

# Digital Safety

1. Device Safety
2. Online Safety

# Device Safety

- Device Settings
  - Privacy & Security
  - Location & Improvement Analytics
  - App Permissions
  - NFC (Near Field Communications - e.g. tap & pay)
- Passwords vs Pass Keys



# Online Safety

- Network Settings
- Browser Settings
- WhatsApp Settings
- Phishing



# Device Safety

## Settings

- Similar settings, as below, can be found in both iPhone and Android menus.
- Limit or switch off location and precise (aka accurate) **location services**:
  - iPhone: Settings/Privacy & Security/Location Services
  - Android: Settings/Location and
  - Android: Settings/Google/All Services/Location Accuracy

- Limit **System Services** (iPhone) and **Google Services** (Android):
  - iPhone: Settings/Privacy & Security/Location Services/System Services
  - Android: Settings/Google/All Services/System Services

- Switch off **Usage Diagnostic** and limit **AI Intelligence**:
  - iPhone: Settings/Privacy & Security/Analytics & Improvements
  - iPhone: Settings/Apple Intelligence & Siri
  - Android: Settings/Security&Privacy/More Privacy Settings/Usage & Diagnostics

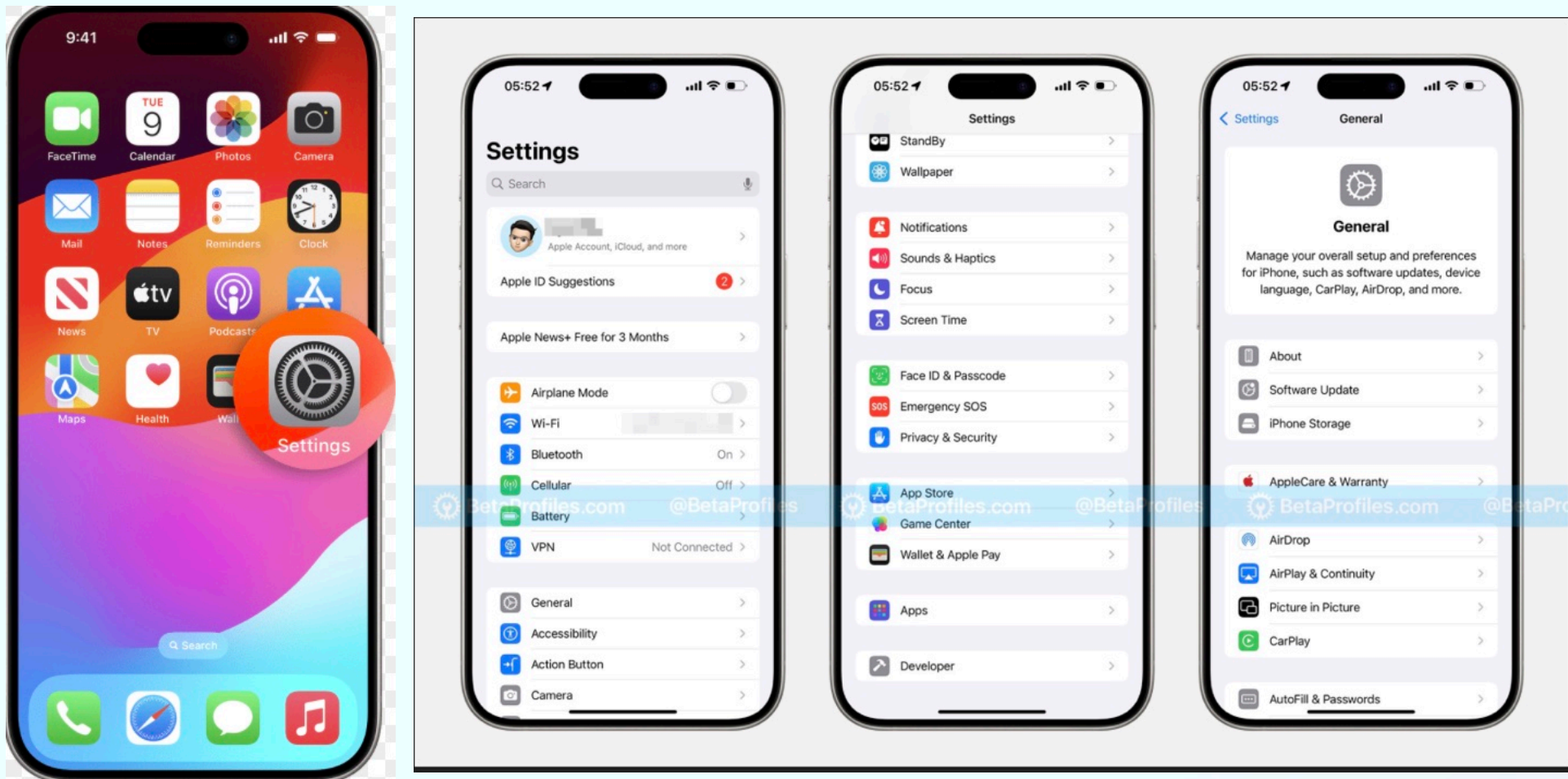
- Clear & Switch off **Personalised Ads**:
  - iPhone: Settings/Privacy & Security/Apple Advertising
  - Android (Reset Ad ID): Settings/Security&Privacy/More Privacy Settings/Get New Advertising ID and
  - Android (switch off): Settings/Google/Click on Profile icon/Manage Google Account/Data & Privacy/Personalised Ads/My Ad Centre/Click drop-down menu and select Turn Off and confirm.
    - Also switch off or Pause Web&App activity/YouTube History/Timeline

- Limit **Camera, Contacts, Phone & Microphone** access:
  - iPhone - switch live camera off: Settings/Camera/Preserve Settings/Live Phone = On, then click on the camera app icon on iPhone screen and click the top right concentric circle to off (shows diagonal line across circle). The Live Phone On setting will ensure Live Camera is off each time you use the camera.
  - Android: Settings/Apps (see All Apps)/Camera/Permissions then click on an allowed permission and select 'don't allow' if you want to withdraw that permission. Substitute 'Camera' for Phone and Contacts. Consider disallowing Location, Nearby Devices and Modify System Settings.

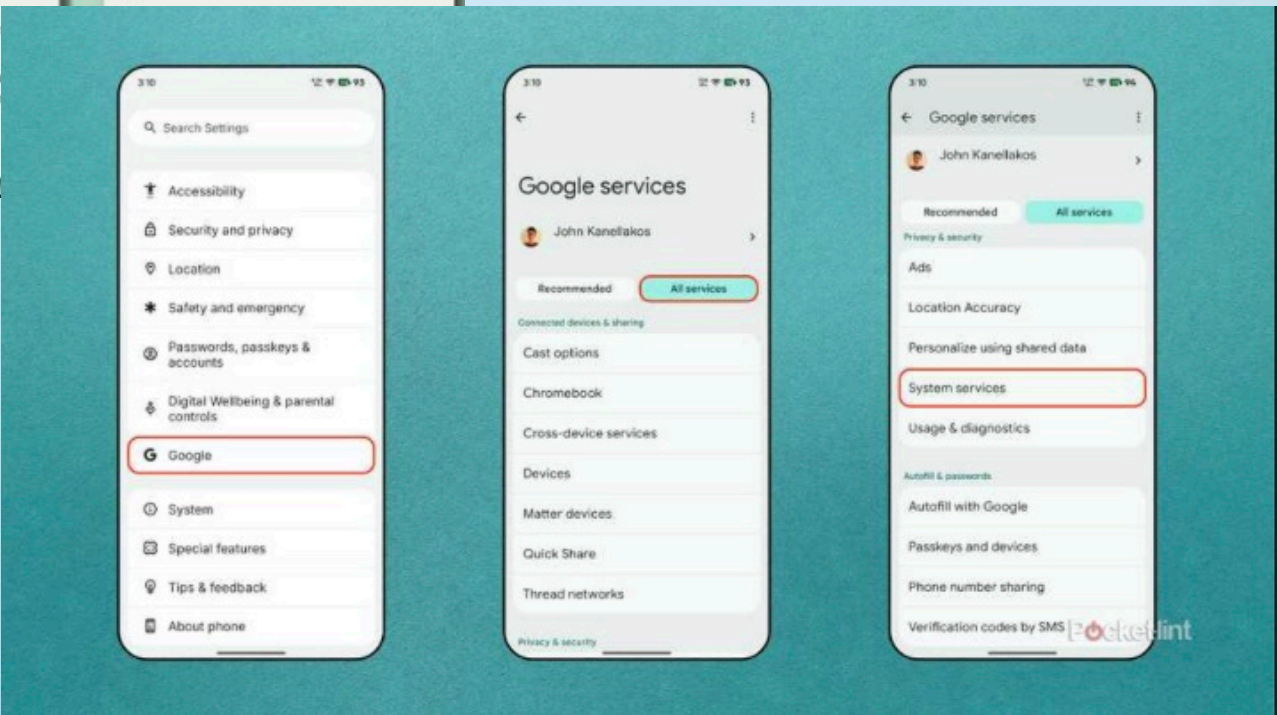
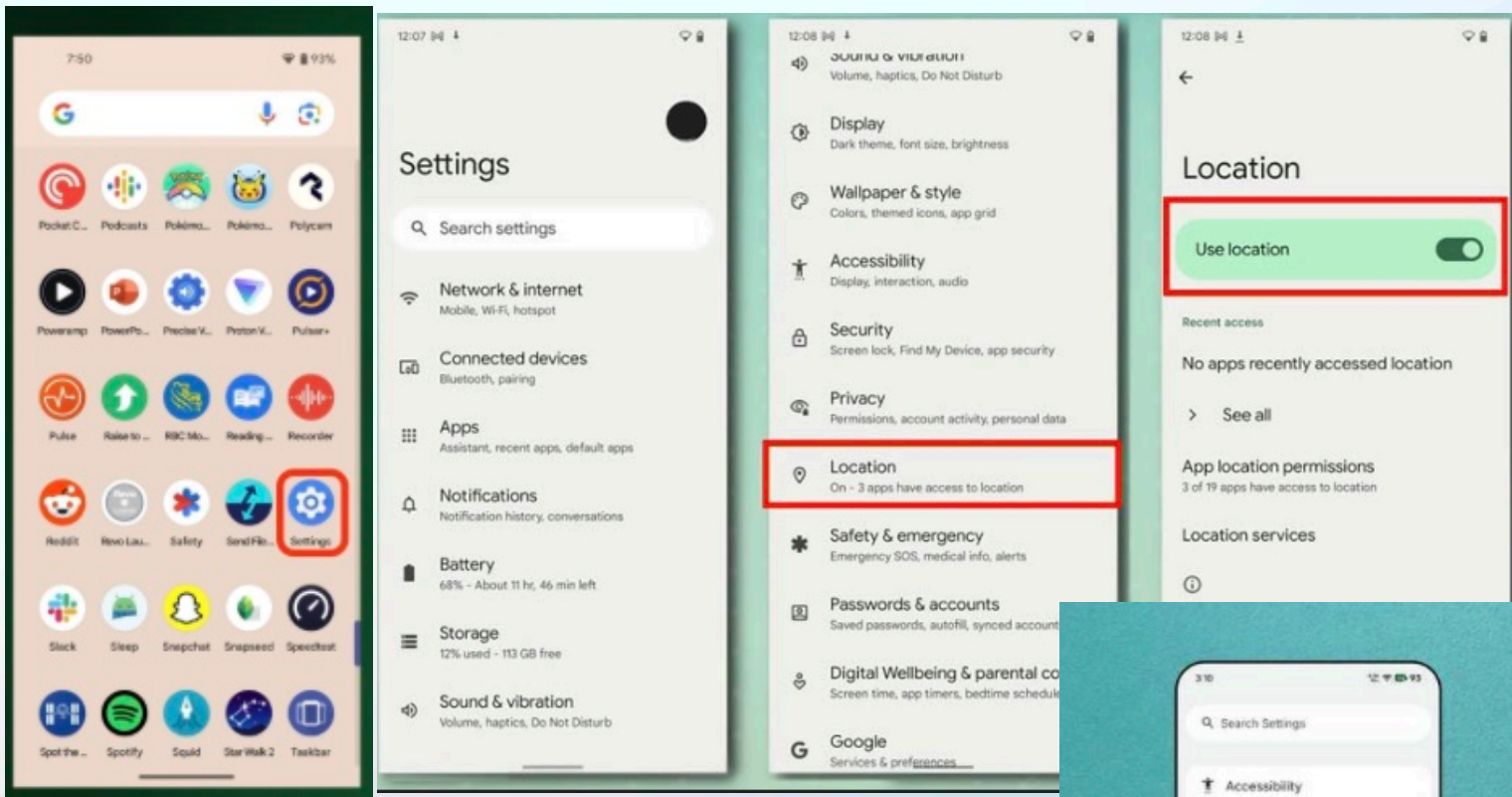
- Limit **App (applications) & App Tracking Permissions** settings:
  - iPhone: Settings/Apps/ - click on each app to view permissions
  - iPhone: Settings/Privacy & Security/Tracking/Toggle off 'Allow Apps to Request Track'
  - Android: Settings/Security & Privacy/Privacy/Permission Manager/ and consider
    - i) Camera; ii) Contacts; iii) Phone; iv) Microphone; v) Nearby Devices; vi) Location; vii) Photos & Videos and
  - Android: Settings/Apps/Special App Access and for each app installed disallow access for:
    - i) Unrestricted data; ii) **Install unknown apps**; iii) Usage access Iv) Wifi Control

- Limit **NFC & Connected Device Settings**
  - iPhone: NFC works automatically on most later models (year 2018 onwards)
  - Android: Settings/Connected Devices/Connection Preferences/NFC = Off. Also check the Quick Share and Cross-device services permissions
  - Android: Settings/Google/All Services/Devices/scan for near by devices
  - Android: Settings/Google/All Services/Quick Share/Who can share with you (switch off Use Mobile data)

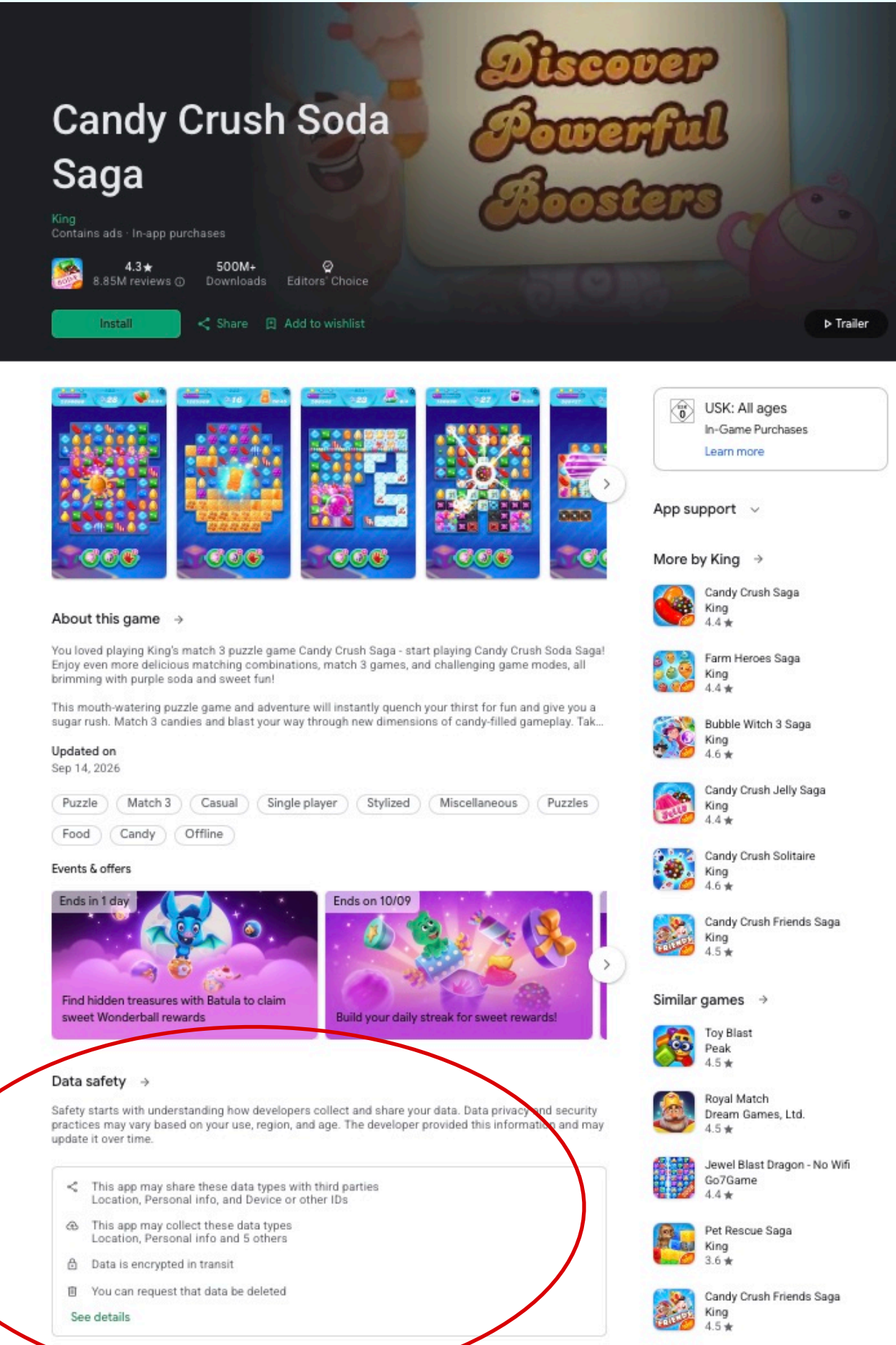
## Apple iPhone Device Settings Screen Example



## Android Device Settings Screen Example



# Google Play Store App Permissions: Example



| Permission                | What It Does                                                                  | Legitimate Use Example                                                                           | Red Flag Example                                                                                        |
|---------------------------|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Location                  | Accesses your device's precise (GPS) or approximate (network-based) location. | A weather app showing you the local forecast. A ride-sharing app finding your pickup spot.       | A simple calculator or puzzle game asking for your precise location 24/7.                               |
| Camera                    | Allows the app to take photos and record videos.                              | A video conferencing app like Zoom. An app for scanning QR codes.                                | A music player app that has no photo or video features.                                                 |
| Microphone                | Allows the app to record audio.                                               | A voice assistant like Google Assistant. A language-learning app that checks your pronunciation. | An offline-only game with no voice chat functionality.                                                  |
| Storage / Files and Media | Accesses all files on your phone, including photos, videos, and documents.    | A photo editing app loading a picture from your gallery. A file manager app.                     | An app that should only need to save its own small data files asking for full access to all your media. |
| Contacts                  | Reads, and can sometimes modify, your contact list.                           | A messaging app like Signal or Telegram so you can easily find and message your friends.         | A simple utility app, like a unit converter, that has no social component.                              |
| Phone / Call Logs         | Allows the app to make and manage phone calls and access your call history.   | The Phone app itself, or apps that can block spam calls.                                         | Any app that doesn't have a clear and obvious calling feature.                                          |
| SMS                       | Allows the app to read, receive, and send SMS messages.                       | A third-party messaging app. Apps that use two-factor authentication codes from your messages.   | A game or photo filter app. This is a very sensitive permission.                                        |

### Secrets to Becoming a Permissions Pro

Over the years, I've developed a few core principles that guide my decisions. These go beyond the basics and will help you think critically about your digital safety.

- The Context is King Rule:** This is the most important one. Always ask “why?” Why does this Sudoku app need microphone access? Why does this music player need my location? If you can't come up with a very good, obvious reason, the answer should be “Don't allow.”
- My Mistake, Your Lesson:** Years ago, I downloaded a “free” photo editor without checking the developer. I granted it storage access, thinking it was just for saving photos. A week later, my photo gallery was littered with ad images and my phone was sluggish. *The lesson: a permission is only as trustworthy as the app's developer.* Stick to well-known developers with good reviews.
- The Permission Audit Habit:** You don't need to do this every day, but once a quarter, take 10 minutes to go through your most-used apps. Open Settings > Privacy > Permission manager. This gives you a fantastic overview, showing you every app that has access to your camera, location, etc. It's a quick way to spot anything that looks out of place.
- Understand “Special App Access”:** In your phone's app settings, you might see a category called “Special app access.” This is for very powerful permissions, like “Display over other apps” (can draw windows on top of what you're doing) or “Install unknown apps.” Be extremely critical of any app that asks for these.

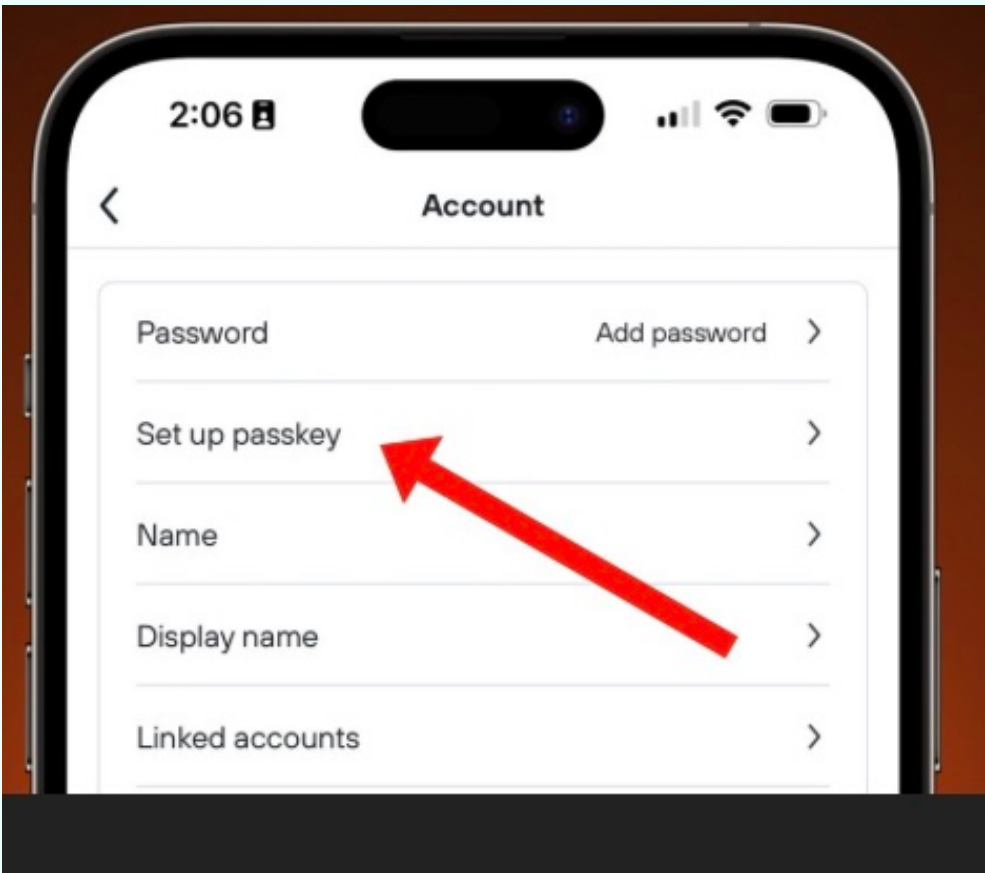
Source: <https://eathealthy365.com/understanding-google-play-app-permissions-explained/>

# Do you use Passkeys? What is Your Experience?

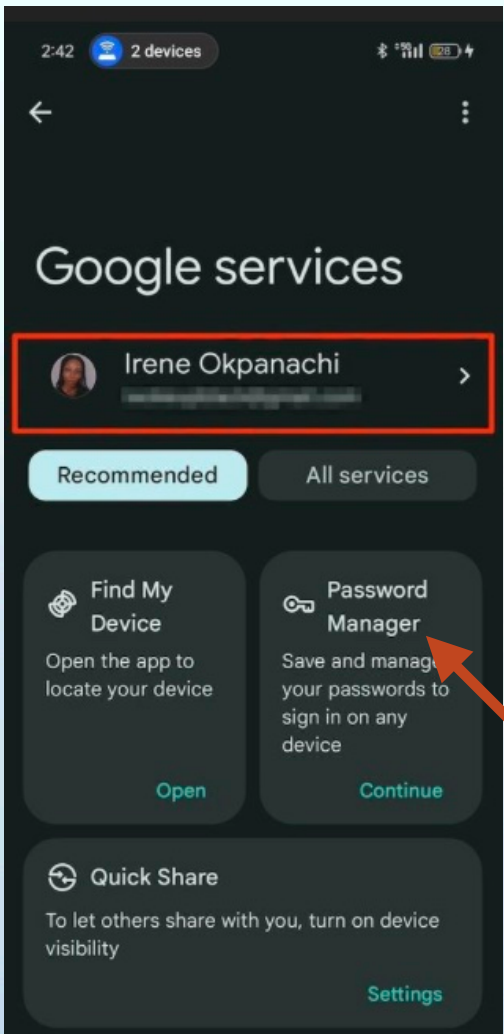
## PasskeySettings:

- iPhone: Settings/General/Autofill & Passwords/Toggle On Autofill Passwords and Passkeys
- Android: Settings/Google/Password Manager/Settings Option

Apple iPhone Screen Example



Android Screen Example



## Device Safety

### Passwords vs Pass Keys



Each passkey pairs a public key on the service with a private key on your device (aka cryptographic keys - encryption and decryption service ), blocking phishing attempts and syncing securely through iCloud Keychain or Android Google Password Manager.

There is no copy of the private key saved on the website, and it's not sent anywhere either. At no point does the service holding the public key ever see the private key.

## Safety of Passkeys Compared to Traditional Passwords

Passkeys are generally considered safer than traditional passwords for several reasons:

### Key Advantages of Passkeys

- **Elimination of Phishing Risks:** Passkeys reduce the risk of phishing attacks since they do not rely on users entering a password that can be stolen.
- **No Credential Reuse:** Unlike passwords, which users often reuse across multiple sites, passkeys are unique to each account, making it difficult for attackers to exploit them.
- **Cryptographic Security:** Passkeys utilize cryptographic keys stored on your device. These keys cannot be intercepted or reused, providing a higher level of security.

### Comparison Table: Passkeys vs. Traditional Passwords

| Feature                | Passkeys                         | Traditional Passwords    |
|------------------------|----------------------------------|--------------------------|
| Phishing Vulnerability | Low                              | High                     |
| Credential Reuse       | Not applicable                   | Common issue             |
| Storage Method         | Device-stored cryptographic keys | User-memorized or stored |
| Interception Risk      | Very low                         | Moderate to high         |

In summary, passkeys offer enhanced security by addressing common vulnerabilities associated with traditional passwords, making them a safer choice for account protection.

# Device Safety Tips

## General Suggestions

- Switch off: Re-start & shut down phone regularly.
- **Take control:** Switch off Phone Wi-fi & Mobile Data. Only switch on when you want to check messages etc.
- Avoid connecting to public wi-fi.
- Check permissions before installing an app. Are you happy to grant them?
- Check phone after major update to ensure some settings have not been set back to default.
- Only download from trusted sources such as Google & Apple Store.
- Beware of NFC - Near Field Communications/RFID - Radio Frequency Identification Skimming Attacks: Be mindful of people lingering around close to you. Switch NFC off when not in use and use RFID protection wallets for credit cards and car keys.



# Useful Links

- YouTube: 'iOS 26 Scary Privacy Settings to Turn Off Now'
- <https://www.howtogeek.com/android-permissions-explained-which-ones-you-shouldnt-ignore/>
- <https://eathealthy365.com/understanding-google-play-app-permissions-explained/>
- <https://devicology.com/guide/tips-to-prevent-nfc-scams/5620/>
- <https://www.kaspersky.com/blog/nfc-gate-relay-attacks-2026/55116/>



# Online Safety

- Network Settings
- Browser Settings
- WhatsApp Settings
- Phishing



# Online Safety

## Network Settings: Auto-Join

### Auto Join Feature

- The auto join feature works by:
- Storing a list of Service Set Identifiers -SSIDs (aka network name, e.g. 'Hilton\_Inn\_Free' in the devices Preferred Network List (PNL)
- When WIFI is switched on it seeks out the SSIDs in the list that are within range and connects automatically.

### Performance & Security Risks of Auto Join

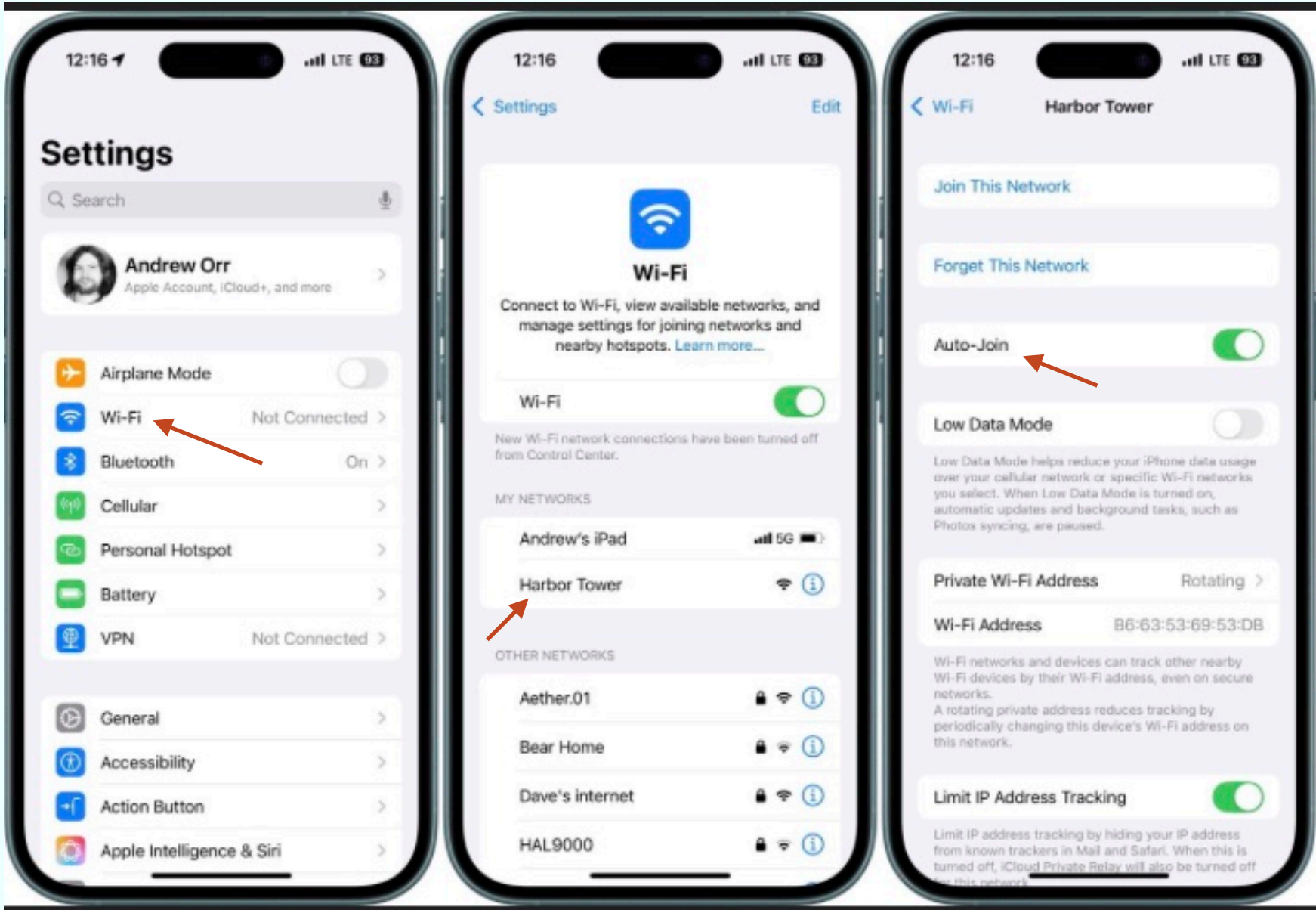
- Auto join can drain the battery as it is constantly scanning for network matches, particularly in built up areas with possibly hundreds of routers available.
- **'Evil Twin' Attack:** A hacker sets up a similar Wireless Access Point (WAP) with the same or similar SSID to a legitimate public network such as 'Hilton\_Inn\_Free'.
- If auto join is active it may connect to the hackers equipment instead of the legitimate source providing access to your:
  - Browsing history details
  - Cookie information that may contain stored passwords and account information
  - Personal communications
  - Login credentials

### The Verdict on Auto Join Settings

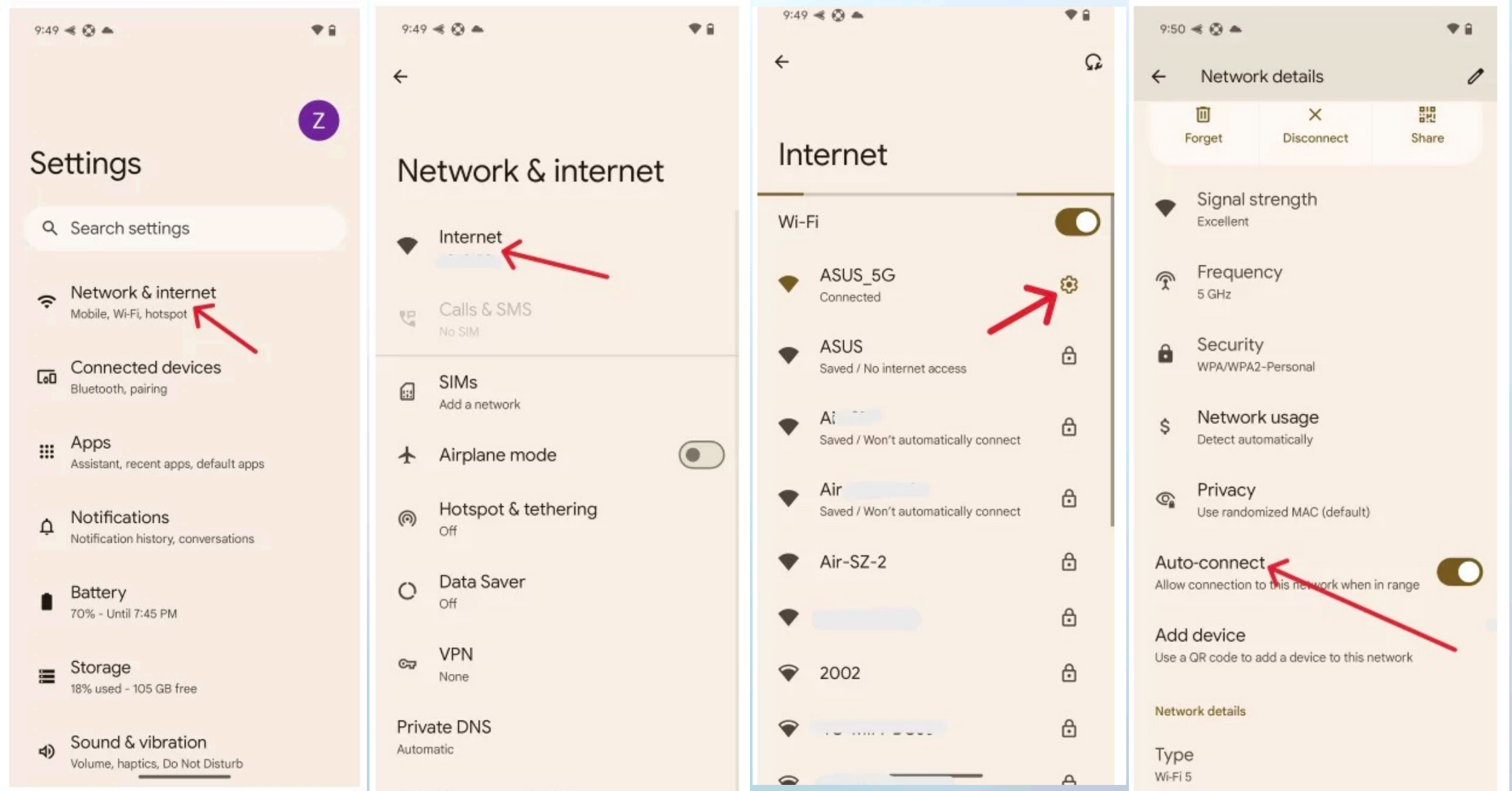
The determination of whether WiFi should be on auto join depends on the specific network environment. For the majority of users, the optimal configuration is a hybrid model.

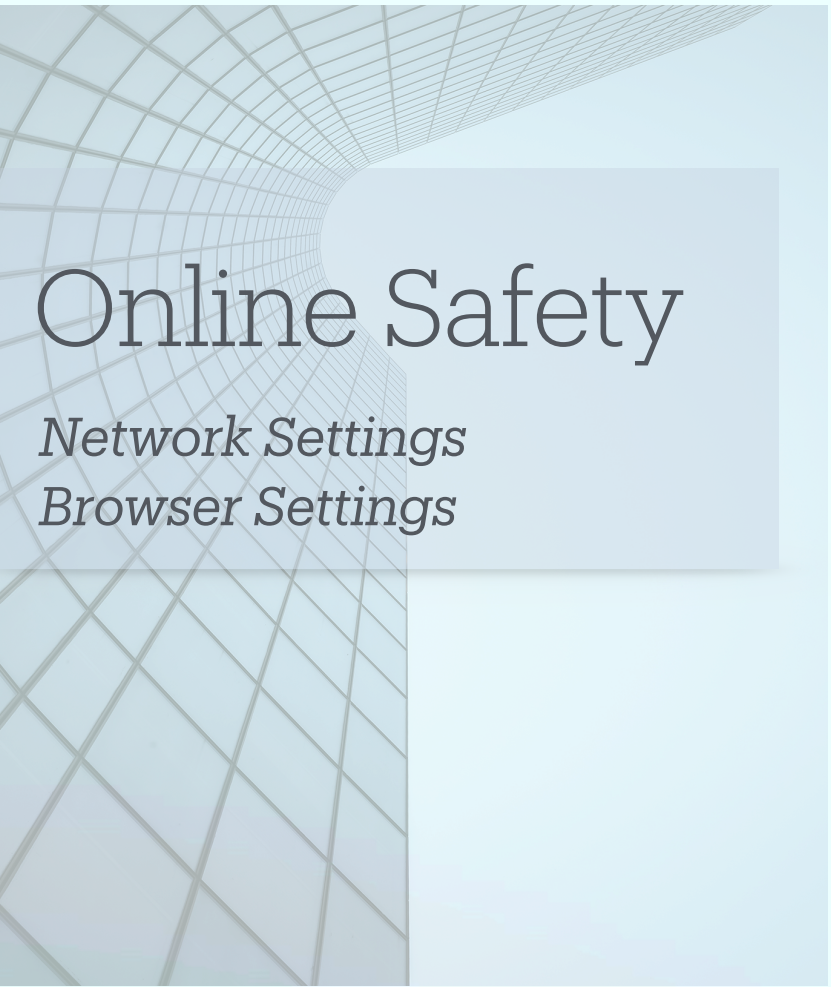
- Enable Auto Join for Trusted Networks: Keep the setting active for home, office, and verified private residences.
- Disable Auto Join for All Public Entities: Treat any network in a coffee shop, airport, or hotel as a manual-entry connection only.
- Regularly Purge the PNL: Periodically enter the device settings and "Forget" networks that are no longer in use. This reduces the number of probe requests the device broadcasts, shrinking the attack surface.
- Use a VPN for Necessary Public Connections: If a public network must be used, a Virtual Private Network (VPN) creates an encrypted tunnel, rendering intercepted data useless to an attacker.

### Apple iPhone Example



### Android Example

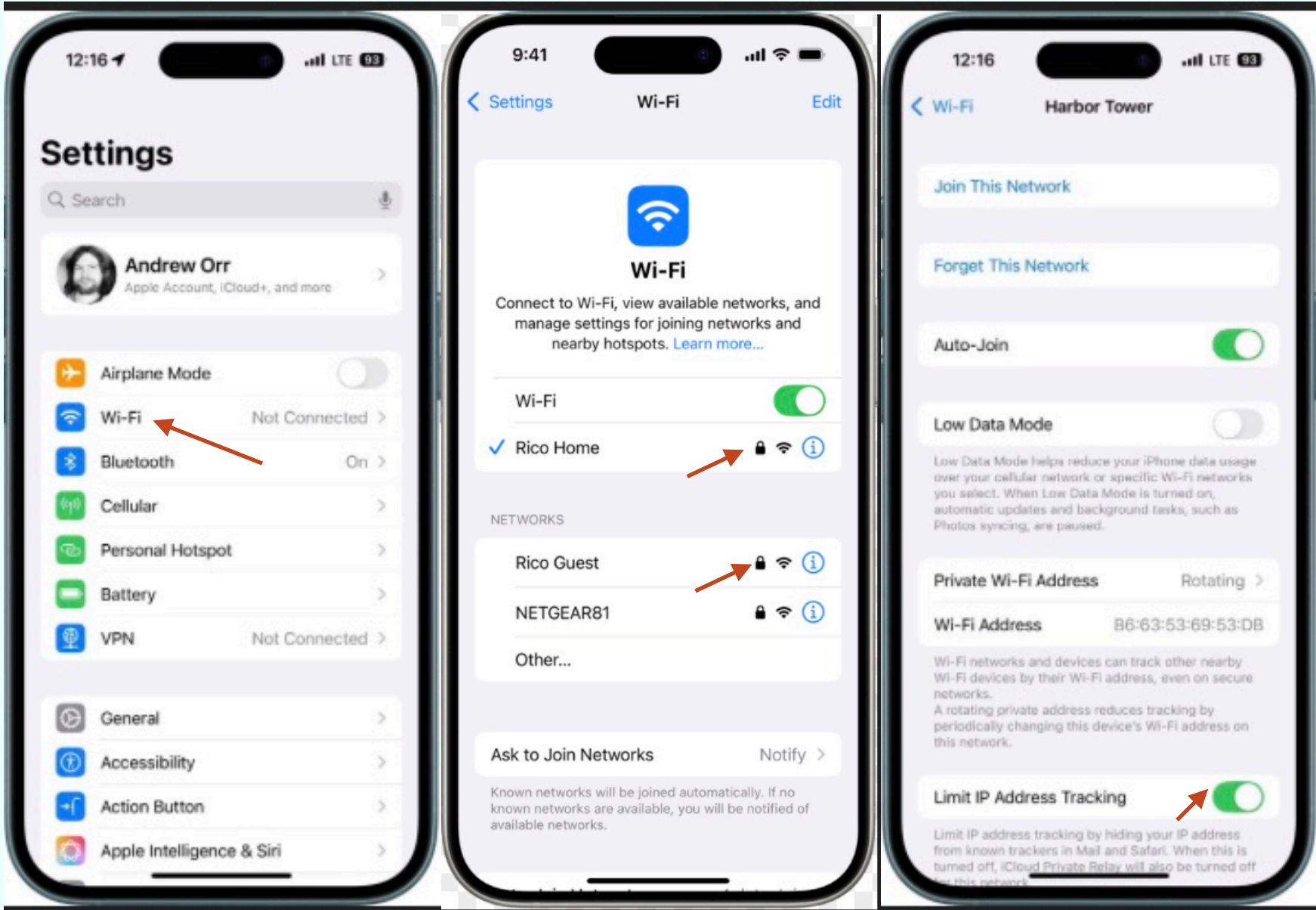




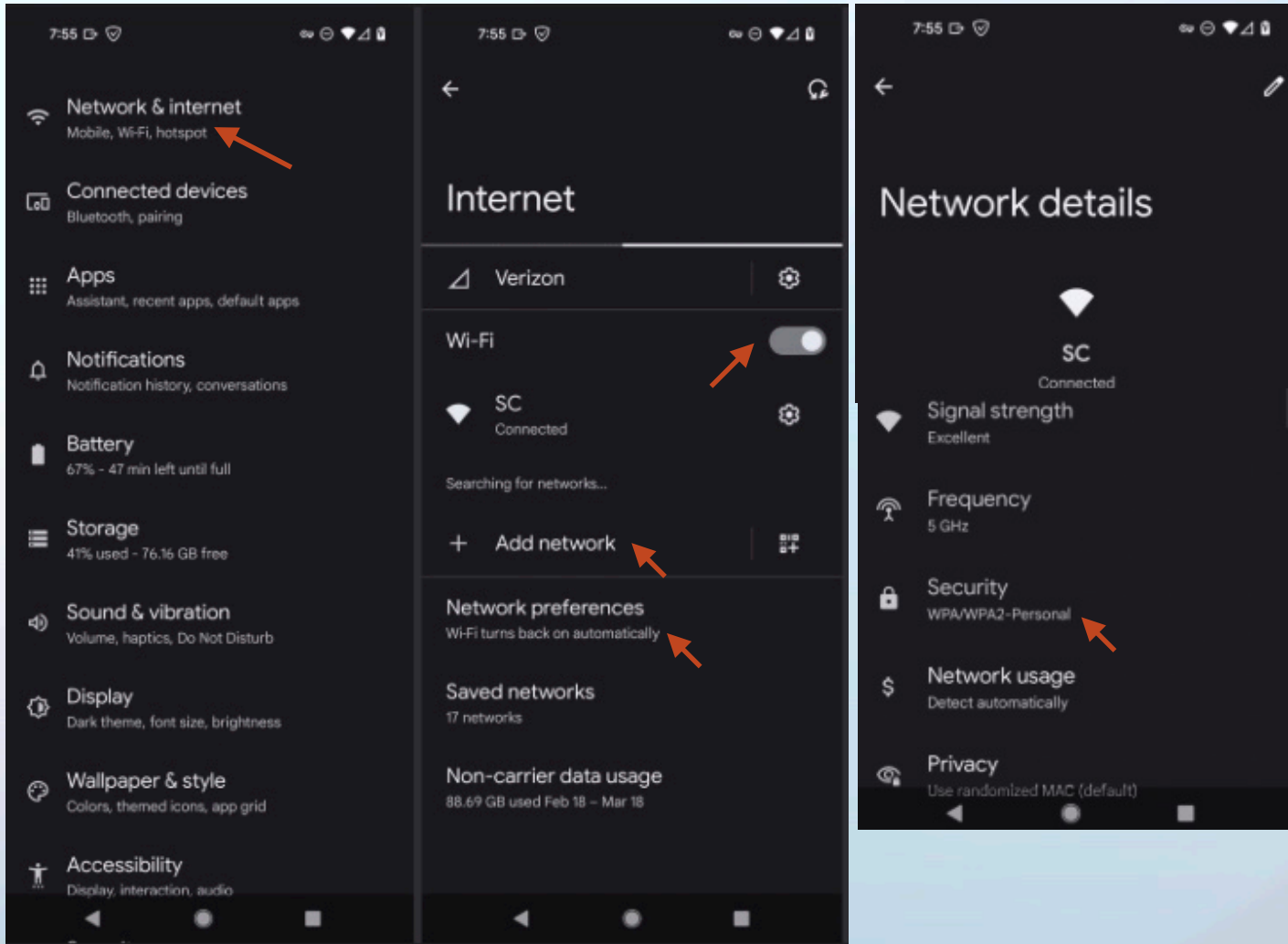
### Recommendations

- When connecting your phone to your home **wi-fi network setting** ensure the connection is **password protected** and has the **right security level assigned** to it:
  - iPhone: Settings/Wi-Fi/Click on desired network name and follow prompts to connect
  - Android: Settings/Network & Internet/Internet/Toggle on Wi-Fi/Add Network
- Switch off Bluetooth** when not in use:
  - iPhone: Settings/Bluetooth/toggle off
  - Android: Settings/Connected Devices/Connection Preferences/Bluetooth/Toggle off
- Network Protection**
  - iPhone: If using iCloud - Settings/Profile Name/iCloud/Private Relay
  - Android: Settings/Security & Privacy/More Security Settings/Network Protection/Toggle on warnings
- Browser Settings**
  - iPhone: Settings/Apps/Safari/Check long list of settings such as block pop-ups, **prevent cross-site tracking, fraudulent website warning**, not secure connection warning, clear history and website data. Scroll down and select Advanced - ensure Remote Automation is switched off.
  - Android: Open browser app (e.g. FireFox, Chrome)/Click 3 dots top right/Select settings (adjust settings such as cookie pop-up protection, **app tracking, web tracking, https-only mode**, delete browsing data on quit, **clear cache regularly**. Switch off auto-fills and try to remember your password or use passkeys.

### Apple iPhone Example



### Android Example



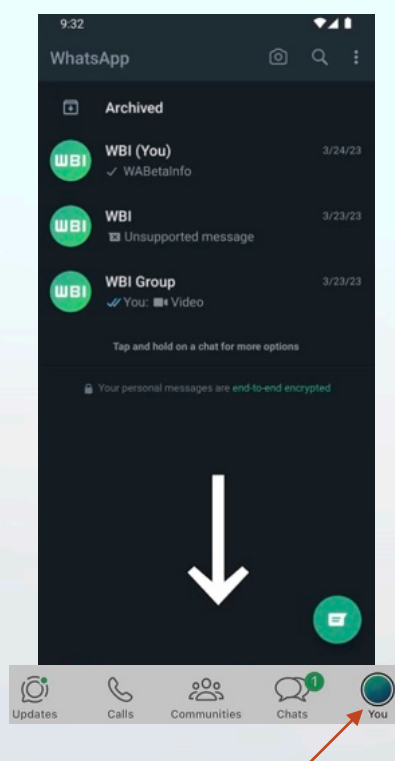
## Recommendations

Consider adjusting the following **WhatsApp settings**:

- Android & iPhone: Click on WhatsApp icon to launch app then select 'You' bottom right/ Privacy. Check settings such as Disappearing Messages, Live Location, Advanced features such as blocking unknown account messages, disable link previews, protect IP address in calls.

**Clean up WhatsApp Storage.** WhatsApp can take up a lot of space with old pictures and audio files.

- Android & iPhone: Click on WhatsApp icon to launch/Select 'You' bottom right/ Select Storage and Data/Select Manage Storage.
- To Bulk delete WhatsApp files larger than 5 MB, click on 'Larger than 5MB' and tap to check the 'select all' box in the top right hand corner then click on the dustbin icon in the top right hand corner. To delete specific pictures, tap on the desired picture until a tick appears then click on the dustbin icon to delete.
- To Bulk delete WhatsApp files from specific people/chats, click on the relevant name listed under 'Chats' and tap to check the 'select all' box in the top right hand corner then click on the dustbin icon in the top right hand corner. To delete specific pictures, tap on the desired picture until a tick appears then click on the dustbin icon to delete.



Latest version has a 'You' option

## Switch Off Media Visibility

If you want to keep your WhatsApp safe, then turn this feature off immediately by following the steps given below.

1. Open WhatsApp.
2. Click the three dots (:) at the top right of the screen.
3. Select the Settings option.
4. Go to the Chats section.
5. Turn off the Media Visibility toggle.

### What will happen if I turn off this feature?

- No files, photos or videos received on WhatsApp will be downloaded without your permission.
- Your phone will be safe from malicious data/files and viruses.
- Your data will be protected from unwanted access, keeping your personal chats and media safe.

This feature of WhatsApp looks good but can be dangerous from the cyber security point of view. So, if you have kept the media visibility feature on till now, then turn it off immediately.

## Conclusion

If you receive any link or file on your WhatsApp, you should always avoid clicking on it, until you are confirmed about the link. You should first check the number from which the file has come. Because many times, WhatsApp may also contain links that trap you, which can land you in trouble.

- **Other WhatsApp versions:** Click on WhatsApp icon to launch app then select 'You' bottom right/select chats from menu/Toggle off media visibility.



## What is Phishing?

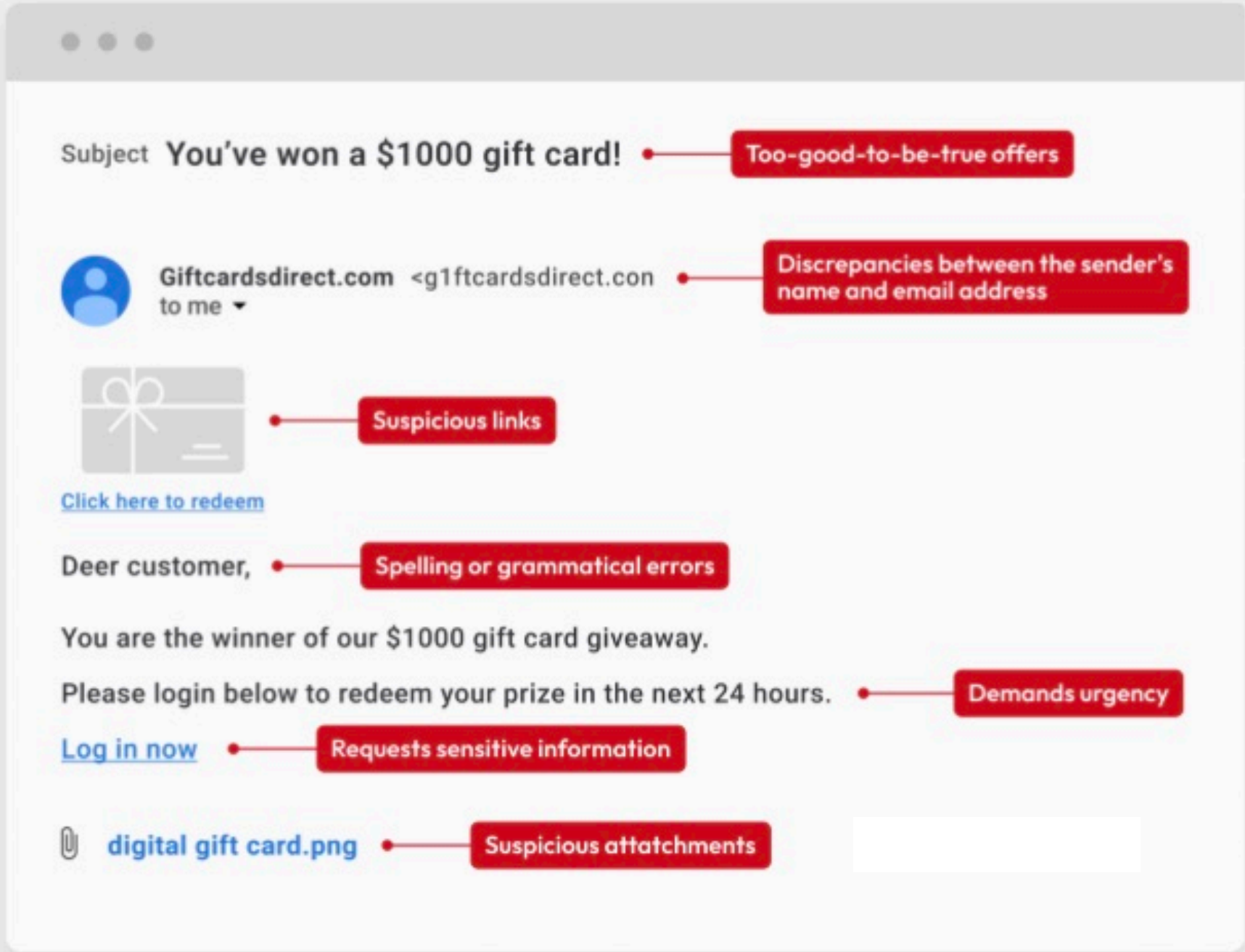
' Phishing is a type of cybercrime where scammers pretend to be a trusted source to trick you into sharing sensitive information or clicking harmful links. These messages often look real and urgent, and they can happen through email, text messages, phone calls, or social media. '

Source: malwarebytes.com & McAfee

## Types of Phishing

| Type of Phishing         | Description                                                                                                                                       |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Email Phishing           | Attackers send <b>fraudulent emails</b> pretending to be from legitimate sources to steal sensitive information.                                  |
| Whaling                  | Targeted phishing aimed at <b>high-profile individuals</b> like CEOs or CFOs to steal company-sensitive data.                                     |
| Vishing (Voice Phishing) | Attackers use <b>phone calls</b> to impersonate trusted entities, asking for sensitive information like account details.                          |
| Smishing                 | Phishing through <b>SMS</b> , often with links that lead to malicious websites or malware downloads.                                              |
| Angler Phishing          | Phishing via <b>social media</b> , where attackers impersonate customer service accounts to deceive users into visiting malicious websites.       |
| HTTPS Phishing           | <b>Fake websites with HTTPS encryption</b> that mislead users into thinking they are secure, collecting sensitive information like login details. |
| Spear Phishing           | Highly targeted phishing using <b>personalized information</b> about the victim to make the attack appear legitimate.                             |
| Pharming                 | An attack that redirects a victim's traffic to a fake website by <b>altering the DNS or browser settings</b> .                                    |
| Pop-up Phishing          | <b>Malicious pop-ups</b> appear on legitimate websites, tricking users into clicking links or entering sensitive information.                     |
| Clone Phishing           | Attackers <b>replicate a previously sent legitimate email</b> , replacing links or attachments with malicious content.                            |
| Evil Twin                | A <b>fake Wi-Fi hotspot</b> set up to steal sensitive data from users who connect to it.                                                          |

## How To Identify a Phishing Email



# Online Safety

## Phishing Exercise



Banking ALERT: Your account has been locked

**B** fraudunit@bankofamirica.com  
To Thomas Stall, DDS



### **BANKING ALERT.**

Hello Online Banking Customer,

Several login attempts have been made on you're account. As a result, we have temporarily locked your account. For added security the fraud unit has added an extra verification process.

To begin the verification process, please [click here](#). If you fail to update your account information within the next 48 hours, your account will have to be manually unlocked by visiting a local branch.

Were here to help if you need it. Visit the [Fraud Unit Help Center](#) for more info or [connect us](#).

Sincerely,

Bank of Amirica Fraud Detection  
fraudunit@bankofamericas.com  
888-555-1234



*Phishing Email Example*

1. *Email Address: Spelling mistakes*
2. *To: Vague Names*
3. *Not addressed to a specific name*
4. *Spelling mistake in text e.g. 'you're' should be 'your'*
5. *Suspicious links - NEVER click on suspicious links. Try to hover over the link to check the URL address*
6. *Time pressure/Urgency*
7. *Grammar e.g. 'connect us'*
8. *Bank name spelt incorrectly*
9. *Don't use telephone numbers given. Call your bank customer services and speak to them directly*
10. *Email address at Bottom does not match with email address at top.*

# Quishing

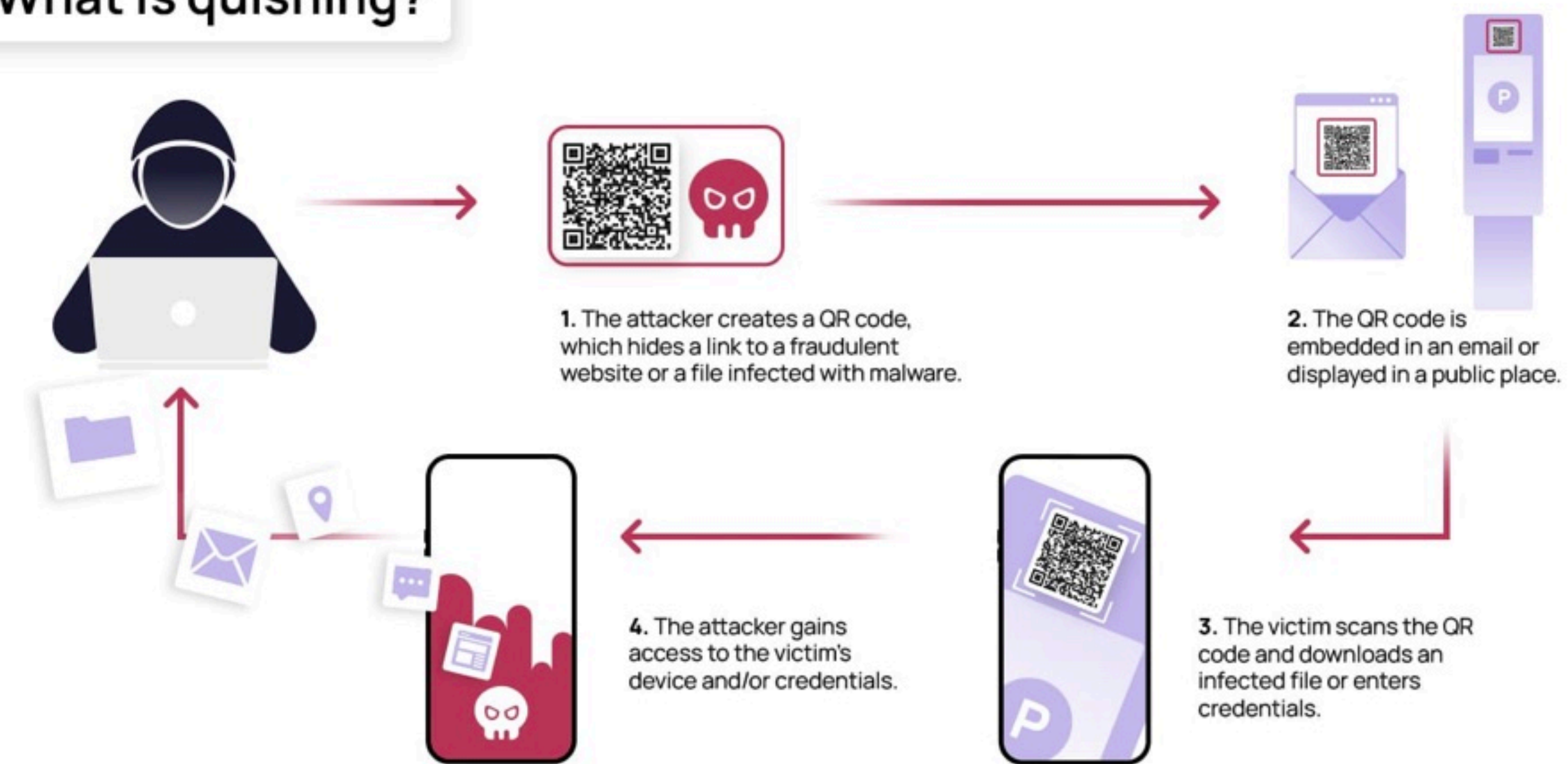
Quishing (QR code phishing) hides harmful links inside QR codes. Scanning such a QR code can send you to a fake site designed to collect logins, payment details, or other personal details.

In July 2025, [the FBI warned](#) the public about unsolicited packages with QR codes attached. This new iteration of [brushing scams](#) involved unexpected deliveries accompanied by QR codes that led to malicious websites. [QR code scams](#) could also appear on fake parking notices, menus, or bus stops, tricking people into scanning codes that lead to fraudulent sites.

## Common quishing tactics:

- QR codes placed on parking meters, pay stations, or fake violation notices.
- Unsolicited packages containing QR codes that promise more information.
- Emails or text messages using QR codes instead of clickable links to bypass filters
- QR codes on fake menus, Wi-Fi access signs, or event materials.
- QR codes leading to fake login pages or payment portals.

## What is quishing?



# Useful Links

- <https://www.grafdom.com/blog/5-whatsapp-settings-you-should-change/>
- <https://techflare.net/should-my-wifi-be-on-auto-join-the-ultimate-security-guide/>
- <https://www.doppel.com/blog/8-phishing-email-examples-every-business-should-know>
- <https://us.norton.com/blog/online-scams/types-of-phishing>
- <https://lifelock.norton.com/learn/fraud/types-of-phishing>



*Thank-you!*