

Protect yourself against Identity fraud, phishing and in the worst case, account hacks!



Identity fraud through known or public Wi-Fi networks **occurs when attackers exploit user trust in familiar network names or unsecured public connections to steal personal information**. Common methods include "Evil Twin" attacks, where criminals create a fake hotspot with the same name as a trusted one (e.g., "CoffeeShop_Free" vs. "CoffeeShop_Guest"), and "**man-in-the-middle**" attacks, where they intercept data between a device and the router

Common Identity Fraud Tactics via Wi-Fi

- **Evil Twin Access Points:** Fraudsters set up a malicious Wi-Fi hotspot with a similar or identical name to a legitimate, trusted network (e.g., in a hotel, cafe, or airport).
- **Packet Sniffing:** Attackers use specialized software to monitor unsecured network traffic, capturing personal data like passwords, bank details, and social media credentials in real time.
- **Fake Captive Portals:** Upon connecting to a "free" network, users are redirected to a fake login page that requests personal information (birthdays, email addresses, passwords), which are then stolen.
- **Malware Injection:** Attackers may inject malicious ads or prompt users to download fake updates, which install spyware to record keystrokes or steal stored credentials.
- **Automatic Reconnection Exploits:** Smartphones often automatically connect to "known" networks. Hackers exploit this by naming their fraudulent network after a common, generic name like "FreeWiFi" or "Airport_Guest," causing nearby phones to connect automatically without the user realizing

Warning Signs of a Compromised Network

- **No Password Required:** Open networks in public places are often unencrypted, making them easy targets for attackers.
- **Disconnections:** Constant or unexpected disconnections from a network can indicate that a hacker is performing a "de-authentication attack," forcing you off the real network to connect to their fake one.
- **Duplicate/Misspelled Network Names:** Be suspicious of networks with similar names to the venue, such as "Starbuckz" instead of "Starbucks_Free".
- **Suspicious Redirects:** If your browser suddenly redirects to a generic login page or a site you did not intend to visit, your session may be intercepted.

How to Protect Yourself

- **Use a VPN:** A Virtual Private Network (VPN) encrypts all data, making it unreadable to hackers even on a compromised network.
- **Disable Auto-Connect:** Turn off the feature on your phone or laptop that automatically joins known Wi-Fi networks.
- **Delete unused "known" networks:** Regularly check your laptop and phone for unused known networks and remove them to avoid unwanted WiFi connections. See the instructions.
- **Verify the Name:** Confirm the exact network name with staff at the cafe, hotel, or airport.
- **Avoid Sensitive Transactions:** Never access online banking, enter credit card details, or log into sensitive accounts while on public, non-password-protected Wi-Fi.
- **Check for HTTPS:** Look for the padlock symbol in your browser's address bar, indicating that the website **itself** is encrypting your traffic (and not a firewall or proxy server)
- **Use Cellular Data:** When possible, use your mobile carrier's data network instead of public Wi-Fi.
- **Forget Networks:** After leaving a location, select "Forget" for that network in your device settings



Clear unused “known” WiFi networks on all your devices

(company and non company devices)



Delete Previously Used Networks on a iPhone (Not Nearby)

1. Go to **Settings** > **Wi-Fi**.
2. Tap the **Edit** button in the top right corner of the screen.
3. You may be asked to authenticate with Face ID or Touch ID.
4. Tap the **delete button** (red minus sign) next to the network you want to remove, then tap **Delete**.
5. Alternatively, tap the "i" info button next to a network and select "Forget This Network" or change the setting to off for “Auto join”.



Delete Previously Used Networks on a Android (Stock/Pixel/General):

1. Go to Settings
2. Network & internet
3. Internet
4. Saved networks, then tap the network and choose **Forget**.

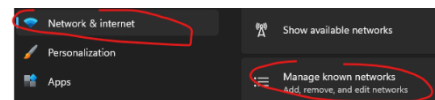


Delete Previously Used Networks on a Samsung Galaxy:

1. Go to Settings (gear button)
2. Connections
3. Wi-Fi and tap top right corner on Three-dot menu
4. Advanced settings
5. **Manage networks**. Tap on the network to remove, then choose **Delete** or **Forget**.

Delete Previously Used Networks on Windows laptop: (Via Windows Settings (10/11))

1. Open the **Start Menu** and click the **Settings** gear icon.
2. Select **Network & Internet**.
3. Click on **Wi-Fi** in the left menu or main panel (Windows 11).
4. Click **Manage known networks**.
5. Find the network you want to delete.
6. Click the network name and click the **Forget** button



You can find all other letters about information security on our intranet.

Link (Always check if the link is correct by hovering over it with the mouse):

[Information Security – Intranet TKH Airport Solutions](https://intranet.tkh-airportsolutions.com/?cat=6)



Still questions: Mail to it@tkh-airportsolution, raise an IT-ticket or call us.