Hotspots and Passkeys

A few notes about keeping secure on the internet and elsewhere

The Password Problem

- Key points:
-
- The most common passwords are still: 123456, password, and qwerty.
-
- A simple 8-character password can be cracked in seconds.
-
- Humans are not good at creating or remembering strong passwords.
-
- Password reuse is a massive security risk.

The Password Golden Rules

- Key points:
-
- Length over complexity: Aim for 16 characters or more.
-
- Make it a "passphrase": A string of random words is easier to remember.
-
- Use a unique password for every account.
-
- Never write them down on a sticky note.

The Solution: Password Managers

- Generates long, random, and unique passwords.
- Stores all your passwords in a secure, encrypted vault.
- Remembers and auto-fills your login information.
- You only need to remember one master password.
- Popular options include 1Password, LastPass.

Google - Chrome Browser Storage

- Basic Chrome Browser Save:
- A convenience feature.
- Passwords are saved to a local file on your computer.
- Vulnerable to malware and local attacks.
- Not a robust security solution.

Google - Password Manager:

- A secure, encrypted vault offered by Google.
- Accessible at passwords.google.com and via the browser!.
- Encrypted with your Google account credentials.
- Syncs securely across all your devices (Chrome, Android, etc.).
- The choice: Do not rely on local browser save; use the secure, encrypted manager.

What is 2-Factor Authentication?

- A second layer of security.
-
- Requires two distinct "factors" to log in.
-
- Factor 1: Something you know (your password).
-
- Factor 2: Something you have (e.g. a unique code sent via text).
-
- Even if a password or device is stolen, the account is still safe.

Types of 2-Factor Authentication

- SMS Text Message:
- Pros: Easy to use, no extra app needed.
- Cons: Less secure. Vulnerable to SIM swap attacks.
-
- Authenticator App (e.g., Google Authenticator):
- Pros: More secure, works offline, not tied to a phone number.
- Cons: Requires a separate app to be installed.
-
- Security Key (e.g., YubiKey):
- Pros: The most secure option. A physical device - impossible to hack.
- Cons: A physical device that can be lost or misplaced.

How to Set Up 2FA

- Go to account security settings for the service (Google, Amazon, Norton)
-
- Look for "2-Factor Authentication," "2-Step Verification," or "Multi-Factor Authentication (MFA)."
-
- Choose a method (Authenticator app is recommended).
-
- Scan a QR code to link your phone.
-
- Save your backup codes somewhere safe.

PINs in Modern Credit & Debit Card Security

- The EMV Chip: Your card has a secure, specialized chip that acts like a Secure Enclave.
-
- A Local Key: Your PIN is not a password. It is a local key to unlock the chip on your card.
-
- Secure Authentication: The PIN is verified directly on the card and the terminal. It is never transmitted over the network.
-
- Unique Transaction Codes: If the PIN is correct, the chip generates a unique, one-time-use cryptographic code for that specific transaction.

PINS vs Passwords for Windows/Android/Apple devices

- A PIN is not used for authentication itself.
- It is a key to unlock the passkey in the Secure Enclave.
- The passkey is a unique, complex cryptographic key stored in hardware.
- Brute-force attacks are impossible.
- Modern devices have rate-limiting measures.
- After a few failed attempts, the device locks for a longer & longer time.
- After 10 failed attempts, the device can automatically erase itself.

PINs for Modern Operating Systems

- Microsoft Windows (“Window Hello”).
-
- Apple iPhone.
-
- Apple MacOS.
-
- Google (Android).

PINS - Why Third-Party Services Don't Use Them

- Most other major players do not use PINs for authentication. They rely on other methods for a few key reasons:
-
- PINs are device-bound.
-
- They rely upon the “Shared Secret” Model.
-
- Passkeys are now seen as the solution.

Biometrics on Your Devices

- Biometrics are unique physical or behavioral traits used for authentication.
-
- Fingerprint Scanning:
- Facial Recognition:
-
- Your raw biometric data (e.g., your actual fingerprint image) is never stored and never leaves your device.
-
- It's an unguessable, physical key that is protected by hardware.

Introducing Passkeys: The Future of Login

- What they are: A passwordless way to log in to websites and apps.
-
- How they work: Use your fingerprint, face, or device PIN to sign in.
-
- The Goal: To replace passwords and even traditional 2FA.
-
- The Experience: Fast, easy, and seamless.

How Passkeys Work: No Password, No Phishing

- Uses Public-Key Cryptography (the same as for encryption).
-
- Your device creates a unique public and private key pair for each account.
-
- Only the public key is stored on the server.
-
- The private key is securely stored on your device (and never leaves it).
-
- This eliminates phishing: a passkey only works on the correct website, so you can't be tricked by a similar URL or fake link.

Using a Passkey in Practice

- Windows Hello: On a Windows machine, you simply select a "Sign in with a passkey" or "Windows Hello" option. Your face, fingerprint, or PIN is used to authorize the login.
-
- Android: On a website or app that supports passkeys, you'll see a prompt to "Sign in with a passkey". You then use your phone's biometrics or screen lock to confirm.
-
- The User Experience: You simply authenticate with a quick physical action you're already familiar with.

The Key Benefits of Passkeys

- Ultimate Security: Phishing-resistant and immune to data breaches.
-
- Simplicity: No more typing passwords or 2FA codes.
-
- Cross-Device Syncing: Passkeys are synced securely across your devices (via iCloud Keychain, Google Password Manager, etc.).
-
- Convenience: The same unlock method for your device is your login method.

The Lost Device Problem: A Passkey Solution

- Passkeys should be synced across multiple devices.
-
- They are securely backed up to your cloud account (e.g., Apple iCloud Keychain or Google Password Manager).
-
- If you lose a device, you can recover your passkeys on a new one.
-
- You can use another trusted, existing device to approve a new one.
-
- In the worse case scenario, the recovery process requires an old-school login (password + 2FA) to verify your identity.

Passkey Security: A Stolen Device

- Passkeys are tied to your device's biometric/PIN lock.
- They are stored in a Secure Enclave or Trusted Platform Module (TPM).
- This is a separate, highly secure chip on your device.
- The passkey private key cannot be used without your fingerprint, face, or PIN.
- A thief cannot access your passkeys even if they have the physical device.
- You can also remotely wipe your device as a final security measure.

What's a Wi-Fi Hotspot?

- Key points:
-
- A location offering wireless access to the internet .
-
- Uses radio waves to broadcast a signal.
-
- Two types: Public and Private.

Public Wi-Fi Hotspots: Insecure by Default

- Convenient but insecure.
-
- Man-in-the-Middle (MITM) Attacks are a major risk.
-
- Evil Twin hotspots can trick you.
-
- A password to connect does not guarantee encryption.

How to Stay Secure on Public Wi-Fi

- Use a VPN for an encrypted tunnel.
- Look for HTTPS and the padlock icon 🔒.
- Disable file sharing and other services.
- Use your own data/hotspot for sensitive tasks.

Private Wi-Fi Hotspots: Your Own Secure Network

- Home Wi-Fi Router: Your primary private network.
-
- Mobile Hotspot: Your smartphone as a portable hotspot.
-
- Security depends on the protocol.
-
- WPA3 is the gold standard; WPA2 is good; WEP is obsolete.

Setting Up Your Private Hotspot

- Smartphone Hotspot:
-
- Settings > Personal Hotspot (iPhone) or Mobile Hotspot (Android).
-
- Turn it ON and set a strong password.
-
- Uses your mobile data contract - be aware of usage limits..
-
- Always use a unique, complex password.

Wi-Fi Hotspots in Your Car

- Many new cars have a built-in mobile modem and antenna.
- This creates a private Wi-Fi hotspot for passengers.
- Example: FordPass Connect uses a dedicated mobile connection.
- Provides a stronger, more reliable signal than a smartphone.
- Requires a separate data contract or subscription.

Key Takeaways: Public vs. Private Hotspots

- Key points:
-
- Public: Insecure; use for low-risk tasks (news, weather).
-
- Private: Secure; use for all sensitive tasks (banking, passwords).
-
- Final Rule: If in doubt, don't enter sensitive information. Protect your personal data.