8 Ways You Can Make Your Mac More Secure Right Now

Opinions expressed by *Entrepreneur* contributors are their own.

If you follow technology-related news, you might have noticed the growing threat of data breaches and malware attacks in recent years.

That means it’s more important than ever to review your own security setup these days. You might wonder that if companies as big as Facebook and Block (formerly Square) get hacked, how can you manage to protect your own personal information with the limited resources you have? The good news is that it’s easier than you might think.

A key aspect of IT security is personal vigilance. After all, most malware attacks succeed because people click phishing links and download malicious files. That’s why you have an advantage over much larger tech juggernauts – your surface of attack is much smaller and you’re in full control of your security protocols.

Not sure where to start with getting your Mac more secure? Here are the most important security policies that you should follow.

Related: Cybersecurity Is No Longer An Option. Your Money Is in Immediate Danger.

1. Install an MDM profile

You might know that companies often run MDM (mobile device management) solutions. MDM gives an administrator remote

access to corporate devices for the purpose of updating software, monitoring compliance or remotely wiping them.

You can benefit from using MDM in your personal life as well – if your Mac is ever stolen, you'll be able to locate it and lock it before any of your data gets leaked.

Apple devices have a built-in framework that supports MDM and can be enrolled into MDM solutions through Apple Business Manager.

2. Use a password manager

Password managers are not only secure, but they are also faster compared to manual logins and help you avoid phishing attacks when logging in to online services, by not filling our credentials on incorrect websites.

When it comes to login credentials, it's critically important to:

- Not store passwords in clear text
- Not print passwords on paper
- Not share passwords with anyone via unencrypted communication

Select the best password manager for you and your family, and make sure to use it every time you need to create a new login.

Related: Cybersecurity Practices That Protect Your Small Business

3. Turn on multi-factor authentication

Having secure login credentials creates a single wall of defense against potential attackers. But it's much better to have two.

Two-factor authentication (2FA) requires you to confirm your login on another device, either by creating an OTP (one-time password) via email, an authentication app or SMS, or sending a push notification to your smartphone. Note: 2FA authentication via SMS is not considered best practice due to a SIM swap threat.

4. Enable disk encryption

Keeping all data confidential across your devices should be your highest priority. Encrypting your hard drive ensures that the data on it can’t be read through a data dump in case you lose your device.

Turning on disk encryption on a Mac is as simple as enabling FileVault:

1. Open System Preferences.
2. Go to Security and Privacy.
3. Click to lock to make changes and enter your user password.
4. Turn On FileVault.

5. Back up all data

Having access to recent backups helps avoid data loss due to a stolen or corrupted device, especially with the rise of ransomware attacks.

To back up data on Mac, you need an external hard drive (or a cloud storage solution) and backup software. The most popular backup tool on Mac is Time Machine, a default macOS app.

To turn on Time Machine:

1. Open System Preferences.
2. Go to Time Machine.
3. Select Backup Disk.

4. Check “Encrypt backups” and set a password.
5. Click Use Disk.

Related: The Budget-Friendly Way to Secure Your Business Against Cybercrime

6. Update software and the operating system

Software and macOS updates frequently contain bug fixes and security patches that make your Mac more protected. Make sure to always install the latest updates.

For macOS, use the Software Update pane in System Preferences. For most apps, you can use the App Store Updates tab or check the update availability manually.

7. Keep VPN turned on in public spaces

While you’re at home, you can assume that your internet connection is secure. Just make sure to use a strong password for your WiFi access point and an encryption algorithm such as WPA2 or WPA3.

Outside your home or office environment, it’s important to use a VPN (virtual private network) for additional security. VPN encrypts traffic as it leaves your device, preventing others from snooping on it, especially on public WiFi networks not protected by passwords.

8. Always lock your device

Leaving your device unattended and unlocked is a clear invitation for someone to steal your data and other important information.

If your Mac keyboard doesn’t have a lock screen button, you can quickly lock your screen with a shortcut of Control + ⌘ + Q.

Alternatively, assign a Hot Corner on your screen to lock it:

1. Open System Preferences.
2. Go to Desktop and Screen Saver.
3. Switch to the Screen Saver tab.
4. Click Hot Corners.
5. Set any corner to Lock Screen.

Now, every time your cursor hits a particular screen corner, your screen will lock automatically.

The tips above only cover a few fundamental security practices. But following them will help secure your devices and protect them from attacks and data breaches.

In addition, make sure to go over important security protocols with your family or anyone who uses the same WiFi network on a regular basis. Teach them about spotting phishing attacks and staying clear of any suspicious communications in the future. After all, your security is only as strong as its weakest link.

Business Strategies, Entrepreneurial Advice & Inspiring Stories are all in one place. Explore the new Entrepreneur Bookstore.

https://www.entrepreneur.com/article/427358