CyberGuardLab

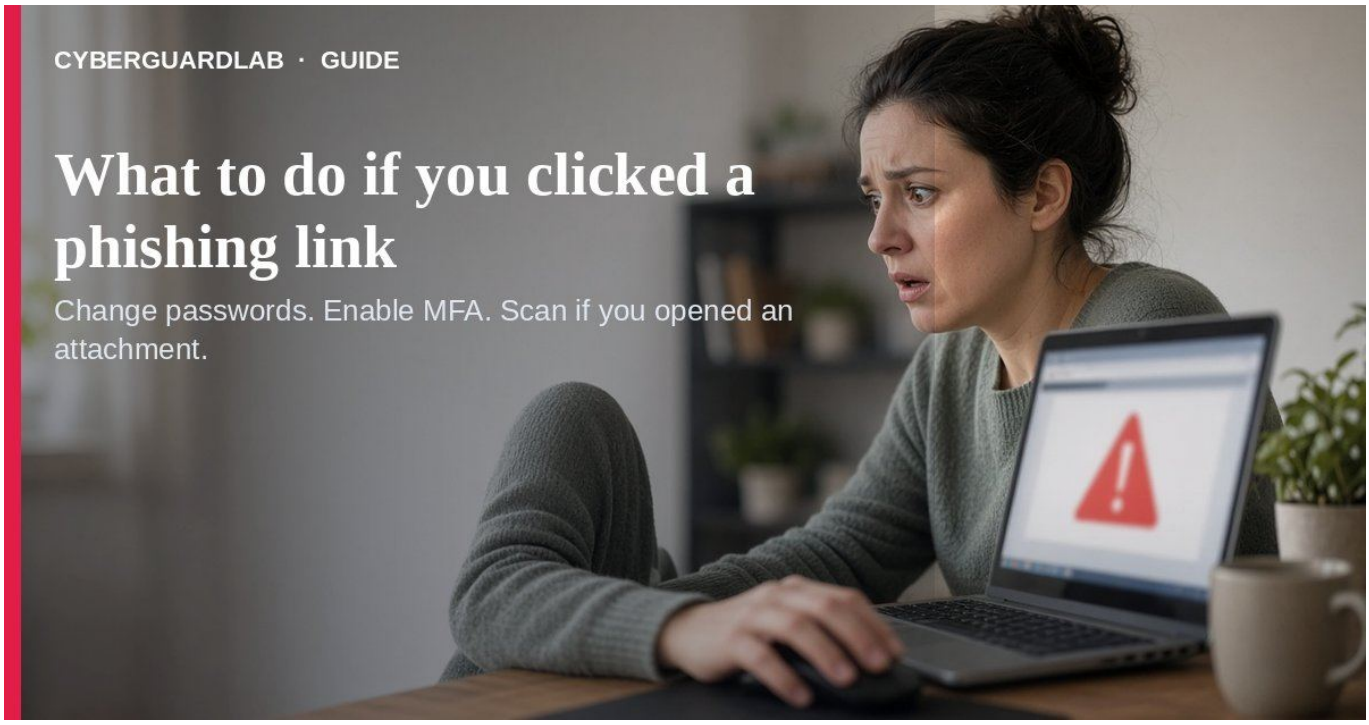
Household antivirus, explained

cyberguardlab.com

# What to do if you clicked a phishing link

https://cyberguardlab.com/blog/clicked-phishing-link-first-hour

Independent US household comparison site. Not the vendor. Paid links below may earn a commission. Confirm first-year price, renewal, device limit, and refund terms at checkout.




You clicked a phishing link (or opened a phishing attachment) when a message tricked you into visiting a fake site or downloading something harmful. Per the FTC, if you think a scammer has your Social Security, credit card, or bank details, start at IdentityTheft.gov; if you think malware downloaded, update your security software, run a scan, and remove what it finds.

This guide is the first-hour recovery after a click, not how to spot a phishing email before you click. Stay calm: most households can lock accounts down without buying anything if Defender (or your phone's built-in protections) is already on.

**Paid link**

**Norton 360 | See the Norton first-year offer**




## 1. First 15 minutes - stop the damage

From FTC phishing advice and CISA "recognize and report" guidance:

* Disconnect if you entered a password on a fake page. Close the tab. On Wi?Fi you do not trust, switch networks or turn off Wi?Fi briefly while you change passwords from a known-good device.
* Change the password for the account the phish targeted (bank, email, shopping, employer portal) using a device/browser you trust - not the fake page's "reset" form.
* Change your email password next if the phish might have captured it - email resets everything else. See hacked email or social account.
* Turn on multi-factor authentication where it is missing - FTC lists MFA as a core phishing defense. Household walkthrough: turn on 2FA.
* Do not call numbers or reuse links from the phishing message. Contact the company via the app, statement, or website you type yourself (CISA).

## 2. If you entered financial or SSN details

* Go to IdentityTheft.gov for steps matched to what was stolen (FTC).
* Call the number on the back of your card or in your banking app for unauthorized charges - see also credit card fraud first hour and bank account hacked.
* Place fraud alerts / consider a credit freeze if SSN or identity data was shared - see credit freeze vs identity monitoring.
* Check whether your email appears in known breaches: check email data breach.

## 3. If you fear malware from a link or attachment

FTC: update security software, run a scan, remove problems it finds.

* On Windows, update Microsoft Defender and run a full scan; for stubborn infections consider an Offline scan.
* On phone, update the OS, remove unknown apps, and on Android run Play Protect.
* Uninstall shady browser extensions: remove scam Chrome extension.

* Back up important files once the device is cleaned (FTC lists backups as phishing protection).

## 4. Report and warn the household

* Forward phishing email to reportphishing@apwg.org; forward phishing texts to 7726 (SPAM) - FTC.
* Report at ReportFraud.ftc.gov - report a scam to the FTC.
* Tell family members which message was fake so they do not click the same lure.
* Review recent sign-ins on Google, Apple, Microsoft, and bank apps for unknown devices.

## FAQ

### What should I do first after clicking a phishing link?

Close it, change the targeted account password from a trusted device, enable MFA, then scan for malware if you opened an attachment or installed anything (FTC).

### Is clicking always game over?

No. Many phish fail if you did not enter credentials or download malware. Still change passwords for anything you typed and report the message.

### Where do I go if they have my SSN or bank numbers?

IdentityTheft.gov plus your bank/card issuer (FTC). Also see report identity theft.

### How is this different from "how to spot phishing"?

Spotting is prevention; this page is recovery after a click. Start with how to spot a phishing email next time.

### Do I must buy antivirus right now?

No. Defender + OS updates + password/MFA changes are a valid buy-nothing path. Paid suites are optional - see Is Microsoft Defender enough?.

## If you still want a paid suite

Recovery after a phishing click does not require a paid suite if Defender (or your phone's built-in tools) is current. If the household wants multi-device paid protection, use only these on-site paid links: TotalAV (paid link), Norton (paid link), Bitdefender (paid link), McAfee (paid link), Avast (paid link).

## Sources

* How To Recognize and Avoid Phishing Scams (FTC)
* Recognize and Report Phishing (CISA)
* ReportFraud.ftc.gov (FTC)
* IdentityTheft.gov (FTC)

## Also read

* How to spot a phishing email
* How to turn on 2FA for Gmail, Apple, and bank
* What to do if your email or social account is hacked
* How to check if your email is in a data breach
* What to do if your credit card is used fraudulently
* How to run a Microsoft Defender Offline scan
* How to report a scam to the FTC
* How to report identity theft at IdentityTheft.gov