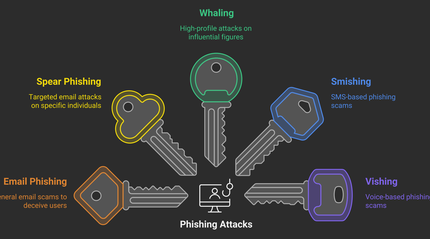
Phishing Awareness Training

Purpose of this module : This module is designed to educate users on the dangers of phishing attacks, how to recognize them, and how to avoid becoming a victim. It includes explanations, real-world examples, and interactive quiz.

What is Phishing?

Definition: Phishing is a type of cyberattack where attackers impersonate legitimate entities to trick individuals into providing sensitive information to steal credentials, financial data, or deploy malware

Types of Phishing Attacks



Recognizing Phishing Emails

Phishing Emails – Key Red Flags:

- **Sender Email Address:** Slight misspellings or unknown domains (e.g., support@paypal.com instead of support@paypal.com).
- **Urgency or Threats:** Messages that say "Act now!" or "Your account will be suspended!"
- **Attachments or Links:** Unsolicited files or URLs that don't match the official website.
- **Requests for Sensitive Info:** Legit companies never ask for passwords or OTPs via email.
- **Generic Salutations:** "**Dear User**" instead of using your actual name

Identifying Fake Websites

- **Suspicious URLs:** Look for misspellings or odd characters (e.g., go0gle.com).
- **No HTTPS:** Absence of a padlock icon in the browser means it's not secure.
- **Poor Language:** Bad grammar, odd formatting, or blurry logos.
- **Layout:** Fake pages often look rushed, inconsistent, or outdated.

Social Engineering Tactics

- **Pretexting**: Creating a fabricated scenario to get data
- **Baiting**: Offering something enticing (e.g., free downloads)
- **Quid Pro Quo**: Offering service in return for info
- **Tailgating**: Gaining physical access through manipulation

Best Practices to Avoid Phishing

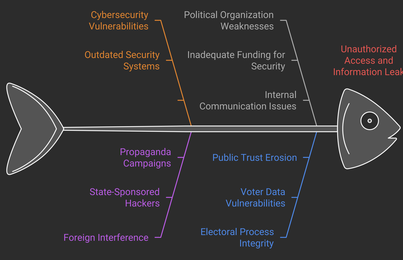
- Use **strong, unique passwords** and enable MFA (because "password123" is basically an open door)
- Regularly **update software** and antivirus
- Be cautious with **unsolicited emails** or messages
- Educate yourself and others through training
- **Report suspicious** emails to your IT/security team

Real-World Examples

1. 2016 DNC Hack

1. A spoofed Gmail login page tricked a staffer, leading to a massive email leak that rocked U.S. politics

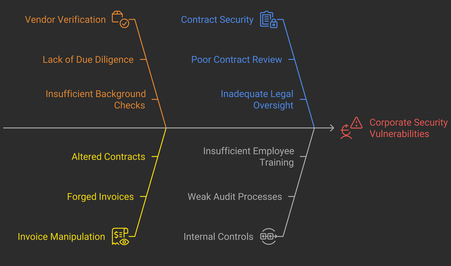
Anatomy of the 2016 DNC Cyberattack



2. Google & Facebook Scam:

An attacker faked a hardware supplier and sent invoices that tricked both giants into paying over $100 million.

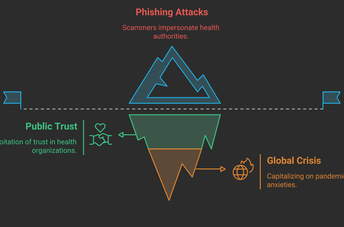
Analyzing the Google and Facebook Scam



3. COVID-19 Scams:

Phishers posed as WHO or health authorities offering "urgent pandemic info" to lure clicks—because nothing says "trust me" like a global health crisis

Phishing scams exploit global health crisis.



Interactive Quiz

1. **Which of the following is a sign of a phishing email?**
   - A) Personalized greeting
   - B) Spelling errors and urgent threats ☑
2. **True or False: You should trust any link that includes your bank's name.**
   - False ☑
3. **What should you do if you suspect an email is phishing?**
   - A) Click and check
   - B) Delete immediately
   - C) Report to IT ☑
4. **Which of these is NOT a social engineering tactic?**
   - A) Baiting
   - B) Quid Pro Quo
   - C) Debugging ☑