PHISHING & SOCIAL ENGINEERING SAFETY CHECKLIST

A plain-language guide for everyone | Print & share freely

Phishing attacks trick you into handing over passwords, money, or personal information by pretending to be someone you trust -- a bank, a tech company, or even a friend. Use this checklist every time you receive an unexpected message, link, or phone call. Print it out and keep it somewhere visible!

[EMAIL] Emails & Text Messages

- ☐ **Check the sender's full email address -- not just the display name**
  Click on the sender's name to reveal the real address. "PayPal Support" might actually be coming from random123@fakesite.ru. If the address looks odd or unfamiliar, do not trust it.

- ☐ **Be suspicious of urgent language or threats**
  "Your account will be CLOSED in 24 hours!" is a classic pressure tactic. Legitimate companies rarely threaten you or demand immediate action via email.

- ☐ **Never click links in unexpected emails -- go directly to the website instead**
  Type the official address (e.g. yourbank.com) into your browser yourself. Hover your mouse over any link first -- the real destination appears at the bottom of your screen.

- ☐ **Be very cautious with unexpected attachments**
  Do not open .zip, .exe, .docm, or .xlsm files from strangers. Even PDFs can be dangerous. If you were not expecting a file, call the sender to confirm before opening it.

- ☐ **Look for spelling mistakes and unprofessional formatting**
  Real companies proofread their emails. Odd fonts, blurry logos, or sentences that don't quite make sense are classic red flags of a scam.

QUICK TEST: Hover your mouse over any link (do not click!). The real web address will appear at the bottom of your browser or email window. If it looks nothing like the company being mentioned, it is almost certainly a scam.

[PHONE] Phone Calls & Voicemail (Voice Phishing)

- ☐ **Never give personal information to someone who called YOU**
  Your bank, the IRS, Microsoft, or Amazon will never call out of the blue asking for your password, Social Security number, or credit card number over the phone.

- ☐ **Hang up and call back on a number you find yourself**
  If a caller claims to be from your bank, hang up. Find the real phone number on the back of your card or on their official website, then call that number yourself.

- ☐ **Beware of "tech support" callers saying your computer has a virus**
  This is one of the most common scams. Microsoft and Apple do NOT proactively call you. Never let an unsolicited caller access your computer remotely.

- ☐ **Caller ID can be faked -- a familiar number proves nothing**
  Scammers can make calls appear to come from your bank, the government, or a local number. Always verify the caller's identity independently before sharing any information.

[SECURITY] Passwords & Account Security

- ☐ **Use a different password for every important account**
  If one account is hacked, attackers try that same password everywhere else. Use a free password manager (like Bitwarden) to remember strong, unique passwords for you.

- ☐ **Turn on two-factor authentication (2FA) wherever possible**

2FA sends a one-time code to your phone when you log in. Even if someone steals your password, they still cannot get in without that code. Enable it in your account settings.

- [ ] **Never share a one-time code with ANYONE -- ever**
  Scammers call pretending to be support staff and ask you to read back the code sent to your phone. No legitimate company will EVER ask you to share that code.

- [ ] **Make passwords long -- aim for 12 or more characters**
  A short password like "Summer1!" is cracked in seconds. A passphrase like "PurpleTaco!Runs42" is far stronger and still easy to remember.

[WEB] Websites & Links

- [ ] **Carefully check the website address (URL) before entering any information**
  Scammers create look-alike sites: "paypa1.com" or "amazon-login.net" are NOT real. The real domain is the part right before ".com" -- make sure it matches exactly.

- [ ] **Look for the padlock icon (HTTPS) -- but do not rely on it alone**
  HTTPS means the connection is encrypted, but it does NOT mean the site is safe or real. Fake websites use HTTPS too. Always double-check the actual address in your browser.

- [ ] **Be cautious with QR codes in public places**
  Scammers place fake QR code stickers over real ones on parking meters, menus, and posters. Before scanning, check whether the sticker looks tampered with or stuck over another one.

- [ ] **Avoid entering passwords on public Wi-Fi without a VPN**
  Coffee shop and airport Wi-Fi can be monitored by others. Use a VPN service, or wait until you are on a trusted home or work network to log into sensitive accounts.

[SOCIAL] Social Media & Impersonation

- [ ] **Verify before you trust -- even messages that appear to come from friends**
  Hackers take over accounts and message everyone on the contact list. If a friend sends a strange link or asks for money, call or text them directly to confirm it is really them.

- [ ] **Limit personal information you share publicly**
  Your birthday, phone number, hometown, and employer help scammers create targeted attacks. Review your privacy settings on Facebook, Instagram, LinkedIn, and other platforms.

- [ ] **Be skeptical of "too good to be true" offers or prizes**
  "You have won an iPhone! Click here to claim." Real prizes never ask you to pay a fee or enter credit card details upfront. If it sounds too good to be true, it is.

[ALERT] If You Think You Have Been Phished -- Act Fast!

- [ ] **Change your password immediately on the affected account**
  Then change it on any other account where you used the same password. Do this from a device and network you trust (e.g. your home internet connection).

- [ ] **Enable two-factor authentication (2FA) on the account if you have not already**
  This prevents the attacker from accessing your account again even if they still have your old password.

- [ ] **Contact your bank right away if any financial information was shared**
  Call the phone number on the back of your debit or credit card immediately. They can freeze your account and dispute any fraudulent charges on your behalf.

- [ ]

Report the phishing attempt

Forward phishing emails to reportphishing@apwg.org. Report suspicious texts by forwarding them to 7726 (spells SPAM on most phones). This helps protect others from the same scam.

☐ **Tell someone you trust**

Do not be embarrassed -- these scams fool millions of smart people every year. Telling a family member, colleague, or IT department helps prevent it from happening to others.

REMEMBER: When in doubt, do not click! Stop -- Think -- Verify. Take 60 seconds to confirm something is real before you act. Scammers rely on you acting fast without thinking. Slowing down is your single most powerful defence.