Passwords, Passkeys & Safe Online Banking

An integrated security approach is the answer!

All security systems at your bank are continually updated to protect your personal information. Here are key facts, tips, and updates that can significantly reduce the chances of becoming a victim of identity theft or account fraud.

Authentication

Authentication is the process of verifying your identity to allow secure account access. It ensures that only you can access your bank accounts.

Online banking requires secure authentication protocols designed with customer privacy in mind. The answer is **multi-factor authentication** — an approach that combines two or more types of credentials for enhanced security.

New research continues to focus on safeguarding privacy and preventing fraud. One emerging solution is **Passkeys,** a next-generation authentication technology that does not require a password.

Password protection

A password is a confidential string of characters used to gain access to your accounts.

Experts recommend using **a unique password for every account** and changing each one **at least twice a year** for stronger protection.

Password Selection

Password strength is the foundation of your security. Strong passwords are:

- At least **10 characters long**
- Include **uppercase and lowercase letters, numbers, and symbols**
- Avoid personal information like names, birthdays, or addresses

Example: P59nD#s1z*
Never share your passwords with anyone.

Password Use

Remember that passwords protect everything from financial accounts to your home Wi-Fi or even smart devices.

Do ***not*** reuse the same password across multiple accounts.

Takeaway: Passwords safeguard your financial information—**protect them carefully.**

■ Passkey protection

Passkeys were designed with **privacy** and **convenience** in mind. Your personal information is never revealed or transmitted. Passkeys rely on **multi-factor authentication** to confirm your identity without sharing your actual credentials.

Your information is unlocked by a **private key** stored securely on your device.

Passkey Technology

Passkeys use a pair of mathematically related keys:

- A **public key,** which encrypts the login process.
- A **private key,** which verifies your identity on your device.

The private key never leaves your device, and no shared secret is transmitted during login.

Passkey Use

Passkey users log in using **biometric authentication** (such as fingerprints or facial recognition) or the **device PIN,** making access both faster and more secure.

Takeaway: Whether you use passwords or passkeys, these are the final steps to unlocking your personal information securely.

Password / Passkey Management

Consider using a **reputable password manager** to securely store and encrypt your passwords and passkeys across all your devices.

While some services charge a small fee, they offer convenience and strong protection.

Note: Your web browser is not the safest place to store password information.

Multi-Factor Authentication

Multi-Factor Authentication (MFA) requires at least two different types of proof to verify your identity. It's used by banks for secure online access.

1. **Something You Know** – Passwords, PINs, or security codes.
2. **Something You Have** – A physical item like a phone, smart card, or token device.
3. **Something You Are** – Biometrics such as fingerprints, facial recognition, or voice identification.

Using two or more of these factors provides **strong, layered security** against fraud.

Network security

Wi-Fi network options can sometimes be confusing. Always double-check that you've selected the correct, secure network before logging in.

Secured Network

A secure Wi-Fi network will show a **lock icon** or the word **"secured."**

When connecting at a hotel, café, or conference, always use the official network and ensure it's password protected.

Home Network

Your home Wi-Fi router is your gateway to the internet.

Use a **strong router password,** and rename your network so it doesn't reveal your location or identity.

Keep your router's **firmware updated** regularly to maintain security.

Virtual Private Network (VPN)

A **VPN** (Virtual Private Network) creates a private, encrypted link between your device and the internet, ensuring your data remains unreadable to others.

Choose a **trusted, top-rated VPN service** and install it on all devices that connect via Wi-Fi.

Resources

- Federal Trade Commission: **www.ftc.gov**
- Identity Theft Resource Center: **www.idtheftcenter.org**
- Financial Fraud Enforcement Task Force: **www.stopfraud.gov**
- National Cybersecurity Alliance: **www.staysafeonline.org**

Final Reminder

Your personal information is unique and private. Be cautious of **emails, texts, or calls** asking for personal details or payment to "resolve" account issues — these are almost always fraudulent attempts.

The real goal of fraudsters is to trick you into revealing your personal or financial information. Stay alert and stay safe.