



Person of Non-Interest

[Home \(https://beaponi.com/\)](https://beaponi.com/) > [Learn \(https://beaponi.com/learn\)](https://beaponi.com/learn) > How to spot phishing

How to spot phishing

Scam messages are getting more convincing. A few simple habits still beat them.

Last reviewed October 18, 2026 · [See the sources](#)

In short: Phishing is a message that pretends to come from someone you trust so you'll click a link, open an attachment, or share information. Don't act on the message itself. Pause, then check it through the company's own app or website, or a number you already trust. Report it, then delete it.

What phishing is

[Phishing \(https://beaponi.com/learn/glossary#phishing\)](https://beaponi.com/learn/glossary#phishing) is a message that pretends to come from someone you trust, like your bank, a delivery company, a government office, or a friend, so you'll click a link, open an attachment, or hand over information such as a password or a code. It can arrive by **email, text message, social media message, or phone call.**

It works on smart, careful people. Scammers rely on hurry, not on anyone being foolish.

The warning signs

- **It's urgent or emotional.** "Your account will be closed today." "Your package will be returned." "You've won." Pressure to act right now is the biggest sign of all.
- **It asks for personal or money information.** Passwords, codes, card numbers, your Social Security number, or a payment.
- **The link or email address is slightly off.** A letter added or swapped, an extra word like "secure" or "support," or a strange ending. Scammers copy real names closely.
- **The link is shortened** so you can't see where it really goes.
- **It asks for a code that was just sent to you.** Never share a verification code with anyone who contacts you. Scammers ask for it so they can get into your account.

No single sign proves a message is fake, and real messages can be urgent too. The safe habit is the same either way: check it yourself through the company's own app or website, or a number you already trust.

Don't count on spelling mistakes. Scam messages used to be full of errors. Now, with AI, many have perfect spelling and grammar. Watch for the signs above instead.

What to do with a suspicious message

1. **Pause.** Take ten seconds before you do anything. That's the 10-second pause (<https://beaponi.com/checklist#rushed>).
2. **Don't click, don't reply, and don't call any number in the message.** That includes any "unsubscribe" link.

3. **Check it another way.** If it might be real, go to the company's website or app yourself: type the address or search for it, then sign in or call the number listed there. If it seems to come from a friend, text or call them on a number you already have.
4. **Report it.** Use the "report spam" or "report junk" button in your email or messages app. You can also forward suspicious emails to **reportphishing@apwg.org**, a group that tracks phishing.
5. **Delete it.**

If you already clicked, replied, or gave something away

Don't panic, and don't be embarrassed. It happens to careful people every day. Act quickly:

- **You gave away a password:** create a new, strong password (<https://beaponi.com/learn/strong-passwords>) for that account, and anywhere you used the same one.
- **You gave away a code, or want stronger protection:** turn on two-step verification (<https://beaponi.com/learn/two-step-verification>). A passkey (<https://beaponi.com/learn/passkeys>) is even better, because it can't be phished at all.
- **Money, your Social Security number, or someone on your computer:** follow the steps in Help with a scam (<https://beaponi.com/help-with-a-scam>), and report it at ReportFraud.ftc.gov (<https://reportfraud.ftc.gov>).

Practice

Try the PONI Challenge on our home page (<https://beaponi.com/#challenge>): a fictional delivery text, three choices, and why the safe one works.

Common questions

Can phishing happen in a phone call? Yes. Phishing can come by email, text, social media message, or phone call. If a caller asks for a password, a code, or a payment, hang up and contact the company using a number you look up yourself.

Will a real company ask me for the code it just sent me? Treat that request as a scam. Google, for example, says it won't call you to verify a code, and that you should never share verification codes with anyone.

Does reporting a phishing message actually help? Yes. Reporting helps protect you and others. Use the "report spam" button in your email or messages app, and you can forward suspicious emails to reportphishing@apwg.org, which uses them to help track and prevent phishing.

Sources

Checked on October 18, 2026. Next review: by October 2027.

- [Recognize and Report Phishing \(https://www.cisa.gov/secure-our-world/recognize-and-report-phishing\)](https://www.cisa.gov/secure-our-world/recognize-and-report-phishing) (CISA)
- [Report Phishing \(https://apwg.org/reportphishing/\)](https://apwg.org/reportphishing/) (Anti-Phishing Working Group)
- [Turn on 2-Step Verification \(https://support.google.com/accounts/answer/185839\)](https://support.google.com/accounts/answer/185839) (Google): never share verification codes
- [Implementing Phishing-Resistant MFA \(https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf\)](https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf) (CISA fact sheet, PDF)
- [ReportFraud.ftc.gov \(https://reportfraud.ftc.gov\)](https://reportfraud.ftc.gov) (FTC)

From beaponi.com/learn/spot-phishing · Last reviewed October 18, 2026 · General education, not professional advice.