☑ ONLINE SECURITY CHECKLIST

BY CULLEN THOMAS AND RHETT INTRIAGO

The majority of personal cyber-defense boils down to just a handful of practices and the discipline to maintain them.

ACCOUNT PROTECTION:

☐ Use **strong and unique credentials**. Lock your devices with unique passcodes and use a password manager (but not your web browser) to store strong and unique credentials that you don't have to memorize for every account. If you must use a password, use a passphrase.

☐ Use **multi-factor authentication** (MFA) wherever possible. Passkeys or FIDO certified hardware keys (such as Yubikeys) are the best, push notification systems such as Microsoft's Authenticator are next best (if available), app-based one-time codes are next after that, followed by text message-based one-time codes. Any multi-factor system is better than none.

☐ Lock down your **primary email address**. Only use a modern email system like iCloud email, Outlook, or Gmail with protections turned on, such as MFA, a legacy contact, and recovery codes. Use this account as a recovery option for other accounts.

☐ Avoid **public Wi-Fi**. Instead, use a hotspot. If you must use public Wi-Fi, employ a reputable virtual private network (VPN) such as Nord VPN and avoid accessing private information while connected.

SCAM AND FRAUD DEFENSE:

☐ **Verify the sender**. Check the source address and domain of any incoming email or message before clicking any links. Check the validity of connections made on social media and dating apps using reverse image searches, phone lookups, and by insisting on video calls. When receiving a call about something urgent or scary, hang up and call them back at the official number.

☐ Use **privacy-focused browsers** on the web, including social media. Safari and Firefox are good options. Use a privacy-focused web search such as Duck Duck Go, and employ anonymizing tools like Apple's Private Relay and Hide My Email. Together these reduce the amount of personal and identifying information that can be aggregated about you based on your internet usage.

☐ Use **secure storage** for information that can identify you, such as medical records or passports, and do not transmit it through unsecured connections.

DEVICE DEFENSE:

☐ **Keep your devices up to date** with the latest operating systems and security patches.

☐ Use **anti-malware scanning** software on your Mac or Windows machine and run scans routinely. We recommend Malwarebytes. There are no malware scanners for iPhone, iPad, Apple TV, or Apple Watch.

☐ **Protect your home Wi-Fi router**. Use strong unique credentials both for your Wi-Fi password and for the administrator dashboard. Require multi-factor authentication for the admin dashboard. If possible, disable public web access to admin settings.

☐ **Avoid web browser extensions** except for your password manager and ad blocker.

☐ Run an **ad-blocker** to reduce your exposure to malicious advertising. We recommend NextDNS or Ghostery.

☐ Be cautious with **third-party apps**. Apps have access to your device in ways that websites do not. Prefer Apple-native apps to third-party options—Apple does collect data about your use of its native apps, but its policies about using and sharing that data are excellent at protecting your privacy. If Apple's apps do not provide the function you need, try a website rather than a third-party app. You can bookmark websites to your Home Screen in Safari with Share > Add to Home Screen. Always think twice before installing a third-party app, and remove the ones you don't use.

GLOSSARY OF TERMS

Credential: Anything that can be used to identify an individual as having permission to access a privileged resource such as an account. Most web accounts use a combination of a username (usually an email address) and a password as their credential to identify their users. A credit card is also a credential, since the numbers on it verify permission to draw on the line of credit.

Password: A string of characters known only to you. Used interchangeably with passcodes. Combined with a username as part of a credential. A good way to generate memorable, secure passwords is the three random words method (a passphrase). Longer is better than weirder—don't use one word with numbers and obscure characters. That is hard for you to memorize and easy for computers to guess. Instead, use a set of random words (passphrase) that is easy to memorize but long.

Passcode: A string of numbers known only to you. Used interchangeably with passwords. When you use a passcode (or password) to secure an iPhone, iPad, or Windows PC, the passcode is stored on the device and never transmitted from it. On Apple devices, the passcode is used to generate a unique encryption for all the device's content, so even Apple cannot decrypt an iPhone without knowing the passcode. Also, to use the passcode, you have to have the physical device (eg the iPhone) on hand. Thus, there are two factors which both verify your identity, the device (sort of like a large key) and the passcode (which verifies that it's you since only you know it). These combine to make a credential that can be used to log you in to other accounts and services.

Passkey: This is Apple's name for a system to replace passwords, developed by the FIDO alliance. The full name for this system is FIDO2 WebAuthN, and it is a strong system that relies on hardware keys to unlock accounts instead of passwords and usernames. It's the same system that Yubikeys and other hardware keys use, but using your iPhone instead of a third-party piece of hardware. When you have secured an account with a passkey, the service first verifies that you have your iPhone on hand, then that it's really you with the iPhone's biometric locks. Passkeys can replace passwords, but they may also be used in addition to passwords or other credentials for ultra strong multi-factor authentication.

Passphrase: A string of words only you know. The passphrase, which must be 15 characters long at least, is a more secure version of a password, and can be used in any form that asks for a unique password. Historically, websites and services have asked us to create passwords fitting arcane rules (such as using one letter and one capital letter) that make the resulting password difficult to memorize without significantly increasing its security against computerized attacks. A passphrase represents a better approach to generating passwords, as a string of random words is much easier for a person to memorize, and much more secure.

Hardware Key: A physical key for your online accounts. Normally, these look like USB keys, but they don't store files. Instead, they serve to cryptographically confirm your identity using the same FIDO2 WebAuthn protocol used by passkeys. This is the strongest form of multi-factor authentication because it can't be accidentally given away in a phishing scam or look-alike website.

Key material: Credentials. Usually this term is used in the context of low-level computers talking to computers.

Password Vault: The place you keep all your credentials.

OTP: An ambiguous term that can refer to either recovery codes or TOTP codes. It can stand for One Time Pad, which is an old but still effective form of cryptography, or for One Time Password.

Recovery Codes or One Time Passwords: Codes that can be used once and only once to regain access to an account in the event that the usual password is lost. These codes are generated when you create the account, and are meant to be printed out and stored someplace safe.

TOTP: Time-Based One Time Pad, or sometimes Time-Based One Time Password. A code you are either sent or generate yourself to supplement your primary credential as part of a multi-factor authentication process. Note that, despite being called a One Time Password, an TOTP is always a randomly generated code, not a word.

MFA: Multi Factor Authentication. The practice of requiring more than one credential to affirm an identity. For most websites, a username and password form the basic credential. Since passwords can be guessed or stolen, additional identifying factors are required for an account to remain secure. MFA has become standard practice, but its adoption is not universal.

2FA: Two Factor Authentication. This is just a synonym for MFA.

All products included in this roundup were selected by the iPhone Life team using our editorial selection process, which is independent of our advertising department. We do, however, receive an affiliate commission for Malwarebytes and Nord VPN.