NSHE CYBERSECURITY AWARENESS MONTH · OCTOBER 2026

Laying Low

Your step-by-step guide to a smaller attack footprint

Companion handout to the session presented by
Garess Espinosa, Principal Solutions Architect at Arctiq

Before you start. These steps are for your **personal devices and home network**. On university-managed computers and accounts, follow your campus IT department's guidance, since campus systems may already filter DNS and manage updates for you.

Two habits that make every step easier. Write down a setting before you change it, so you can switch back. If a menu name doesn't match what you see, search your device's settings for the word in **bold**.

What's inside

1. Your home router: the front desk
2. Secure DNS with Cloudflare 1.1.1.3
3. The hosts file, for shared computers
4. Stop email tracking pixels
5. Block trackers and add one ad blocker
6. Remove the location from your photos
7. Smart devices: does it need the internet?
8. Passwords, multi-factor authentication, and passkeys
9. Turn on automatic updates
10. Freeze your credit
11. Spot and stop scams
12. If something goes wrong

START HERE

Your quick-start checklist

The first five items are the action items from the session. Pick two tonight and finish the rest this week. Times are approximate.

Done	Action	Where	Time	Page section
☐	**Secure DNS (1.1.1.3)**	**Router, or each device**	**5–10 min**	**Step 2**
☐	**Email images off**	**Each email app**	**2 min**	**Step 4**
☐	**Photo location off**	**Phone camera**	**2 min**	**Step 6**
☐	**Ask: does it need the internet?**	**Smart devices**	**10 min**	**Step 7**
☐	**One ad blocker**	**Each browser**	**3 min**	**Step 5**
☐	Router basics	Router admin page	10–15 min	Step 1
☐	Password manager and MFA	Email first, then the rest	20+ min	Step 8
☐	Automatic updates	Phone, computer, browser	5 min	Step 9
☐	Credit freeze	Three credit bureaus	a few min each	Step 10

The three habits behind everything: unique passwords plus multi-factor authentication, keep things updated, and slow down. The FBI's phrase for that last one is "take a beat."

STEP 1

Your home router: the front desk

Your router gives the whole house one public address and keeps strangers at the front desk. These settings keep the front desk attended.

1. **Find the admin page.** Look on the router's label for the address (often something like 192.168.0.1 or 192.168.1.1), or open your internet provider's or router maker's app.
2. **Change the administrator password.** This is the password for managing the router, not your Wi-Fi password. Use a long, unique passphrase and save it in your password manager.
3. **Update the firmware.** Look for **Firmware** or **Software update**, and turn on **automatic updates** if offered. If the maker no longer releases updates, plan to replace the router.
4. **Turn off remote management** (sometimes called remote access or web access from the internet) unless you set it up on purpose.
5. **Turn on the guest network.** Give it its own password, and use it for visitors and smart devices.
6. **Use strong Wi-Fi security.** Choose **WPA3**, or **WPA2/WPA3** if some older devices need it.

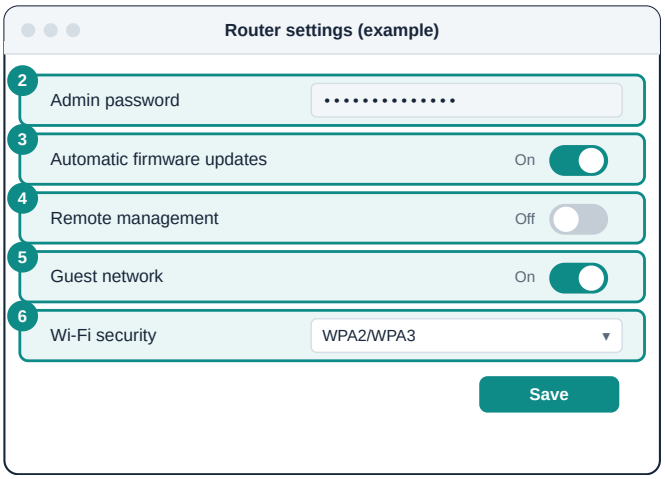


Illustration only. Menus and wording vary by device and software version. Numbers match the steps.

STEP 2

Secure DNS with Cloudflare 1.1.1.3

Cloudflare's free 1.1.1.1 for Families service answers your device's "what's the address for this name?" questions and refuses to answer for known malicious and adult sites. Set it once on your router to cover the whole house, or set it on each device.

What you enter	Value for 1.1.1.3 (blocks known malware and adult content)
Primary DNS (IPv4)	`1.1.1.3`
Secondary DNS (IPv4)	`1.0.0.3`
IPv6 (if asked)	`2606:4700:4700::1113` and `2606:4700:4700::1003`
Encrypted DNS hostname (Android Private DNS)	`family.cloudflare-dns.com`
DNS over HTTPS address (if your router or browser asks)	`https://family.cloudflare-dns.com/dns-query`

Prefer to block only malware? Use `1.1.1.2` and `1.0.0.2` (hostname `security.cloudflare-dns.com`) instead.

> A filter, not a force field. It works from lists of known bad sites, so brand-new ones can slip through. And remember: on university-managed devices, leave DNS as your IT team set it.

2A. On your home router (covers every device at home)

1. Log in to the router's admin page (see Step 1).
2. Find the **DNS** settings. They are often under **Internet**, **WAN**, or **DHCP/LAN**.
3. Replace the automatic DNS servers with `1.1.1.3` and `1.0.0.3`.
4. Select **Save**, then restart the router if asked.

Some internet-provider routers lock the DNS setting. If yours does, set DNS on each device instead (below).

2B. Windows 11

1. Select **Start** > **Settings** > **Network & internet**.
2. Select the connection you use, **Wi-Fi** or **Ethernet** (for Wi-Fi, open your network's properties).
3. Next to **DNS server assignment**, select **Edit**.
4. Change **Automatic (DHCP)** to **Manual**.
5. Turn on **IPv4**. Enter `1.1.1.3` as Preferred DNS and `1.0.0.3` as Alternate DNS.
6. Optional: turn on **IPv6** and enter the IPv6 addresses from the table.
7. Select **Save**.

Windows 10: Settings > Network & Internet > Change adapter options > right-click your connection > Properties > Internet Protocol Version 4 > Properties > **Use the following DNS server addresses**.

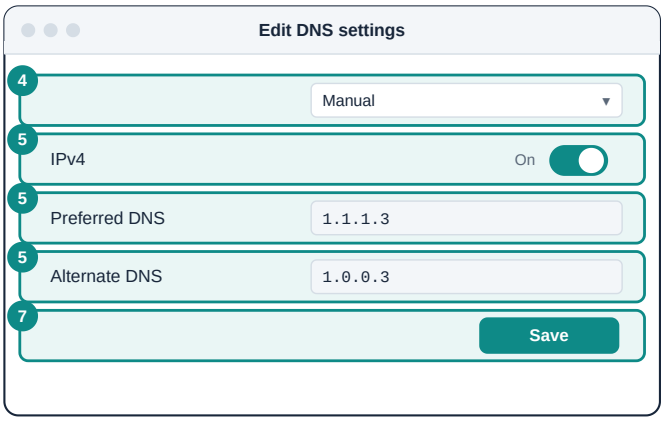


Illustration only. Menus and wording vary by device and software version. Numbers match the steps.

2C. Mac

1. Open **System Settings** (press Command + Space and type System Settings).
2. Select **Network**, then your connection (**Wi-Fi** or **Ethernet**).
3. Select **Details**, then **DNS**.
4. Under **DNS Servers**, select **+** and enter `1.1.1.3`. Select **+** again and enter `1.0.0.3`.
5. Select **OK**.

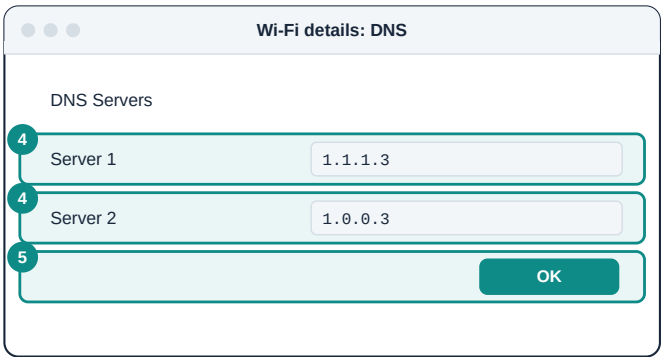


Illustration only. Menus and wording vary by device and software version. Numbers match the steps.

2D. iPhone and iPad

Option 1 (recommended, works on cellular too): the free “1.1.1.1: Faster Internet” app from Cloudflare.

1. Install the app from the App Store and accept the terms.
2. Install the profile the app asks for, then switch it to **Connected**.
3. Tap the **menu** button, then **Advanced** > **Connection options**.
4. Under **DNS settings** > **1.1.1.1 for Families**, choose the option that blocks malware and adult content.

Option 2: manual, Wi-Fi only. Repeat it for each Wi-Fi network; it does not cover cellular.

5. Open **Settings** > **Wi-Fi**, and tap the **(i)** next to your network.
6. Scroll down and tap **Configure DNS**, then choose **Manual**.
7. Remove the existing servers, tap **Add Server**, and enter `1.1.1.3`, then `1.0.0.3`.
8. Tap **Save**.

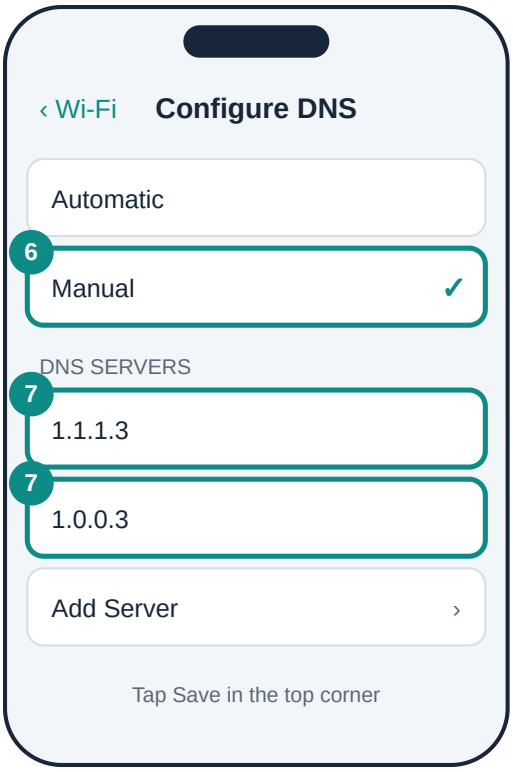


Illustration only. Menus and wording vary by device and software version.

2E. Android (version 9 and later)

1. Open **Settings** > **Network & internet**. (On many Samsung phones: **Settings** > **Connections** > **More connection settings**.)
2. Tap **Private DNS** (it may be under **Advanced**).
3. Choose **Private DNS provider hostname**.
4. Enter `family.cloudflare-dns.com` and tap **Save**.

Private DNS is encrypted and applies on Wi-Fi and cellular. Cloudflare’s app (Option 1 above) is also available on Google Play.

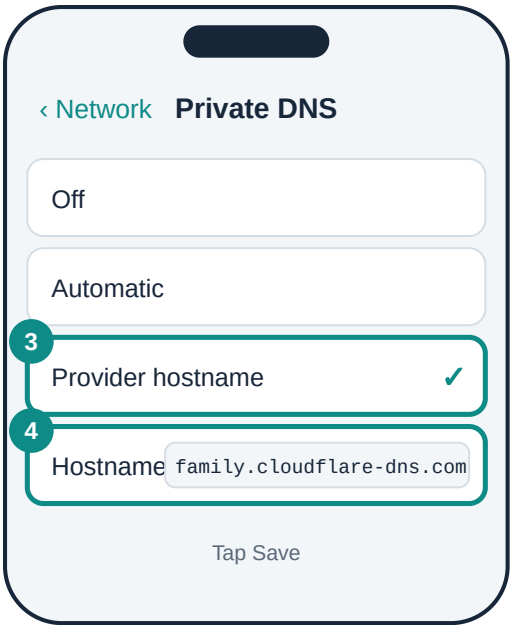


Illustration only. Menus and wording vary by device and software version.

2F. Check that it works

1. On the device you just set up, visit `https://malware.testcategory.com/`. With the filter working, the page should **not** load.
2. Cloudflare’s setup page lists a second test address for the adult-content filter.

> **Hotel or coffee-shop Wi-Fi won’t show its login page?** Some sign-in pages fail with a custom DNS setting. Switch back to Automatic, sign in, then switch DNS back.

STEP 3

The hosts file, for shared computers

Your computer checks this small file before it asks DNS. A line in it can send a website name to a dead-end address. **This is not a security tool:** it is a quick way to control access on a shared family or lab computer, and anyone with administrator rights can undo it.

Windows

1. Select **Start**, type **Notepad**, right-click it, and choose **Run as administrator**.
2. Select **File** > **Open**, go to `C:\Windows\System32\drivers\etc`, change the file type to **All files**, and open **hosts**.
3. At the bottom, add a line such as `0.0.0.0 distracting-site.example`. Add a second line for the `www.` version.
4. Save the file. Optional: open Command Prompt as administrator and run `ipconfig /flushdns`.

Mac

1. Open **Terminal** and type `sudo nano /etc/hosts`, then enter your Mac password.
2. Use the arrow keys to go to the bottom and add the same lines.
3. Press Control + O, then Return to save, and Control + X to exit.
4. Clear the cache: `sudo dscacheutil -flushcache; sudo killall -HUP mDNSResponder`

hosts (example)

```
# Lines starting with # are comments
127.0.0.1       localhost
0.0.0.0         distracting-site.example
0.0.0.0         www.distracting-site.example
```

Illustration. The two highlighted lines block one example site on this computer only.

> **To undo it,** delete the line or put a `#` at the start. **If you open the file and find entries you didn't write,** call your IT help desk, because malware sometimes edits it. And, as promised in the session: please don't use this to prank your significant other.

STEP 4

Stop email tracking pixels

A tracking pixel is a tiny hidden image. When your email app loads it, the sender learns your address is real and that you just opened the message. Turning off automatic image loading keeps the dot quiet.

Gmail on the web

1. Select the **gear** icon, then **See all settings**.
2. On the **General** tab, find **Images**.
3. Choose **Ask before displaying external images**.
4. Scroll to the bottom and select **Save Changes**.

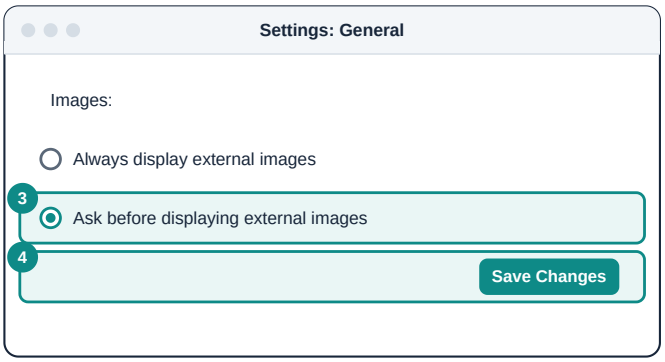


Illustration only. Menus and wording vary by device and software version. Numbers match the steps.

Gmail app (Android, iPhone, iPad)

1. Tap the **menu**, then **Settings**, then your account.
2. Tap **Images** and choose **Ask before displaying external images**.

After setting it on the web, open the Gmail app on your phone and confirm it took.

Apple Mail

1. **iPhone or iPad:** open **Settings** > **Apps** > **Mail** > **Privacy Protection** (on older versions, Settings > Mail). Turn on **Protect Mail Activity**, which loads content privately and hides your IP address. To stop images entirely instead, turn it off and turn on **Block All Remote Content**.
2. **Mac:** in Mail, choose **Mail** > **Settings** > **Privacy**, and use the same options.

Outlook

1. **Outlook on the web and the new Outlook: Settings** > **General** > **Privacy and data** > **External images**, and choose **Always use the Outlook service to load images**.
2. **Classic Outlook for Windows: File** > **Options** > **Trust Center** > **Trust Center Settings** > **Automatic Download**, and keep **Don’t download pictures automatically** checked.

> Services that load images through their own servers hide your IP address, but opening the message can still be confirmed. “Ask before displaying” is the strongest choice.

STEP 5

Block trackers and add one ad blocker

One web page can pull in dozens of outside services. Your browser can block many of the trackers, and an ad blocker removes a common hiding place for malicious ads, which the FBI has recommended using while searching.

Turn on tracker blocking

1. **Safari: Prevent Cross-Site Tracking** is on by default. Check it on iPhone under Settings > Apps > Safari.
2. **Firefox:** Settings > **Privacy & Security** > **Enhanced Tracking Protection**, and choose Standard or Strict.
3. **Chrome:** Settings > **Privacy and security** > **Third-party cookies** > **Block third-party cookies**.
4. **Edge:** Settings > **Privacy, search, and services** > **Tracking prevention**, and choose Balanced or Strict.

Add one reputable ad blocker

5. Install only from your browser's **official store**: Chrome Web Store, Firefox Add-ons, Microsoft Edge Add-ons, or the App Store for Safari.
6. Choose a well-known option and check the developer and reviews. Common choices: uBlock Origin (Firefox), uBlock Origin Lite (Chrome, Edge), and AdGuard (Safari).
7. Install **one**, not five. On a university-managed device, ask IT first.

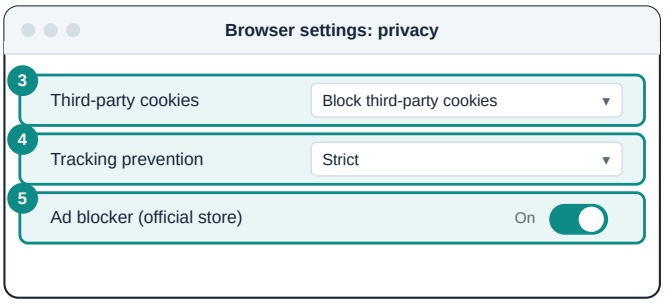


Illustration only. Menus and wording vary by device and software version. Numbers match the steps.

> **The rule that matters most:** never download software from an ad or a search result. Type the company's address yourself, use a bookmark, or use your device's official app store. That is how the 2025 Nevada state attack began.

STEP 6

Remove the location from your photos

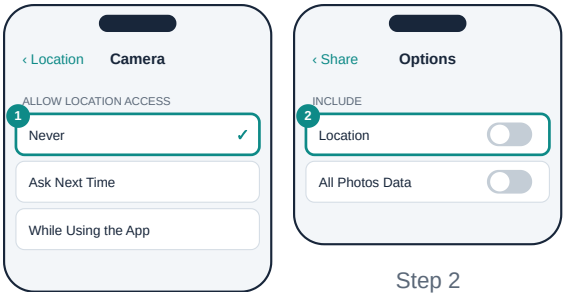
Phone photos can carry hidden GPS coordinates. You can stop that at the camera, or strip it when you share.

iPhone

1. **Stop it at the source:** Settings > **Privacy & Security** > **Location Services** > **Camera** > **Never**.
2. **Strip it when sharing:** tap **Share**, tap **Options** at the top, and turn off **Location**.
3. **Remove it from a photo you already took:** open it in Photos, tap **(i)**, tap **Adjust** next to the location, and choose **No Location**.

Android

4. Open the **Camera** app and tap the **settings** (gear) icon.
5. Turn off **Save location** (Google Pixel) or **Location tags** (Samsung). Other phones use similar wording.
6. In Google Photos, check the privacy settings for location before sharing albums by link.



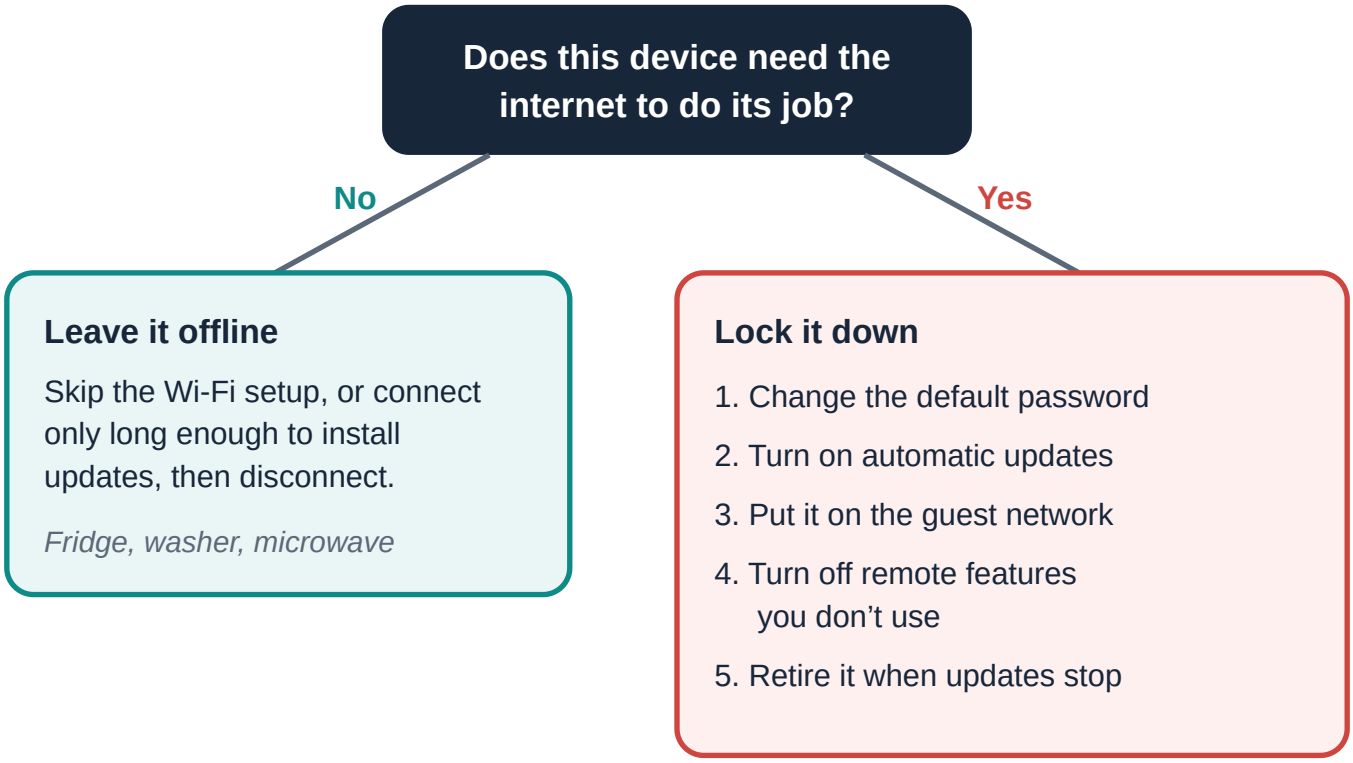
Step 1 Step 2

Illustration only. Menus and wording vary by device and software version.

STEP 7

Smart devices: does it need the internet?

Connected TVs, doorbells, cameras, thermostats, and appliances are often built to be cheap and convenient, not secure. Walk through each one.



Do you really need to download the automatic setting for roasting a chicken? If not, the microwave can stay offline.

1. **Make a list** of every device at home that connects to Wi-Fi, other than phones and computers.
2. For each one, ask the question in the chart.
3. **If it doesn't need the internet:** skip the Wi-Fi setup, or connect it only long enough to install updates.
4. **If it does:** change the default password, turn on automatic updates, move it to the guest network (Step 1), and turn off remote features you don't use.
5. **When the maker stops releasing updates,** retire the device or take it off the network. A smart TV can go back to being a regular TV with an inexpensive streaming stick that still gets updates.

STEP 8

Passwords, multi-factor authentication, and passkeys

Microsoft reports that more than 97% of identity attacks are password attacks, and that multi-factor authentication blocks over 99% of identity-based attacks.[1]

1. **Pick a password manager.** The one built into your phone or browser (such as Apple's Passwords app or Google Password Manager) or a reputable standalone app.
2. **Protect it** with a long passphrase you don't use anywhere else, and turn on multi-factor authentication for it.
3. **Start with your email account.** Give it a unique password and turn on multi-factor authentication. Email is the key to resetting everything else.
4. **Then do your bank, phone carrier, social media, and shopping accounts.** Let the password manager create a new random password for each one.
5. **Choose the strongest second factor offered:** a passkey or hardware security key first, then an authenticator app, and text messages only if nothing else is available.
6. **Turn on passkeys where offered.** Look in the account's **security** settings for **passkey**. A passkey can't be typed into a fake website.
7. **Save the backup codes** each site gives you, in your password manager or a safe place.

STEP 9

Turn on automatic updates

Verizon's 2026 breach report found that exploiting software weaknesses is now the most common way a breach begins.[2] Updates close those doors.

1. **Windows 11:** Settings > **Windows Update**. Select **Check for updates**, and turn on **Get the latest updates as soon as they're available**.
2. **Mac:** System Settings > **General** > **Software Update**, then select the **(i)** next to Automatic updates and turn the options on.
3. **iPhone and iPad:** Settings > **General** > **Software Update** > **Automatic Updates**, and turn them on.
4. **Android:** Settings > **System** > **Software update** (on Samsung: Settings > **Software update**). Wording varies by phone.
5. **Browsers:** restart your browser when it says an update is ready.
6. **Router and smart devices:** see Steps 1 and 7.

STEP 10

Freeze your credit

A credit freeze makes it much harder for anyone to open new accounts in your name. According to the FTC, it's free and doesn't affect your credit score.[3]

Equifax	Experian	TransUnion
Create account	Create account	Create account
Place freeze	Place freeze	Place freeze
✓ Frozen	✓ Frozen	✓ Frozen

Free · does not affect your credit score · lift it temporarily when you apply for credit

You need to freeze your credit separately at each of the three bureaus.

1. Go to each bureau's freeze page: **Equifax** `equifax.com/personal/credit-report-services/credit-freeze`, **Experian** `experian.com/freeze/center.html`, and **TransUnion** `transunion.com/credit-freeze`. Type the address yourself rather than clicking a link in an email.
2. Create an account and place the freeze.
3. Save each login or PIN in your password manager.
4. When you apply for a loan, credit card, or apartment, **temporarily lift** the freeze at the bureau the lender uses (or all three), then let it re-freeze.

STEP 11

Spot and stop scams

Today's phishing messages are written in smooth, natural language and can sound like a relative or a colleague. Judge the request, not the grammar.

From: Jordan Lee (Chair) <j.lee@univ-example-edu.com> 1

Subject: **Quick favor before 3 pm** 2

Hi Sam,

I'm stuck in a session and can't take calls. Could you pick up gift cards for our visiting speaker? I'll reimburse you today. 3 4 Just reply here when you have them.

Thanks, Jordan

1 Look-alike address, real name 2 Urgency 3 Blocks the call-back check

4 Unusual payment. Perfect grammar, so judge the request, not the spelling.

Example of a modern phishing email. The names and addresses are fictional.

Take a beat

1. **Watch for the three ingredients:** urgency ("act now"), authority ("I'm from your bank"), and secrecy ("don't tell anyone").
2. **Watch for payments that can't be reversed:** gift cards, wire transfers, cryptocurrency, or a courier picking up cash.
3. **Hang up or stop replying,** then contact the person or company using a number or address you already have, not one in the message.
4. **Agree on a family code word** that a real relative in trouble would know and a cloned voice would not.

Holiday rules

- **Don't click, go direct.** Type the retailer's address or open its app.
- **Track packages** inside your own account, never from a text link.
- **Pay with a credit card** and turn on purchase alerts.
- **Too-good price, unfamiliar site, odd payment?** Stop.
- **A message that creates panic** is a signal to take a beat.
- **Gift cards are for gifts,** never for paying someone who contacted you.

STEP 12

If something goes wrong

Move quickly, and don’t be embarrassed. Criminals run these scams as a business.

1. **Stop all contact** with the scammer.
2. **Call your bank or card issuer right away**, using the number on your card, to try to stop or reverse payments.
3. **Change passwords** for any affected account, starting with email, and turn on multi-factor authentication.
4. **Freeze your credit** (Step 10).
5. **Report it:** to the FBI at `ic3.gov`, and to the FTC at `reportfraud.ftc.gov`. For identity theft, use `identitytheft.gov` for a recovery plan.
6. **If a university account or device is involved,** contact your campus IT help desk immediately.
7. **Keep records:** the scammer’s name or company, how they contacted you, dates, payment methods, and where any money went.

> **Keep this handout.** Revisit the checklist whenever you get a new phone, computer, router, or smart device.

Sources

1. Microsoft Digital Defense Report 2025, as summarized by eSecurity Planet, Oct 17, 2025: esecurityplanet.com/de/news/ransomware-powers-cyberattacks/
2. Verizon, 2026 Data Breach Investigations Report: exploitation of vulnerabilities was the most common initial access vector (31%). Summary: helpnetsecurity.com/2026/05/25/lessons-from-verizon-dbir-2026-findings/
3. Federal Trade Commission, “Credit freeze or fraud alert: which is right for you?”: consumer.ftc.gov/credit-freeze-or-fraud-alert-right-you
4. Cloudflare Docs, 1.1.1.1: IP addresses, Set up (including 1.1.1.1 for Families and test pages), Windows, macOS, iOS, and Android guides: developers.cloudflare.com/1.1.1.1/
5. Google Help, “Turn images on or off in Gmail”: support.google.com/mail/answer/145919
6. Microsoft Support, “External image protection in Outlook.com”: support.microsoft.com/en-us/outlook/external-image-protection-in-outlook-com
7. FBI IC3 Public Service Announcement on search-engine ad impersonation, Dec 21, 2022: ic3.gov/PSA/2022/PSA221221. FBI “Take a Beat” guidance: fbi.gov/news/press-releases/cryptocurrency-and-ai-scams-bilk-americans-of-billions

Device menus are described as of October 2026 and may change with software updates. All screen images in this guide are illustrations, not screenshots of any company’s product.