

# Phishing Awareness Training: Spot the Hook!

This training helps you understand phishing, its risks, and how to stay safe.

 **by Roshni Sharma**



Roshni Sharma

# What is Phishing?

## Definition

Phishing is a type of **cyber attack** where criminals impersonate legitimate organizations (like banks, social media platforms, or companies) to trick individuals into revealing sensitive information such as:

- **Passwords**
- **Credit card numbers**
- **Social Security numbers**
- **Bank account details**

## Common Methods

1. **Email Phishing** – Fake emails pretending to be from legitimate companies.
2. **Spear Phishing** – Targeted attacks (e.g., impersonating your boss or a colleague).
3. **Smishing (SMS Phishing)** – Fraudulent text messages with malicious links.
4. **Vishing (Voice Phishing)** – Scam calls pretending to be from tech support or your bank.
5. **Clone Phishing** – A duplicate of a real email but with malicious links.

## Goals

- Steal credentials
- Install malware
- Extract data
- Financial gain

# Phishing Email Red Flags

## Suspicious Sender Address

Mismatched domain:

Looks like [support@amazon.com](mailto:support@amazon.com) but is actually [amazon@secure-service.net](mailto:amazon@secure-service.net).

Extra characters: paypa1-security.com (instead of paypal.com).

## Typos and Grammar

**Odd phrasing or errors:**

- *"Urgent: Youre account hass been compromised."*

## Generic Greetings

**Impersonal salutations:**

- *"Dear Customer" or "Dear User"* (instead of your name).

## Urgent or Threatening Language

**Pressure to act immediately:**

- *"Your account will be suspended in 24 hours!"*
- *"Unauthorized login detected—verify now!"*

**Too-good-to-be-true offers:**

- *"You've won a free iPhone! Click to claim."*

## Mismatched Links

Hover over links to see the real URL:

Displays <https://www.paypal.com> but leads to paypal-login.scamsite.com.

Unexpected attachments:

Files like "Invoice.zip" or "Document.exe" may contain malware.

# Spotting Malicious Links



## Hover to Check

Preview URLs before clicking to spot fakes.



## URL Shorteners

Beware of Bit.ly, TinyURL hiding true web addresses.



## Misspelled Domains

Look for small character changes like "goooogle.com".



## HTTPS Isn't Enough

Encryption helps, but verify the domain too.



## Use Security Tools

Scan links with Virustotal, URLscan.io for safety.

# Website Phishing Tactics

## Fake Login Pages

Designed to look like trusted sites to steal passwords.

## Padlock Icon

Check SSL presence but confirm actual domain name first.

## Domain Variations

Watch for subtle misspellings or added words in URLs.

## Verify Site Legitimacy

Search reviews and confirm real contact details before use.

# Social Engineering Tricks

## 1 Pretexting

Pretend to be someone trustworthy to get info.

## 2 Baiting

Offer enticements to lure victims into traps.

## 3 Quid pro quo

Trade services for confidential data.

## 4 Scareware

Fake alarms to scare victims into paying money.

## 5 Examples

Fake tech support and "You've won!" scam messages.

# Real-World Examples

## Fake "Account Suspension" Email (Banking Scam)

### Example Email:

**Subject:** "URGENT: Your Bank Account Has Been Locked!"  
**Sender:** security@bankofamerica-alerts.com (fake domain)

**Message:**  
"We detected unusual activity on your account. Click [here] to verify your identity, or your account will be suspended in 24 hours."

## Fake "Package Delivery" SMS (Smishing)

### How It Works: Red Flags:

- Shortened link (hides real URL)
- No tracking number provided
- USPS doesn't ask for personal info via text

### What Happens If You Click?

- You're taken to a fake USPS site asking for:
  - Address
  - Credit card ("pay a small redelivery fee")

## Fake "Tech Support" Call (Vishing)

### Example Call:

"Hello, this is Microsoft Support. We detected a virus on your computer. Press 1 to speak to an agent."

### How It Works: Red Flags:

- Unsolicited call (Microsoft doesn't call users)
- Fake urgency ("virus detected!")
- Asks for remote access or payment

### What Happens If You Comply?

- Scammers install malware or steal credit card info.

## Fake "CEO Fraud" Email (Business Email Compromise)

### Example Email:

**Subject:** "Wire Transfer Needed ASAP"  
**Sender:** ceo@yourcompany.org (spoofed to look real)  
**Message:**  
"Hi [Employee], I need you to process an urgent payment. Here are the details: [malicious link]"

### How It Works: Red Flags:

- Email looks like it's from the CEO but has a slight domain mismatch
- Urgent request with no prior discussion
- Asks for a wire transfer or sensitive data





# How to Protect Yourself



## Think Before You Click

Always verify senders and links carefully.

## Strong Passwords

Use unique passwords and a trusted password manager.

## Enable MFA

Add multi-factor authentication for extra security.

## Update Software

Keep apps patched to fix security vulnerabilities.

## Stay Educated

Keep learning about evolving phishing tactics.



# Reporting Phishing Attempts

## Email Reports

- **Email Providers** →
  - **Gmail:** Click "Report phishing" (three-dot menu → "Report phishing").
  - **Outlook:** Use "Report phishing" (Junk → "Phishing").
  - **Apple Mail:** Forward to [reportphishing@apple.com](mailto:reportphishing@apple.com).
- **Anti-Phishing Groups** →
  - **FTC:** [reportfraud.ftc.gov](https://reportfraud.ftc.gov)
  - **APWG (Anti-Phishing Working Group):** [reportphishing@apwg.org](mailto:reportphishing@apwg.org)

## Website Reports

- Submit phishing sites to Google Safe Browsing  
[https://safebrowsing.google.com/report\\_phishing/](https://safebrowsing.google.com/report_phishing/)
- What to Include:
- **URL of the fake site.**
  - **Screenshot** of the phishing page.
  - **Description** of how you encountered it (e.g., via email, social media).

## IT Alerts

Where to Report:

- **FTC:** [reportfraud.ftc.gov](https://reportfraud.ftc.gov)
- **FCC (for SMS scams):** [consumercomplaints.fcc.gov](https://consumercomplaints.fcc.gov)

What to Include:

- **Screenshot** of the text/call log.
- **Phone number** used in the scam.

## Social Media Reports

Where to Report:

- **Facebook** → Use "Report Post" (three dots → "Find support or report").
- **Twitter/X** → Click "Report Tweet" (... → "Report post").
- **LinkedIn** → Flag suspicious messages via "Report this message."

What to Include:

- **Username** of the scammer.
- **Link/Screenshot** of the fake profile or message.