How to Recognize and Avoid Phishing Emails, Texts, and Fake

Computers and Electronics · about 27 minutes · 2026-11-06

Pause before an unexpected message becomes a clicked link, a stolen password, or a fraudulent payment. These 23 steps cover message context, urgency, sender addresses, lookalike domains, link previews, attachments, QR codes, requests for one-time codes, independent verification, safer reporting, security updates, unique passwords, MFA, malware scans, compromised passwords, payment providers, identity-theft recovery, and ongoing monitoring.

Things you will need

- An updated phone or computer with official security protections enabled
- Existing bookmarks or official apps for important accounts
- Trusted contact details from statements, cards, or independently verified websites
- A unique-password manager and protected recovery information
- Multifactor authentication with securely stored backup options
- A private incident log for dates, messages, disclosures, payments, and recovery contacts

Pausing and Assessing Unexpected Messages

1. **Pause before touching an unexpected message**
   Stop before clicking, replying, scanning, calling, or forwarding an unexpected message.
2. **Match the message to a real relationship**
   Check whether the message fits a transaction or relationship you actually have.
3. **Name the pressure in the request**
   Identify pressure, fear, urgency, secrecy, or an unusually attractive reward in the request.
4. **Compare the display name with the address**
   Compare the display name with the actual sender address, number, or account profile.
5. **Weigh wording as a clue, not proof**
   Review wording and presentation as supporting clues rather than a final verdict.

Inspecting Links, Attachments, and Requests

6. **Preview the link without opening it**
   Inspect a link's destination only through a preview that does not open it.
7. **Type the address yourself to reach it**
   Read the actual domain carefully and navigate independently when you need the service.
8. **Keep attachments and codes untrusted**
   Treat unexpected attachments, downloads, QR codes, and document-sharing prompts as untrusted.
9. **Refuse requests for codes and remote access**
   Refuse unexpected requests for passwords, one-time codes, payment details, identity numbers, or remote access.
10. **Hang up and find the real number**
    End an unsolicited call and avoid calling the number supplied in the message or shown by caller ID.

Verifying Through Independent Channels

11. Check the claim inside the official app

Open the service's established app or type its known web address yourself to check the claimed issue.

12. Reply through a channel you already trust

Contact the organization through a channel you already trust when the account information does not resolve the question.

13. Verify a friend's request on another line

Verify a surprising request from a friend, relative, or coworker through a separate existing conversation.

14. Reconcile the invoice with your own record

Cross-check invoices, deliveries, refunds, and payment instructions inside the relevant account before taking action.

15. Keep the evidence, then block and report

Preserve only the evidence needed for a report, then use the service's report and block controls.

Strengthening Accounts and Devices

16. Update software and keep tested backups

Enable automatic security updates for your operating system, browser, phone, and security software, and maintain tested backups.

17. Store unique passwords and recovery details safely

Use a unique password for every account and store recovery information securely.

18. Add a second factor to key accounts

Turn on multifactor authentication for important accounts, especially email, finance, and password-management accounts.

19. Filter spam and agree a household rule

Use spam filtering, blocking, and household verification habits to reduce repeated exposure.

Responding After a Click, Payment, or Disclosure

20. Assess the damage without replying to them

Stop the interaction and assess what happened without contacting the sender again.

21. Reset passwords from a trusted device

Change compromised passwords from a known-clean device and secure the account recovery routes.

22. Call your bank before the money moves

Contact the bank, card issuer, payment service, exchange, or gift-card company immediately if you paid or disclosed financial details.

23. File the report and monitor your records

Document the incident and use the appropriate identity-theft, fraud-reporting, and monitoring resources.

Sources

1. Recognize and Report Phishing
   https://www.cisa.gov/secure-our-world/recognize-and-report-phishing
2. Recognize and Report Phishing
   https://www.cisa.gov/secure-our-world/recognize-and-report-phishing
3. Proceed with Caution, California: Attorney General Bonta Alerts Consumers to Ongoing Scam Activity
   https://oag.ca.gov/news/press-releases/proceed-caution-california-attorney-general-bonta-alerts-consumers-ongoing-scam
4. Avoiding Social Engineering and Phishing Attacks
   https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks
5. Who do I contact for help with a scam or fraud?
   https://www.consumerfinance.gov/ask-cfpb/i-think-i-or-someone-i-know-was-the-victim-of-a-scam-or-financial-exploitation-who-can-i-contact-
6. Identity Theft Recovery Steps
   https://www.identitytheft.gov/

Written as a checklist from https://www.howcompass.com/how-to/Recognize-and-Avoid-Phishing-Emails-Texts-and-Fake-Websites. Corrections