# Password Security Checklist (2026)

## Core Rules

**Use a unique password for every account**
Reusing passwords significantly increases the risk of credential-stuffing attacks. Once a single service is breached, attackers automatically test the same login details across email, cloud services, social media, and banking accounts. Unique passwords stop this chain reaction.

**Use long passwords (at least 14–16 characters)**
Password length matters more than complexity. Long, randomly generated passwords are exponentially harder to crack than short ones with special characters. Modern password managers handle long passwords effortlessly, so there is no reason to compromise.

**Rely on randomness, not patterns**
Names, dates, dictionary words, or predictable substitutions are easy targets for attackers. Secure passwords should be fully random or generated passphrases without any personal meaning or recognizable structure.

## Password Managers

**Store passwords exclusively in a reputable password manager**
Sticky notes, browser storage, or unencrypted files are not secure. A modern password manager encrypts your credentials, reduces human error, and centralizes access securely across devices.

**Enable zero-knowledge encryption whenever available**
Zero-knowledge means only you can decrypt your data – not even the provider has access. In 2026, this should be considered a baseline security requirement.

**Use the built-in password generator**
Manually created passwords are almost always weaker. Built-in generators ensure true randomness and eliminate unconscious reuse or predictable patterns.

## Multi-Factor Protection

**Enable MFA/2FA on all critical accounts**
Email, cloud platforms, social networks, and financial services should always be protected by multi-factor authentication. Even if a password is compromised, MFA can stop unauthorized access.

**Prefer authenticator apps or hardware security keys over SMS**
SMS-based codes are vulnerable to SIM-swapping and interception attacks. Authenticator apps and hardware keys provide a much higher level of protection.

**Use biometrics as a convenience feature, not a replacement**
Fingerprint or facial recognition improves usability but should never replace a strong master password. Biometric data cannot be changed once compromised.

## Breach & Leak Protection

**Enable breach or dark web monitoring**
Many password managers monitor known breach databases. Early alerts allow you to act before attackers exploit exposed credentials.

**Change passwords immediately after a service breach**
Time matters. The faster you update compromised credentials, the lower the risk of follow-up attacks on other accounts.

**Never reuse old or compromised passwords**
Once a password is exposed, it is permanently unsafe. Reusing it – even years later – puts new accounts at risk.

## Common Mistakes to Avoid

**Never share passwords via email, messaging apps, or screenshots**
Unencrypted communication channels are easy to intercept or forward. Use secure sharing features provided by password managers instead.

**Avoid storing passwords in notes, spreadsheets, or browser autofill without encryption**
These locations are common malware targets. Without encryption, stored credentials are effectively exposed.

**“I’ll remember it” is not a security strategy**
Human memory leads to reuse, simplification, and errors. Strong security relies on systems, not recall.

## Advanced Security

**Use passkeys where available**
Passkeys eliminate traditional passwords and are resistant to phishing attacks. They represent one of the most important authentication advancements moving forward.

**Use hardware security keys for high-value accounts**
Administrators, business owners, journalists, and public-facing professionals benefit greatly from hardware-based authentication.

**Separate personal and business password vaults**
Keeping private and professional credentials in separate vaults reduces risk, prevents accidental sharing, and simplifies access control.

**Bottom line:**
Password security in 2026 is no longer about remembering better passwords – it’s about using better security systems.