BLOG POSTS

Our Best Practices for Securing your Macbook

MacOS has privacy and security tools for hardening your computer. Here are our top tips and best practices to for securing your Macbook. Many of these tips are pretty straightforward, free, or even seem deceptively simple, but together these give you the essential cybersecurity tools and best practices for securing macOS computers at your business.

Many features that someone might consider "convenient" for everyday use can, unfortunately, make it surprisingly easy for hackers to access your macOS. For computers with access to large customer databases or government systems, optimizing your security settings is a critical task.

These days companies develop information security policies, which set guidelines and communicate anything employees are responsible for doing. If your business uses the Carbide Platform to manage your infosec program, you can sign in and see if your company policies require you to follow any of the procedures in our guide below.

So let's look at these tips to set up your computer to protect yourself and your data.

Securing your Macbook: How to Harden Your macOS

Hardening your Mac means that you're configuring the settings to reduce opportunities for a virus, hacker, ransomware, or another kind of cyberattack. Our guide here includes how to use antivirus tools, disable auto-login, turn off remote access, set up encryption, and more.

You can think about security for your computer (with all your personal, financial, or company data), much like you'd think about security for your house. Hardening your Mac is like you're closing the doors and checking the locks. You want to make it harder for hackers to break in.

It might be convenient to leave the front door to your house unlocked or even open all the time. That way, you could avoid the hassle of carrying keys or even bothering with doorknobs. But doesn't that go against the common sense we live by every day? We learn at a young age to close the door and lock it when you leave. Leaving your door wide open is like an invitation for anyone to walk into your house.

Hardening your Mac is a great step in increasing your security. It will minimize the threat of data loss or hacking. We are going to review some of the general best practices when it comes to hardening your Apple computer and review some settings changes that are quick and easy to make on your own. Here are the 11 steps we'll be going over:

1. Turn on the firewall
2. Backup your Mac
3. Disable remote access

4. Encrypt your hard drive
5. Enable or install antivirus protection tools
6. Set up a password-protected screensaver
7. Disable automatic login
8. Create a non-admin account
9. Use a password manager
10. Disable Spotlight suggestions
11. Enable auto-updates

MacOS Hardening Guide: Securing Your Macbook from Hackers, Viruses, Ransomware, and More

1. Turn on The Firewall

MacOS includes an easy-to-use firewall that can prevent potentially harmful incoming connections from other computers.

To turn it on or off:

1. From the Apple menu, select System Preferences.
2. When the System Preferences window appears, from the View menu, select Security & Privacy (10.7 and later) or Security (10.6).
3. Click the Firewall tab. If the orange padlock icon in the lower-left side of the window is closed, click it, and then authenticate with your Mac's administrator username and password. This will allow you to make changes.
4. Click Turn On Firewall (10.7 and later) or Start (10.6) to enable the firewall.
5. To disable the firewall in macOS, click Turn Off Firewall (10.7 and later) or Stop (10.6).

Firewall Configuration in macOS

To configure the firewall, click Firewall Options (10.7 and later) or Advanced (10.6). In the window that appears, choose from the following options:

For the strictest setting, check *Block all incoming connections*.

Check *Automatically allow signed software* to receive incoming connections to allow digitally signed applications access to your network without prompting.

Click *Enable stealth mode* to have your computer ignore pings and similar software that attempts to discover your computer.

Use the plus and minus buttons to add and remove applications from the firewall. When added, you can either allow or block traffic to them.

Click OK to save your settings.

If you use public or unsecured networks at all it is vital to leave this on. even if you were always on a good network that is trusted, having a strong firewall is another benefit to your own personal security.

Company Security Policies on Using Firewalls

A firewall policy defines how your company's firewalls should handle inbound and outbound network traffic. Your firewall information security policy or procedures may need to specify IP addresses or address ranges, protocols, applications, and content types.

To determine what you should include in your firewall policy, you should conduct a risk assessment to develop a list of the types of traffic your company needs and how those should be secured. That includes which types of traffic can cross a firewall and under what circumstances.

If you need to comply with an information security framework, you will want to reference their documentation, such as the NIST guidelines on firewall policies.

Companies may also determine that all inbound and outbound traffic that isn't expressly permitted by their firewall policy should be blocked. Simple steps like enabling firewalls can reduce the risk of a cyber attack.

2. Backup Your Mac

MacOS has a built-in backup tool called *Time Machine*. Once you plug in a hard drive and set up *Time Machine*, it will work automatically in the background, continuously saving copies of all your files, applications, and system files. If you run out of disk space, *Time Machine* will automatically erase the oldest version of the files to make way for the new ones. It's pretty much a "set-and-forget" system for local backups:

Here is how to set up *Time Machine:*

1. Connect an external hard drive to your Mac. You'll need a drive that is at least the same size as your Mac's internal drive. (*Time Machine will by default use up all the space available on the drive.*)
2. Turn on Time Machine and select the backup destination. Once your external drive is plugged in, go to System Preferences > Time Machine and toggle the switch from "Off" to "On."
3. Then click the "Select Disk…" button to select the drive or volume you want to use for *Time Machine*. *Time Machine* will ask you if you want to use the disk as your backup destination and will give you the option to encrypt the backups with a password. The drive needs to be formatted as Mac OS X Extended (Journaled); if it's not, *Time Machine* will prompt you to reformat the drive (which will erase all files on it!)
4. (Optional): Exclude items or get notified of old backup deletions. The "Options" button in *Time Machine* will let you exclude volumes from the backups or get notifications when old backups are deleted.
5. Let *Time Machine* do its work.

Time Machine keeps:

Hourly backups for the past 24 hours

Daily backups for the past month

Weekly backups for all previous months

This blog is meant to provide a starting point for implementing cybersecurity practices within your company. Due to the rapid progression of technology, this is an ongoing and ever-evolving subject!

3. Disable Remote Access for macOS

Remote Access is a useful feature of macOS that lets you access files on your computer from anywhere.

However, remote access also lets anyone with your administrator login and password access files on your computer, which is why it is a good idea to shut this feature off if you don't really use it. In fact, your company may already have a security policy about when employees can use remote access. (If you're on a macOS computer, we have instructions for disabling your remote access here.)

Disabling Remote Access for macOS

1. Click the Apple menu in the top-right corner of your MacBook's screen and select System Preferences.
2. Click the Sharing pane under the Network & Internet heading. If you have your sharing settings locked, click the lock in the bottom-right corner and enter the administrator password for your Mac.
3. Uncheck the boxes next to Remote Login and Remote Management. Click the lock again and re-enter your administrator password if you want to prevent future changes.
4. Close your System Preferences.

You're done! You've disabled remote access on your macOS.

The Risk of Remote Hacks

It might sound paranoid or far-fetched to consider that someone would maliciously use remote access. But it's not.

Security researchers actually discovered a vulnerability in Apple computers for enterprise companies that allowed them to hack a brand new Mac the first time it connected to Wi-Fi.

While remote access can be a convenient tool, enabling it all the time can increase your risk exposure. Because of that, companies may implement information security policies to give employees guidance on when they can use it.

4. Encrypt your Hard Drive

We know that encryption is important for the protection of your data. And there's no excuse since your Apple computer comes with tools to encrypt a hard drive in macOS.

Turn on and set up FileVault

1. Choose Apple menu > System Preferences, then click Security & Privacy.
2. Click the FileVault tab.
3. Then click the "lock." Enter your administrator name and password.
4. Click Turn On FileVault.

When FileVault is on, your Mac will require that you log in with your account password.

If other users have accounts on your Mac, you might see a message that each user must type in their password before they will be able to unlock the disk. For each user, click the Enable User button and enter the user's password. User accounts that you add after turning on FileVault will be automatically enabled.

Set How Your Unlock Your Hard Drive

Choose how you want to be able to unlock your disk and reset your password, in case you ever forget your password:

If you're using OS X Yosemite or later, you can choose to use your iCloud account to unlock your disk and reset your password.

If you're using OS X Mavericks, you can choose to store a FileVault recovery key with Apple by providing the questions and answers to three security questions. Choose answers that you're sure to remember.

If you don't want to use iCloud FileVault recovery, you can create a local recovery key. Keep the letters and numbers of the key somewhere safe—other than on your encrypted startup disk.

Encryption occurs in the background as you use your Mac, and only while your Mac is awake and plugged into AC power. You can check progress in the FileVault section of Security & Privacy preferences. Any new files that you create are automatically encrypted as they are saved to your startup disk.

Restart Your Mac After You Turn On FileVault

When the FileVault setup is complete you'll need to restart your Mac. You will use your account password to unlock your disk and allow your Mac to finish starting up. FileVault requires that you log in every time your Mac starts up and no account is permitted to log in automatically.

Your Security Policies May Require You to Turn on FileVault

Stuff happens, so don't be that person who gets an unencrypted laptop stolen from their car which leads to 43,000 patients getting notified their information was stolen. Encrypting your devices is a low-effort way to boost your security.

This is the kind of best practice that many companies require employees to follow in their security policies and procedures. Vendor security questionnaires often ask about your encryption policy and practices.

Especially for B2B companies that are under scrutiny from enterprise customers or regulatory authorities, it's important that all your employees encrypt their hard drives.

5. Enable or install antivirus protection tools

It's important to routinely check your computer for viruses.

You may have been led to believe that you don't have to worry about computer viruses on your Mac. And, to some extent, there's truth to that. Although your Mac can still be infected with malware, Apple does have built-in malware detection and file quarantine capabilities. These are designed to make it less likely that you'll download and run malicious software.

If you're on a Mac computer, learn how you can check for viruses.

Apple introduced malware detection to the Mac OS starting with Snow Leopard (Mac OS 10.6). Because of this system, called File Quarantine (occasionally referred to as XProtect), apps that are known malware cannot be opened at all. Instead, you'll see a message offering the option to toss the app in the trash.

To make sure your Mac malware database is always up to date you'll want to verify that your Mac always automatically installs security updates and related system data files.

Automatically Check For Viruses

1. Open System Preferences
2. Open the App Store preferences
3. Make sure that you check *Automatically check for updates* and *Install system data files and security updates*.

This should keep your Mac free from most malicious software, although it's important to note that it does not make it *impossible* for malicious software to be installed on your Mac. So it's always best to be cautious when downloading software from unknown sources.

And never, never click "install" or dismiss a warning message if something looks suspicious. You don't want to run the risk of infecting your entire company with a virus that gets into your local network.

6. Setup a Password Protected Screensaver

Protecting your Mac's screensaver with a password is simple. Yet many users don't think about doing it.

Set Up a Screensaver With a Password

1. Open System Preferences. If the icon is not in your dock, you can access it by opening the "Apple Menu" that is always visible in the top left corner of your Mac's screen.
2. You can find the screensaver's password settings under the "Security" icon. In the pane that appears, tick the box that says "require password immediately after sleep or screensaver begins."

And boom! You're finished! Now, the next time the screensaver is running you will be prompted for your Mac's password before you can start using it. If these steps don't match the macOS version you have, Apple has a support page you can check.

When you wake your computer or the screensaver comes on after you're inactive, it might seem silly to have to enter in your password to get back in. But a little inconvenience for you means a lot of inconvenience for hackers or someone stealing your computer.

Yes, using a screensaver with a password is optional (unless your company has information security policies that require this setting), but it's your choice to make yourself an easy target.

Password protecting your computer after a screensaver seems basic. And it is. But many people ignore little steps like this. That's why company security policies are so crucial to communicate with employees. If your company requires all work devices to have passwords, that is a security policy that everyone should know and be held responsible for following.

This may even be a topic or policy that prospective business customers ask about in a vendor security questionnaire.

Each time we let our guard down, that leaves a new vulnerability in our computer system or even a company network. If you have a B2B company, lax security practices can ultimately lead to a poor cybersecurity posture that damages your sales.

7. Disable Automatic Login

Automatic login can be either a useful feature for devices in the workplace… or a vulnerability in your security program.

When you set up a new Mac or do a clean installation of a new version of macOS, the first thing you do is create a user account. That account is set, by default, to log in automatically at startup.

Convenient, right? Only if you're working from home 24/7. If you use a laptop and travel for work, this can leave you at a big risk. This automatic login means that anyone who finds your Mac just needs to start it up. They now have access to all your files, including personal and internal emails, or customer data.

You can change this and tell macOS to display a login screen on boot instead. (We also have the steps to change this setting in Windows 10 too.)

Instructions to Disable Automatic Login in macOS

1. Go to the Users & Groups pane of System Preferences and click on Login Options.
2. You'll see a menu that lets you choose which user logs in automatically at startup. Choose Off from this menu to turn off automatic login.
3. That's it! Congrats! Your macOS is more secure now.

Alternatively, you can also change this setting from System Preferences, then clicking the Security & Privacy preferences. If you click on the General tab, you'll see an option to Disable Automatic Login.

Setting your display to timeout is a great way to lessen the chances of someone accessing your device if it is left unattended. The inactivity notification is a configurable period of time during which the user can be inactive, after this period of time the device is locked and will require a password to log back in. Changing the setting will reduce the chances of anyone accessing your device if you step away from it for a moment and forget to lock or close the screen. Not only does this increase the security of your device but it can help increase battery life as well. The timeout should be set in accordance with the security policies of your organization.

This simple step is one of the many easy things you can do to make yourself more secure at work.

8. Create a non-admin account

Before using a company device for non-business purposes or sharing it with another member of your family you should ensure that using a company device for other activities is permitted by your security policies. If it is permitted it is important to set up a specific account for these activities. Check that your company's policy on acceptable use and their device management policy is in line with creating this account. These policies will outline what you can do with the device, as certain organizations will not allow you to use a company computer or personal activities.

When you get a new Apple laptop or desktop the setup assistant asks you for your name, a username and a password and uses this information to set up your first user account. This first user by default is an administrator meaning they have full access to your device. Administrator accounts can change or delete any file and install any software, which may be a risk if the software is malicious. A standard user account will have less access and depending on permissions can be very restricted by default. They can only use, change and create files in their home folder, access folders on shared volumes and depending on permissions, change settings to system preferences. To create a non-admin account click on:

System preferences from the menu

Select users and groups

Click the plus sign to create a new user

While you are entering the information for this users account to ensure that it's set to be a standard user account.

9. Use a password manager

Every organization should have a password policy and when creating your account you should always follow this policy. It will ensure that you are using at least the minimum requirements as outlined by your organization. When creating your passwords for each account depending on the requirements and the number of applications you may have a large number of complex passwords to remember; especially if your password policy requires you to change them every month.

Passwords should never be written down as well so this can make things even more difficult. Using a password manager allows for the creation of complex unique passwords so they're more difficult to crack and creates an encrypted way to store them so the process of entering them can become automated. There are a number of great tools out there for password managers. No matter what your needs are there should be one that fits your organization. along with using a password manager, two-factor authentication should be used when possible on all accounts that support your iCloud account. Two-factor authentication adds an extra level of security on top of your already complex password.

10. Disable Spotlight suggestions

OSX updated the spotlight feature that is commonly used to search your device. the update allowed for suggestions from the internet to be included. these suggestions can be manipulated and allow for data to be tracked by third parties some of the data can be sent to Apple itself or third-party providers such as

Microsoft Bing or Google search engine. to prevent this from happening or limit what appears on spotlight you should update these default settings:

Open System Preferences

Choose Spotlight now

Deselect Spotlight suggestions

Changing these settings will stop this from happening in Spotlight, However, Apple's default browser Safari does the same thing. In order to stop this from happening in Safari click on:

Safari

Select *preferences*

Click *search*

Disable *include spotlight suggestions*

Now, review your security and privacy settings. What applications are you sharing your personal location with? What do the apps you have installed have access to on your device? If you are unsure or want to prevent location data access you need to review your security and privacy settings.

Under the Privacy tab, you will see a listing of all applications and what they have access to on your Mac. Under location services, you can make any changes by logging in as an administrator and unchecking or checking the applications you would like to grant or revoke access to. From these services finally, never leave your computer unlocked and unattended. There's a good chance it will not be there when you return or it could have been altered in some way without you knowing. Always lock your computer when unattended to keep private eyes from rubbing your information or taking your laptop.

11. Enable Auto-Updates

Apple makes it easy to enable auto-updates for your macOS. It all happens in the background while you're going about your day. Apple will never install an update without your permission, but they'll make sure you don't have to wait around your desk for hours when you want to install it.

It will only take you a minute or so to enable auto-updates on your Mac.

Here's How to Automatically Update macOS:

1. Choose Apple Menu > System Preferences, then click App Store.
2. Select "Automatically check for updates."
   To have your Mac download updates without asking, select "Download newly available updates in the background."
   Get your Mac to install app updates automatically by selecting "Install app updates."
   To have your Mac install macOS updates automatically, select "Install macOS updates."
   To have your Mac install system files and security updates automatically, select "Install system data files and security updates."
   updating your software will allow all security patches as they come out to be installed without delay. this is very important to maintaining your security on your own device.

Easy as that! Now you'll never miss an update on your Mac. You can also check Apple's support guide about enabling updates, which may differ a little depending on the macOS version you are using. (Get the steps to enable auto-updates on a Windows 10 system here.)

Why System Updates Are Critical for Your Security

It's important to automatically update your operating system. Or if you need to do it manually, to check and hit update on a regular basis.

Some updates are for critical security reasons. Ignoring security updates leaves you vulnerable to known issues and cyber attacks. The devastating ransomware attacks in 2017, known as Petya and WannaCry, both targeted outdated computer software. It sounds scary, but there are actually some simple steps that will help protect you from ransomware.

You may even have an information security policy at your company that requires you to enable auto-updates. If half the computers at your company were taken down because they had outdated software, that would cause a major business disruption. And that's not a far-fetched scenario. It's a serious risk that companies need to consider and mitigate.

Installing security updates is an easy way to protect yourself. Also your company and all your customers.

ABOUT THE AUTHOR

Kyle Hankins

All Posts Written by Author

in

TAGS: cybersecurity information security

Related Content

BLOG POSTS

Security Best Practices for Your Windows 10 Computer

BLOG POSTS

The (New) Best Practices for Your Password Policy

Carbide

NEWSLETTER SIGNUP

Accelerate your security initiative.

Email Address*

□ Subscribe and stay informed.

PRODUCT
- Platform
- Premium
- Pricing
- Integrations

FRAMEWORKS
- GDPR
- HIPAA
- ISO 27001
- NIST
- PCI DSS
- SOC II

SOLUTIONS
- Build a Program
- Get Compliant
- Operationalize Security
- Enter New Markets

RESOURCES
- All Resources
- Case Studies
- Blog
- Videos
- eBooks
- News
- Glossary

COMPANY
- About Carbide
- Careers
- Contact