



PhishGuard Academy

Phishing Prevention Guide

A PRACTICAL REFERENCE FOR SPOTTING AND REPORTING PHISHING ATTACKS

CodeAlpha Cybersecurity Internship · Task 4 · Version 1.0

1. What is phishing?

Phishing is a cyber attack in which criminals disguise themselves as trustworthy people or organizations to trick you into revealing passwords, card numbers, or other sensitive data. It is delivered by email, text message (smishing), phone call (vishing), and QR codes (quishing). Business Email Compromise (BEC) targets companies through impersonated executives and vendors.

Phishing works on psychology, not technology. Attackers use urgency, authority, fear, and familiarity to make you act before you think.

The attack variants

Variant	Channel	What it looks like
Email phishing	Email	Mass messages impersonating banks, couriers, or services
Spear phishing	Email	Personalized messages researched for a specific victim
Smishing	SMS	Fake delivery, bank, or government texts with links
Vishing	Phone	Callers claiming to be your bank, IT, or authorities
QR phishing	QR code	Codes that lead to fake login pages or downloads
BEC	Email	Impersonated executives/vendors requesting transfers
Fake login pages	Web	Cloned sign-in screens hosted on lookalike domains

Golden rule: stop, verify through a channel you trust, and report anything suspicious. When in doubt, assume it is phishing.

2. Common red flags

If a message has **any** of these, treat it as suspicious:

- ! Urgency and threats ("closed in 24 hours")
- ! Generic greeting ("Dear customer")
- ! Sender address that isn't the real company domain
- ! Misspelled or lookalike domains (amaz0n.com)
- ! Requests for passwords, OTPs, or card details
- ! Unexpected attachments (.zip, .exe, .docm)
- ! Payment in gift cards, crypto, or wire transfer
- ! Link text that differs from the real destination
- ! "Do not discuss this with anyone" secrecy
- ! Poor grammar and odd formatting
- ! Unsolicited QR codes leading to logins
- ! Caller demanding a one-time passcode

Reading a URL correctly

In **<https://chase.com.account-verification.net/signin>**, read the domain right-to-left: the site is owned by **account-verification.net**, not Chase. The registered domain is always the last two labels before the top-level domain. Watch for the @ trick (<https://chase.com@evil.io>) and punycode lookalikes (xn--pple-43d.com).

A padlock (HTTPS) proves encryption only, not that the site is legitimate. Verify the domain yourself.

3. Safe habits that prevent phishing

Before you click or respond

- Hover over (or long-press) links to preview the real destination.
- Type the website address yourself instead of clicking links from messages.
- Use saved bookmarks and a password manager that refuses lookalike domains.
- Verify urgent requests through a second, trusted channel (a known phone number).
- Never share passwords, one-time codes, or card details over email, text, or phone.

Protect your accounts

- Enable multi-factor authentication (MFA) everywhere it is available.
- Use a unique password for every account; use a password manager.
- Keep browsers, operating systems, and mail filters updated.
- Apply email authentication (SPF, DKIM, DMARC) on company domains to stop spoofing.

At work

- Verify any change to bank details or payment instructions by phone, with dual approval for large transfers.
- Report suspicious messages with your mail client's "Report phishing" button.
- Encourage a culture where "let me verify that" is welcomed.

4. You clicked a link or entered data. Now what?

1. **Disconnect.** Close the suspicious page and, if prompted, remove any downloaded file without opening it.
2. **Change your passwords** for the affected accounts, and any account using the same password, from a device you trust.
3. **Enable or review MFA** on the affected accounts immediately.
4. **Watch for follow-up attacks.** Scammers re-contact victims; don't respond to new messages about the incident.
5. **Notify your security team** (or your bank / the platform) with the original message, sender, and what you entered.
6. If money was sent or card data entered, **contact your bank right away** to freeze the card or dispute the transfer.

The sooner you act, the more likely the damage can be limited. Delaying helps attackers, not you.

5. How to report suspicious messages

Email

- Gmail: click the three dots on the email → "Report phishing".
- Outlook: ribbon → "Report" → "Report phishing".
- Work email: forward to your security team including the full message header, and never reply to the sender.

Text (smishing)

- Forward the text to **7726 (SPAM)** to report it to your carrier.
- Block the sender and delete the message.

Phone (vishing)

- Hang up. Call back using the official number from your card, bill, or company website.

Web

- Report phishing pages and URLs to Google Safe Browsing and your browser's report tools.
- In many countries, report to the national CERT or cybercrime unit.

What to include when you report: the full email (not attachments), the sender address, the message date, any links or QR codes (URLs, not clicks), and a note of anything you entered or clicked.

PhishGuard Academy — CodeAlpha Cybersecurity Internship, Task 4. This guide is for education and general awareness; it is not a substitute for your organization's security policies.