Phishing Awareness: Protecting Yourself from Online Scams By Okafor Peter

UNDERSTANDING AND PREVENTING PHISHING ATTACKS

CONTENT

What is Phishing?

Common Types of Phishing Attacks

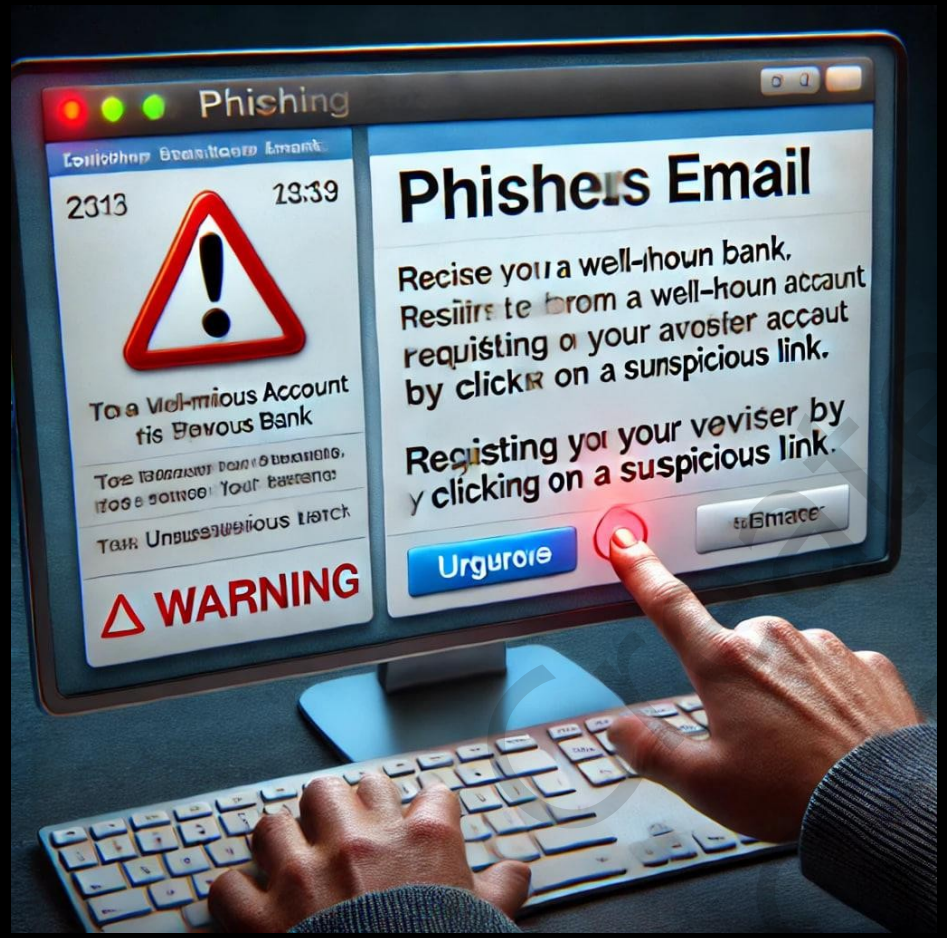
Recognizing Phishing Attempts

Real-World Examples

Preventative Measures

What to Do If You Suspect a Phishing Attempt

Conclusion



What is Phishing?

- **Definition:** A cyberattack where attackers impersonate legitimate entities to steal sensitive information.

Real-Life Phishing Story: The Twitter Bitcoin Scam (2020)

One of the most shocking phishing attacks in recent history happened in July 2020, when hackers took over major Twitter accounts, including those of Elon Musk, Bill Gates, Barack Obama, Apple, and Uber.

How the Attack Happened

- Hackers used spear-phishing to trick Twitter employees into giving up their login credentials.
- Once inside, they bypassed security measures and gained access to high-profile accounts.
- They tweeted a Bitcoin scam, saying:

"Send Bitcoin to this wallet, and we will double your money!"

The Aftermath

⚠ Over $120,000 was stolen from people who believed the scam.

⚠ Twitter had to lock down accounts and improve security.

⚠ Several teen hackers were arrested for orchestrating the attack.

Lesson Learned

☑ Always verify suspicious requests—even if they come from trusted sources.

Common Types of Phishing Attacks

- **Email Phishing** – Fake emails that appear from trusted sources.
- **Spear Phishing** – Targeted attacks on individuals or organizations.
- **Whaling** – Attacks aimed at senior executives.
- **Smishing** – Phishing via SMS messages.
- **Vishing** – Phishing through voice calls.

- **Email Phising - Fake emails that appear from trusted sources.**

Real-Life Phishing Story
1. Email Phishing – The Google & Facebook Scam ($100M Stolen!)
In 2013-2015, a hacker sent fake invoices to Google and Facebook, pretending to be from a legitimate company they worked with.
☑ The emails looked real, and the companies wired over $100 million before realizing the fraud!
💡 Lesson: Always verify payment requests, even from trusted sources.

Spear Phishing - Targeted attacks on individuals or organizations.

Real-Life Phishing Story

The Target Data Breach (40M Credit Cards Stolen!)
In 2013, hackers sent phishing emails to an HVAC company that worked with Target.
☑ They stole login credentials and gained access to Target's payment system, stealing 40 million credit card details!
💡 Lesson: Even small third-party vendors can be exploited to attack big companies.

Smishing - Phishing via SMS messages.

Real-Life Phishing Story

The DHL Delivery Scam
In 2022, many people received fake SMS messages saying:
"Your DHL package is delayed. Click here to reschedule!"
☑ The link led to a fake site that stole credit card details.
💡 Lesson: Never click links in unexpected messages—always visit the official website instead.

Vishing- Phishing through voice calls

Real-Life Phishing Story

The Bank Fraud Call Scam
A woman got a call from "her bank" saying her account was compromised.
☑ The caller knew her name & details, so she believed it was real.
☑ She gave her login details, and the scammers stole thousands from her account.
💡 Lesson: Banks never ask for your password over the phone! Always call back using the official number

Recognizing Phishing Attempts

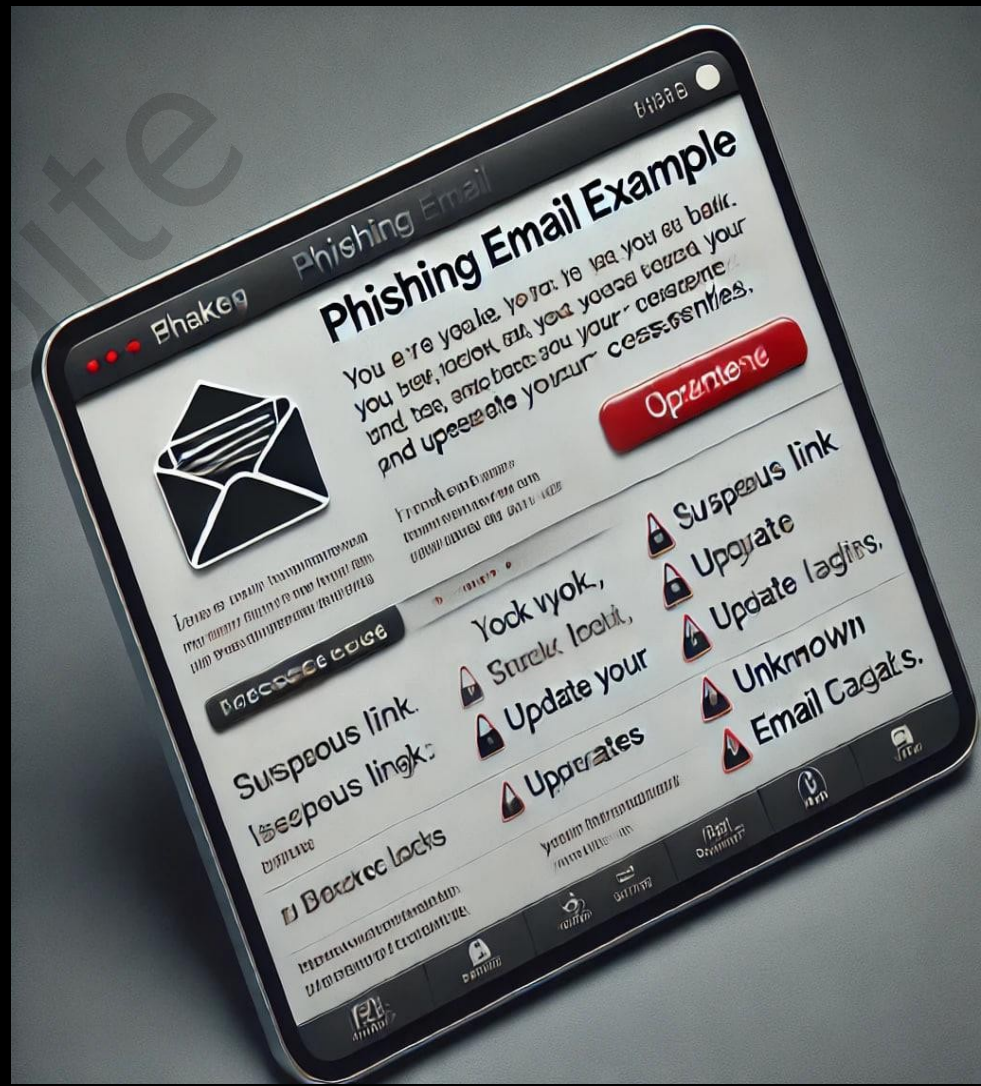
- **Red Flags:**
  + Urgent or threatening language.
  + Unusual sender addresses.
  + Generic greetings.
  + Suspicious links or attachments.
  + Poor grammar and spelling.

Preventative Measures

- Verify sender information.
- Hover over links to check URLs.
- Keep software updated.
- Use multi-factor authentication.
- Educate yourself and others.

What to Do If You Suspect a Phishing Attempt

- Do **not** click on any links or download attachments.
- Report the email to IT or your email provider.
- Delete the suspicious email.



Conclusion

- Vigilance and continuous education are the strongest defenses against cyber threats. In today's evolving digital landscape, attackers constantly refine their tactics, making it crucial to stay informed and proactive.

- ◇ Vigilance helps detect suspicious activities early, preventing potential breaches.
- ◇ Continuous education empowers individuals and organizations to recognize phishing attempts, social engineering tactics, and emerging cyber threats.

- By staying updated on cybersecurity trends and practicing caution, we can build a safer online environment. Cybersecurity is not a one-time effort but a lifelong commitment! 🛡️🔍