P

Phishing: Examples, Warning Signs, and What to Do After a Click

Phishing impersonates a trusted person or service to steal credentials, money, or data. Learn the main types, warning signs, verification steps, and incident response.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

In this guide

01 Common types of phishing
02 Phishing warning signs
03 How to check a suspicious message safely
04 What to do after interacting with phishing
05 How organizations reduce phishing risk
06 Frequently asked questions

Phishing is an impersonation attack that tries to make a person reveal credentials, approve access, send money, install software, or disclose sensitive information. The lure may arrive by email, text, phone, social media, a search advertisement, or a QR code. It often imitates a bank, delivery company, employer, colleague, government agency, or online service.

The stolen-access objective is often described as credential harvesting. In business conversations, email thread hijacking can make the lure unusually convincing by placing a fraudulent request inside a familiar exchange; verify consequential requests through a separate channel.

A phishing message does not need spelling mistakes to be fraudulent. Convincing branding, personal details, a valid HTTPS certificate, and even a real sign-in page used in the wrong authorization flow can all appear in modern attacks.

01 Common types of phishing

Type	How it reaches the target	Typical objective
Email phishing	Bulk or targeted messages with links, attachments, invoices, or alerts.	Credentials, malware delivery, or payment fraud.
Spear phishing	A tailored message using a person's role, contacts, or current project.	Access to a specific account or organization.
Smishing	SMS or messaging-app notices about deliveries, tolls, accounts, or prizes.	Payment details or mobile credentials. See smishing.
Vishing	A phone or voice message impersonates support, a bank, or an authority.	MFA codes, remote access, or urgent transfers.
QR phishing	A QR code hides the destination until it opens on a phone.	Fake sign-in or payment pages.
Consent phishing	A malicious cloud application requests access to mail, files, profile data, or contacts.	Persistent account access without stealing the password.

Type	How it reaches the target	Typical objective
Adversary-in-the-middle phishing	A proxy relays a real sign-in flow while capturing credentials and session tokens.	Session takeover, sometimes despite ordinary MFA.

02 Phishing warning signs

- The complete sender address, reply-to address, or domain does not match the claimed organization.
- The message creates urgency, fear, secrecy, or an unexpected reward.
- A request asks for a password, MFA code, passkey approval, gift card, cryptocurrency, bank transfer, or remote-control software.
- The visible link text and actual destination differ, or the domain contains a subtle misspelling, extra word, or misleading subdomain.
- An unexpected attachment asks you to enable macros, install an update, run a script, or bypass a warning.
- You receive repeated MFA prompts or a call asking you to approve one.
- The process changes established payment or account-recovery instructions without independent confirmation.

One sign alone may have an innocent explanation. Several signs together, or any request involving credentials and money, justify independent verification.

03 How to check a suspicious message safely

1. **Pause.** Do not click the supplied link, scan its QR code, call its phone number, or open its attachment.
2. **Open a trusted route.** Use a saved bookmark, known application, previous statement, or manually typed official address.

3. **Inspect the domain.** Read the registered domain from right to left and distinguish it from subdomains. In `bank.example.attacker.test`, the controlling domain is `attacker.test`.
4. **Confirm through another channel.** Contact the person or organization using details you already trust, not those in the message.
5. **Check the request, not only the sender.** A real account can be compromised and send authentic-looking phishing to its contacts.
6. **Report it.** Use the mail or messaging provider's phishing control and the impersonated organization's official reporting route.

04 What to do after interacting with phishing

You clicked but entered nothing

- Close the page and do not approve downloads, notifications, or application permissions.
- Delete any unexpected download without opening it and run an updated security scan if a file executed or the browser behaved unexpectedly.
- Do not assume that a click alone exposed every account; focus the response on what the site asked for and what the device did.

You entered a password or MFA code

1. Go directly to the genuine service from a clean, trusted device.
2. Change the exposed password and any other account using the same or a similar password.
3. Sign out other sessions, review recovery details and forwarding rules, and remove unknown devices, passkeys, application passwords, and connected applications.
4. Enable multi-factor authentication; prefer passkeys or security keys where supported.
5. Contact the provider or workplace security team, especially if the account contains business, payment, or identity data.

You opened an attachment or installed software

- Disconnect the device from networks if suspicious execution, encryption, pop-ups, or remote control begins.
- Do not use the possibly affected device to change important passwords.
- Run an approved full or offline security scan and preserve relevant messages, filenames, URLs, and alert details.
- For a managed device, contact IT or incident response before deleting evidence or rebuilding it.

You sent money or personal information

- Contact the bank, card issuer, payment service, or employer through a verified number immediately.
- Ask whether the transfer can be stopped and what account protections are available.
- Monitor affected accounts and follow the identity-theft reporting process for the relevant country.

05 How organizations reduce phishing risk

- Use phishing-resistant authentication and conditional access for sensitive accounts.
- Configure email authentication and filtering, but do not treat them as a replacement for verification.
- Provide a simple reporting button and investigate reported messages quickly.
- Require out-of-band confirmation for payment, payroll, vendor, and account-recovery changes.
- Limit application consent, administrative privileges, script execution, and access from unmanaged devices.
- Practice realistic response procedures without blaming employees who report mistakes promptly.

06 Frequently asked questions

Can opening a phishing email infect a device?

Simply reading an ordinary message is usually less risky than opening an attachment, following a link, granting permission, or running a file. However, software vulnerabilities and externally loaded content can create additional risk, so keep the mail client and browser updated.

Does HTTPS mean a sign-in page is legitimate?

No. HTTPS protects the connection to the domain shown in the address bar; it does not prove that the domain belongs to the organization being impersonated.

Is phishing the same as social engineering?

Phishing is a common form of social engineering. Social engineering is the broader category of manipulating people, while phishing typically uses a message or website to deliver the deception.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com