Everyday Soul — CyberScrolls Series

EP07 – After the Click

By Helen Najar | Lionheart

Guides, prevention tips, and poetic scrolls to help you defend, recover, and navigate digital storms with clarity and courage.

⚡ Quick Actions — If You Just Want the Fast Steps

1. **Close the page** — stop interacting.
2. **Disconnect** — turn off Wi-Fi or unplug the Ethernet cable.
3. **Change passwords** on a trusted device (email → banks → stores).
4. **Run a full antivirus scan** on the infected device.
5. **Monitor accounts** and call your bank immediately if you see unauthorized charges.

Keep this page bookmarked. Do the quick actions now, then read the full steps below.

Full Guide — Detailed Steps

1. First thing to know (breath, don't panic)

A wrong click happens to good people. Acting quickly matters — and calm, correct steps stop most damage. This guide moves from immediate actions to follow-up and monitoring.

2. Close the page and stop interacting

Why: Phishing pages sometimes trigger downloads, run scripts, or ask for more details. The moment you stop, you reduce risk.

How (simple):

- **On a desktop or laptop:** click the window's close button (X), or press Alt + F4 on Windows, or Command + W on macOS to close the tab or window. Do not type, enter credentials, or click any buttons such as "Download" or "Allow."
- **On mobile:** tap your browser's tab switcher and swipe the page closed or tap the close button. Do not fill forms or tap "OK."

If a download started:

- Do not open the downloaded file. Delete it from your Downloads folder once you're on a trusted device.

3. Cut the signal (disconnect the device)

Why: Disconnecting stops data from leaving or remote parties from interacting with your device.

How to disconnect (choose one):

- **Unplug the Ethernet cable from your laptop or desktop** — physically pull it out. (This is immediate and sure.)
- **Turn off Wi-Fi:**
  - **Windows:** Click the Wi-Fi icon in the taskbar → click the Wi-Fi button to toggle off.
  - **Mac:** Click the Wi-Fi icon in the menu bar → Turn Wi-Fi Off.

  - **iPhone:** Control Center → tap Wi-Fi to disable; or Settings → Wi-Fi → toggle off.
  - **Android: Quick Settings → toggle Wi-Fi off; or Settings → Network & internet → Wi-Fi → toggle off.**
- **If using mobile data only:** Turn on Airplane Mode (quickest way to cut all signals).
- **If the attacker opened remote access (rare):** Shut the device down completely (power off) and do not reconnect it until you scan from another trusted device.

Why physical unplugging matters: A physical disconnect cannot be bypassed by scripts on the page.

---

4. Use a trusted device to change passwords (order and method)

Important: Use a device you *did not* click from — ideally your phone that was not used, or a separate, known-clean computer.

Priority order (do these first)

1. **Resetting your email account** password protects all recovery flows and linked accounts.
2. **Primary financial accounts** — banks, credit cards, PayPal, mobile payment apps.
3. **Crypto/exchange accounts** — exchanges, wallets (if exchange), or move funds to a cold wallet if you can.
4. **Social media & shopping accounts** (Amazon, Apple, Google Play, etc.)
5. **Other critical services** (work accounts, healthcare portals, cloud storage).

How to change a password (safe method):

- Go directly to the official website or app (do not click links from emails). Example: open https://www.gmail.com manually.
- Navigate to account security settings → change password. Use long, unique passwords.
- **Password guidance:**
  - Use a password manager (1Password, Bitwarden, LastPass) to create and store long random passwords.
  - If not using a manager, use passphrases: three random words + punctuation + number (e.g., Aurora!Stone7River).
- **Enable MFA (multi-factor authentication)** right away (see below).

Sign out everywhere / revoke sessions

- On major providers you can review “logged in devices” and revoke sessions. Do this after changing the password.

- **Google:** Security → Your devices → Sign out of suspicious devices.
- **Facebook / Instagram / Twitter:** Security → Where you're logged in → Log out everywhere.
- **Banks:** Many banks show "active sessions" or let you reset tokens.

---

5. Enable or reinforce MFA (Multi-Factor Authentication)

Why: A password alone is vulnerable. MFA prevents attackers from logging in even if they have your password.

Recommended MFA methods (best to good):

1. **Authenticator apps** (Microsoft Authenticator, Google Authenticator, Authy) — safest.
2. **Physical security keys** (YubiKey) highest security for accounts that support them.
3. **SMS codes** — better than nothing but vulnerable to SIM swap attacks.

How:

- **Use a trusted device:** Go to Account → Security → Two-Step Verification (or 2FA) → Add Authenticator App or Security Key.
- Write down recovery codes and store them offline (not as plain text on the device).

---

6. Run full antivirus/antimalware scans on the affected device

Why: Some phishing attacks drop malware. Scanning finds and removes known threats.

Windows (Microsoft Defender — built in)

1. Open **Start** → type **Windows Security** → open.
2. Go to **Virus & threat protection** → **Scan options** → choose **Full scan** → **Scan now**.
3. When finished, follow instructions to remove/quarantine items.
4. For stubborn threats, use **Windows Defender Offline scan** (restarts into a trusted environment).

macOS

- macOS does not include a user-facing built-in AV scanner like Windows, but Apple has built-in protections (XProtect). For extra assurance, install **Malwarebytes for Mac** and run a full scan. Follow the app's removal instructions.

Linux

- Use **ClamAV** or distro-recommended tools (command line). If unsure, consult a trusted technician.

Mobile (iOS/Android)

- **Android:** Use Play Protect and/or install Malwarebytes, Bitdefender mobile, or similar. Run a scan and remove suspicious apps.
- **iOS:** iOS is harder to infect; if you saw a suspicious app installed, delete it. Update iOS and check for profiles in Settings → General → VPN & Device Management; remove unknown profiles.

If malware is found

- Follow the scanner's recommended removal steps.
- If the device still behaves oddly after cleanup, consider **reinstalling the OS** or factory-resetting (backup important files first) and restoring only clean data.

---

7. Browser checks (extensions, saved passwords, autofill)

Why: Phishing or malicious scripts often add rogue extensions or harvest saved credentials.

What to do:

- **Clear your browser cache and cookies** (Settings → Privacy → Clear browsing data).
- **Check extensions/add-ons**: remove anything you don't recognize.
- **Check saved passwords** in the browser; remove entries that look suspicious. Prefer a password manager instead.
- **Check autofill addresses and payment info** and remove anything unfamiliar.
- **Reset browser settings** to defaults if you notice redirects or odd behavior.

---

8. Financial steps: check accounts, alert banks, and dispute fraud

Why: If credentials or payment details were exposed, quick bank contact can limit losses.

Immediate checklist

- Log into your bank/credit card from a trusted device. Check recent transactions for unauthorized charges.
- If you see suspicious movement, call your bank's fraud line immediately. Use numbers from the back of your card or the bank's official website (not links in emails).

- Ask the bank to freeze or monitor your account; ask about charge reversals and fraud alerts.
- For credit cards: request a new card if details were exposed.

Script for calling the bank:

"Hello — I'm calling because I may have clicked a potentially malicious link, and I want to check my account activity and place a fraud alert. Can you review recent transactions and advise next steps?"

For crypto

- If you sent funds or keys were compromised, contact the exchange support immediately. If possible, move remaining funds to a cold wallet (hardware wallet) and enable all security measures on the exchange (MFA, IP whitelisting).

9. Reporting the phishing or fraud

- **Report to your email provider** — for example, Gmail or Outlook — using their built-in "Report Phishing" option.
- **Report to the impersonated company** — if the email pretended to be from a bank, store, or known brand.
- **Report to local authorities** — if financial theft occurred. Obtain a police report if needed for disputes.
- **Report to your workplace IT or security team** — if the incident happened on a work device or network, notify them immediately.

10. Monitoring & follow-up (timeline)

First 24 hours:

- Close page, disconnect, change passwords for email + bank, run antivirus, call your bank if needed.

24–72 hours:

- Review devices and app permissions, revoke suspicious sessions, enable MFA, and create a timeline of the event (screenshots, emails).

First 2 weeks:

- Monitor bank/credit card statements daily.
- Watch email for password reset notices you didn't initiate.

30–90 days:

- Consider a credit monitoring or identity theft protection service if sensitive info was exposed.

- If the attack included identity theft, file a police report and follow credit bureau recovery steps in your country.

11. Prevention Tips

- Use an **up-to-date password manager** and unique passwords for every account.
- Always enable **MFA** with an authenticator app or security key where possible.
- Never click links in suspicious emails — hover to check the URL or go directly to the official site.
- Learn the common red flags: urgent language, spelling errors, mismatched domain, unexpected attachments.
- Keep your OS, browser, and antivirus definitions updated.

12. Printable Quick Checklist

- Close the suspicious page (do not interact).
- Turn off Wi-Fi or unplug ethernet / enable airplane mode.
- On a trusted device: change email password → bank passwords → other high-value accounts.
- Enable or confirm MFA on all critical accounts.
- Run full antivirus scan and follow removal steps.
- Review browser extensions, saved passwords, and autofill.
- Check bank/credit card activity; call the bank if anything suspicious.
- Report to your email provider and the impersonated company.
- Maintain daily monitoring for 30 days.

13. Helpful Templates

Email to a friend or tech helper:

"I clicked a suspicious link on my [device]. I've disconnected it and changed passwords on a trusted device. Could you help me run a malware scan and check my backup? I don't want to restore anything that might be infected."

Script for a bank:

"I may have been phished. Please check for unauthorized charges and place a fraud alert on my account. I'd like to freeze the card if you advise."

If you need to ask a security-savvy friend to help:

"If you have a few minutes, can you help me check this laptop? I will not reconnect it to the internet until I get your okay."

14. Resources

- Use official vendor help pages for step-by-step: your bank website, Google Account Help, Microsoft Support, Apple Support.
- For malware removal: vendor pages for Malwarebytes, Microsoft Defender, Bitdefender, etc.
- For identity protection: check local government or consumer protection sites for instructions to freeze credit or report identity theft.

15. Reflection — the Lionheart reminder

A wrong click doesn't end the voyage; it teaches how precious the helm is.
Move steady. Protect the heart of your life — your accounts, your identity, your peace.

Appendix — Technical commands & quick references

Windows — quick defender full scan (manual steps)

1. Start → type **Windows Security** → Open.
2. Click **Virus & threat protection** → **Scan options** → select **Full scan** → **Scan now**.

Google Account — sign out everywhere

- Google Account → Security → Your devices → Manage devices → Sign out.

How to clear browser cache (Chrome)

- Menu (three dots) → More tools → Clear browsing data → choose “All time” → Clear data.