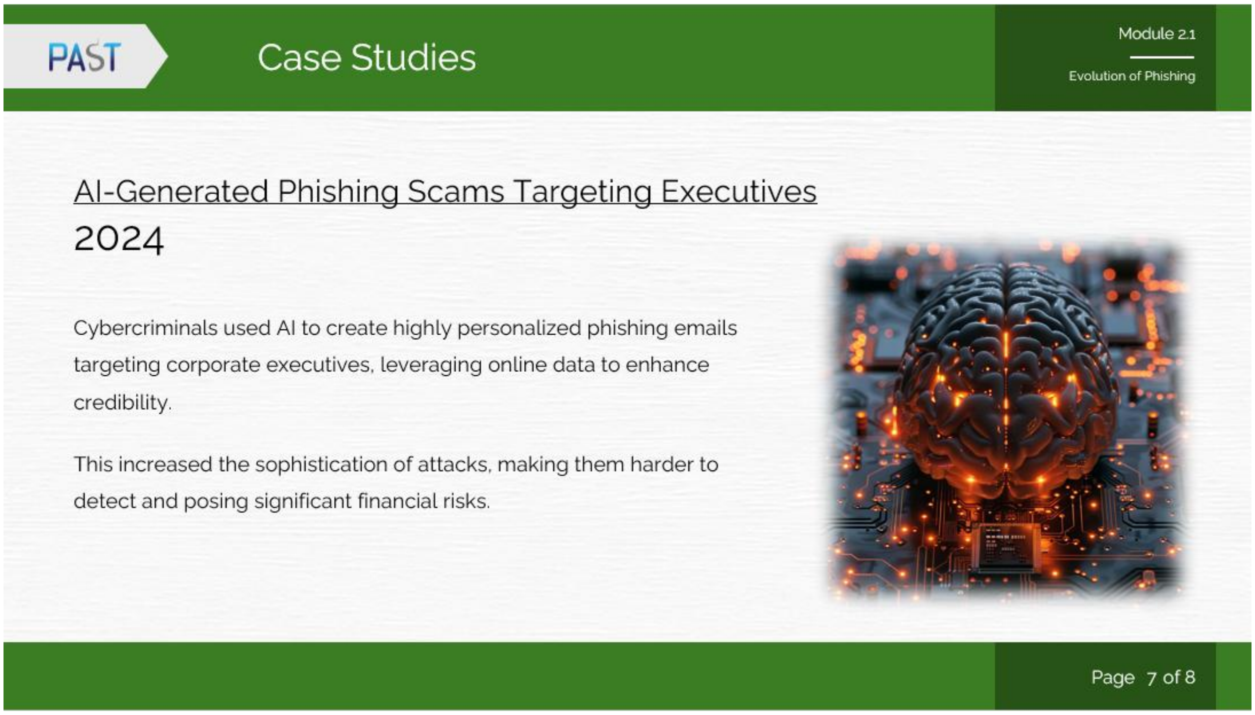
Page 6 of 8

OCBC Bank Phishing Scams (2021-2022)

In late 2021 and early 2022, OCBC Bank customers were targeted by phishing scams involving spoofed SMS messages. These messages directed victims to fraudulent websites resembling the bank's official site, where they were prompted to enter their online banking credentials.

Impact: Financial Losses: Approximately S$13.7 million was lost, affecting numerous customers.

Reparations: OCBC Bank provided goodwill payments to affected customers to cover their losses.



PAST Case Studies

Module 2.1

Evolution of Phishing

AI-Generated Phishing Scams Targeting Executives

2024

Cybercriminals used AI to create highly personalized phishing emails targeting corporate executives, leveraging online data to enhance credibility.

This increased the sophistication of attacks, making them harder to detect and posing significant financial risks.

Page 7 of 8

AI-Generated Phishing Scams Targeting Executives (2024)

In 2024, cybercriminals leveraged artificial intelligence to craft highly personalized phishing emails aimed at corporate executives. These emails utilized details gleaned from online profiles to enhance their credibility.

Impact:

- Increased Sophistication: The use of AI made phishing attempts more convincing and harder to detect.
- Financial Threats: Such scams posed significant financial risks to targeted organizations.

Response: Cybersecurity experts emphasized the need for advanced detection tools and employee training to counter AI-driven phishing attacks.

Summary

Phishing, a cyber threat derived from the concept of "fishing" for sensitive data, traces its origins to early hacking communities. It first emerged in the mid-1990s during the AOL era, where attackers used social engineering to steal user credentials. In the 2000s, phishing expanded through email and fake websites, becoming more widespread. By the 2010s, attackers had adopted more sophisticated techniques, including malware and targeted phishing (spear-phishing). In the 2020s, phishing has evolved further with AI and automation, making attacks more convincing and harder to detect.

Notable cases include the Google and Facebook phishing scheme (2013-2015), where scammers impersonated a supplier to steal over $100 million; the OCBC Bank phishing scams (2021-2022), where fraudulent SMS messages led to S$13.7 million in losses; and AI-generated phishing scams (2024), which leveraged artificial intelligence to craft highly personalized attacks on corporate executives. As phishing tactics continue to evolve, the threat remains a significant challenge for individuals and organizations worldwide.

- END -