PHISHING AWARENESS TRAINING

How to Recognize and Avoid Phishing Attacks.
🧠 Stay sharp, stay safe

Presented by: Oyewole Samad Oluwasanjo.
Internship Project

WHAT IS PHISHING ?

Phishing is a fraudulent attempts to steal sensitive information by impersonating trusted entities.Fake emails, messages, or websites designed to trick you into revealing sensitive info like; Passwords, Credit card numbers, Personal data..

For example, you might receive an email that looks like it's from your bank, urging you to click a link and "verify" your account details. The link leads to a fake website that captures your input. Phishing attacks exploit trust and often use urgency or fear to prompt quick action.

WHY IS PHISHING DANGEROUS ?

Phishing is dangerous because it exploits trust to steal sensitive information or cause harm, often leading to severe consequences like:

1. 💸 FINANCIAL LOSS

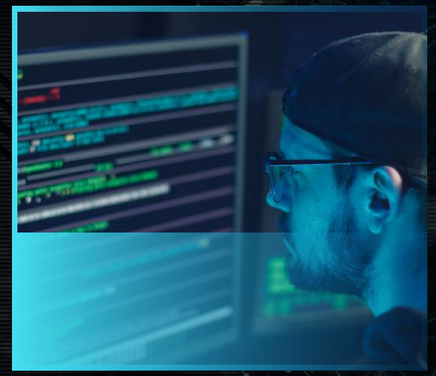
Phishing scams can trick users into providing credit card details or transferring money to fraudulent accounts. For example, a fake PayPal email might prompt a payment to a scammer.

2. 🔐 DATA BREACH

Attackers gain access to sensitive data — passwords, customer records, or business secrets.

3. 👴 IDENTITY THEFT

Attackers can use stolen credentials (e.g., usernames, passwords, or Social Security numbers) to impersonate victims, accessing bank accounts, emails, or other personal accounts.



TYPES OF PHISHING

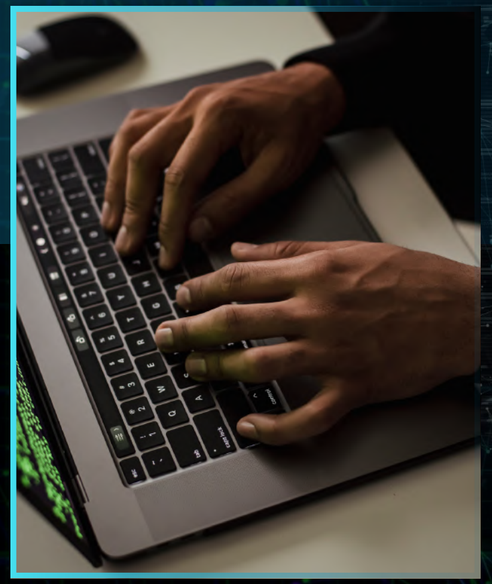
- Type;- Email Phishing
  Target;- General public
  Example ;- "Your Netflix account is suspended"

- Type ;- Pharming
  Target ; - Website visitors
  Example ;- Fake bank login pages

- Type ;- Spear Phishing
  Target ;- Specific individuals
  Example ;- "Hi [You], urgent document from CEO"

- Type ;- Smishing
  Targeet ;- Mobile user
  Example ;- "FedEx: Pay $2.50 to receive package" SMS

SPOT PHISHING EMAILS - RED FLAGS



1. GENERIC GREETINGS ("DEAR CUSTOMER")
2. URGENT/THREATENING LANGUAGE ("ACT NOW!")
3. MISMATCHED SENDER ADDRESSES (AMAZoN-SUPPORT@)
4. **Suspicious links (hover to preview URL)**
5. **Unexpected attachments (.exe, .zip)**
6. **Poor grammar/spelling**
7. **Requests for passwords/PII**

HOW TO DETECT FAKE WEBSITE

1. URL Check:

- Misspellings of website (paypa1.com)
- Wrong domains (.net instead of .com)

2. Trust Indicators:

- COMPANY LOGO QUALITY
- CONTACT INFORMATION
- GRAMMAR CONSISTENCY

TACTICS USED BY HACKERS

1. PRETEXTING :- FAKE SCENARIOS ("IT NEEDS YOUR PASSWORD")
2. BAITING :- "FREE GIFT CARD" OFFERS
3. Quid Pro Quo : - "Send data for a reward"
4. Tailgating: Following into secure areas
5. Authority Exploitation: "This is your manager calling..."

REAL-WORLD CASE STUDIES

1. **TWITTER BITCOIN SCAM (2020)**

- Attackers compromised employee credentials via vishing
- Took over celebrity accounts: "Send Bitcoin to double it!"
- Loss: $118,000 in 1 day

2 **COLONIAL PIPELINE RANSOMWARE (2021)**

- Phishing email → Stolen VPN password → $4.4M ransom
- Caused fuel shortages across US East Coast

QUIZ

EMAIL FROM "AMAZON": "YOUR ACCOUNT WILL BE SUSPENDED! CLICK HERE TO VERIFY."

A. Legitimate

B. Phishing

CALLER: "HI, I'M FROM MICROSOFT. YOUR COMPUTER HAS VIRUSES. WHAT'S YOUR IP?"

A. Legitimate

B. Phishing

PROTECTION CHECKLIST

DO:

- ✅ Verify sender identities (call official numbers)
- ✅ Use MFA everywhere
- ✅ Report suspicious messages
- ✅ Keep software updated

DON'T:

- ❌ Click unexpected links/attachments
- ❌ Share passwords via email/phone
- ❌ Use public WiFi for sensitive tasks
- ❌ Panic over urgent requests

INCIDENT RESPONSE

1. DISCONNECT FROM INTERNET
2. SCAN DEVICE WITH ANTIVIRUS
3. CHANGE PASSWORDS
4. CONTACT IT/SECURITY TEAM
5. MONITOR ACCOUNTS FOR FRAUD

CYBERSHIELD AGAINST PHISHING

🔒 1. STAY SKEPTICAL
- Assume *every* unexpected request is guilty until proven innocent
- Remember: Legitimate companies never ask for passwords via email

📞 2. VERIFY → REPORT → DELETE
- **Verify** sender identity through official channels
- **Report** suspicious messages to IT/Security
- **Delete** anything questionable immediately

🛡️ 3. YOU ARE THE HUMAN FIREWALL
- Your vigilance protects our entire organization
- One cautious click prevents a million-dollar breach

THANK YOU

Oyewole Samad