

Week 2 → Cybersecurity  
Upstare: Breach  
Response.

## Phishing Scams.

Types of phishing

Phishing

Spear-phishing

Whaling

Top 10 spoofed Brands

→ Google

→ YouTube

→ Apple

→ Amazon

→ Spotify

- Netflix
- Microsoft.

Wow! Hackers use HTTPS →  
against the  
intention of it.

## Phishing Emails

- Suspicious sender's address
- Generic greetings & signatures
- Spoofed hyperlinks and websites
- Spelling and layout
- Suspicious attachments.

Impact of Phishing?

The nature of phishing itself has changed, moving far beyond "traditional phishing for username, passwords, and credit card numbers via fraudulent websites, and into more sophisticated cybercrime attacks that mount advanced persistent threats against organizations and steal individuals financial identities with devastating consequences for both users and organizations.

## Impact

- The average financial cost of a data breach is \$3.86m (IBM)
- RFI scans mounted for over \$12

Billion in losses (FBI)

- Phishing account for 90% of data Breaches.
- Phishing attempts have grown 65% in the last year.
- 15% of people successfully phished will be targeted at least one more time within the year.
- 76% of businesses reported being a victim of phishing attack in the last year.
- 30% of phishing messages get opened by targeted users

(version)

Identity Theft high ↑

→ Credit Card Theft

→ Rent or Lease Fraud

→ Bank Fraud.

Vulnerabilities...

Even tech giants like Google  
and Facebook were susceptible  
to a targeted phishing Attack..

↳ Spear Phishing

↳ Systems → Privilege Escalation &  
Bypass UAC.

↳ Double Malware.

~ People taking

↳ Delayed Response-

→ 100 Million payments was taken from FB and Google due to lack of Detection

2015 Scam took

\$98 million from Facebook

\$23 million from Google

↳ They have recovered the money

↳ and the attacker was sentenced to 30 years in July 2019.

Prevention

→ Early Detection

→ Review Invoices and payment-related communications.

→ Create Payment processes

→ Implement 2AF

→ Email System Automation

→ Employee Education & Training

→ SPAM Filter

→ Critical patches

→ Antivirus

→ Encryption

Point of Sale

The main objective is to

the main objective of point of  
Sale Breach is to steal your  
16-Digit Credit Card No...

POS Security .. PCI DSS.

- 1.) Build and Maintain a secure Network and Systems.
- 2.) Protect Card Holder Data
- 3.) Maintain Vulnerability management program
- 4.) Implement strong Access control measures
- 5.) Regularly Monitor and test Networks
- 6.) Maintain a IS Policy.



