CYBERSECURITY

CODE ALPHA INTERNSHIP

Phishing Awareness Training

- Introduction: What is Phishing?
- Social Engineering: The Psychology Behind the Attack
- How to Recognize Phishing Emails
- How to Recognize Fake Websites
- Real-World Phishing Examples
- Best Practices to Avoid Falling Victim
- Final Quiz
- Conclusion

WHAT IS PHISHING ?

- Phishing is a type of cyberattack where attackers impersonate trusted entities (banks, coworkers, services) to trick people into revealing sensitive information such as:
- Passwords
- Credit card numbers
- Login credentials
- Personal or company data

Why it works: Phishing exploits human psychology—urgency, fear, curiosity, and trust

SOCIAL ENGINEERING:THE PSYCHOLOGY BEHIND THE ATTACK

Social engineering is the art of hacking people, not computers.

- Attackers exploit:
- Emotions
- Habits
- Trust
- Fear
- Urgency
- Authority

HOW TO RECOGNIZE PHISHING EMAILS?

RED FLAG#1 SUSPICIOUS LINKS

Hover over links (don’t click).

Displayed text:

www.bank.com

Actual link:

www.bank.verify-login[.]ru

⚠ Look for:

- Misspellings
- Extra words
- Random numbers
- Wrong country domains

HOW TO RECOGNIZE PHISHING EMAILS?

RED FLAG#2 Attachments You Didn't

Dangerous file types:

✓.exe

✓.zip

✓.html

✓.docm

Never open attachments unless you 100% expected them.

HOW TO RECOGNIZE PHISHING EMAILS?

RED FLAG # 3 Poor Grammar & Formatting

- Many phishing emails contain:
- Awkward phrasing
- Misspellings
- Inconsistent fonts
- Weird spacing
- (Not always—but often.)

HOW TO RECOGNIZE PHISHING EMAILS?

RED FLAG # 4 URGENT OR THREATENING LANGUAGE

- Examples:
- “Immediate action required”
- “Account suspension pending”
- “Failure to respond will result in permanent loss”

Real companies **do not threaten** you via email.

How to Recognize Fake Websites

Red Flags

- Misspelled URLs or extra characters
- No HTTPS or invalid security certificate
- Poor design or broken layouts
- Login pages reached through email links

Tip: Always navigate to websites manually instead of clicking email links.

Real-World Phishing Examples

Example 1: Bank Alert Scam

- Email claims suspicious transaction
- Link leads to fake bank login
- User enters credentials
- Attacker drains account

Example 2: Delivery Scam

- SMS: “Your package is delayed”
- Link installs malware
- Phone compromised

Example 3: Workplace Phishing

- Email appears from boss
- Requests gift cards urgently
- Employee sends codes
- Money gone forever

Example 4: Gaming Scam

- Fake Steam/PlayStation login
- Account stolen
- Items sold or account resold

Best Practices to Avoid Falling Victim

- Never click links from unsolicited messages
- Manually type website addresses
- Enable Multi-Factor Authentication (MFA)
- Use a password manager
- Keep software & browsers updated
- Verify requests via another channel
- Slow down—urgency is the enemy

THE “PAUSE & VERIFY” HABIT

Before acting, ask:

- Was I expecting this?
- Does this make sense?
- Am I being rushed?
- Can I verify independently?

Since you prefer routines, this **repeatable checklist** is especially powerful.

FINAL QUIZ

Question 1

You receive an email from your bank asking you to confirm your login details via a link. What should you do?

A) Click the link immediately
B) Reply with your details
C) Visit the bank’s website directly or contact them

Correct Answer: C

Question 2

Which of the following is a common phishing sign?

A) Personalized greeting
B) Professional grammar
C) Urgent threats and pressure

Correct Answer: C

FINAL QUIZ

QUESTION 3

Your manager emails asking for gift cards urgently. What’s the safest action?

A) Buy the gift cards
B) Verify via phone or chat
C) Forward to coworkers

Correct Answer: B

CONCLUSION

Phishing and fake websites succeed when we act on emotion instead of logic. By staying alert to suspicious senders, urgent messages, generic greetings, strange links, and unexpected attachments, and by carefully checking URLs and website design, we can protect our personal information and accounts. The key is to **slow down, verify, and follow safe habits**—manual logins, multi-factor authentication, and cautious clicks turn potential attacks into harmless messages. Vigilance and routine are your best defense against social engineering tricks.