MacOS Security Tips

In addition to cellphones, laptop and desktop computers are typical repositories of highly personal and private information. While Apple's MacOS operating system is a relatively secure platform in its default state, there are a few steps you can take to elevate and maintain that security.

ENABLE ENCRYPTION ON YOUR MAC

Introduced quite some time ago in MacOS 10.3, FileVault encryption helps protect your entire disk from compromise. The latest version is FileVault 2. Assuming you choose a strong password, FileVault is very difficult to bypass and will prevent your data from being accessed if your computer is stolen while it is turned off, and most likely even if just locked or in standby mode. If you are passing through a government security checkpoint, especially one at an international border where your rights are limited, turn your computer off completely beforehand. This makes it more difficult for the password to be forensically recovered from memory, and disables fingerprint reader access until the password is manually entered again. The only easy way in will be if you provide your password.

USE STRONG PASSWORDS FOR YOUR MACOS USER ACCOUNT, ICLOUD, ICLOUD KEYCHAIN & EMAIL

It is important to utilize a strong password for your Mac's user account, your iCloud & iCloud keychain, and your email. The integrity of your encrypted disk is only as good as your account password. Your iCloud account can sometimes be used to unlock your Mac. iCloud can also be used to track your Mac's location, and many of your computer's files and passwords may be stored there. Using a strong and unique email password is critical because if this account is breached, a password reset can be conducted on your other accounts and anyone with access to the email can then access those accounts as well. Access to someone's email is like having the master-key to the kingdom, unless two-factor authentication is in place for other accounts. We highly recommend two-factor authentication be used for iCloud.

You will definitely want to refrain from enabling MacOS's automatic login feature, as it defeats the purpose of using disk encryption. You'll also want to set the screensaver to turn on after a short period, and require authentication after halting the screensaver. All of these features are available in the MacOS settings.

USE A FIREWALL FOR TRAFFIC IN/OUT

Thankfully MacOS includes a built-in software firewall that you can enable, but it does not include much in the way of outbound traffic protection. For this purpose we recommended the Little Snitch application. Little Snitch notifies you of whatever application/process is attempting to send traffic out from your computer. By monitoring Little Snitch's alerts, you can deny threatening or unnecessary communication to third-party servers. Without outbound protection, the contents of your entire hard drive could be uploaded to another party in a matter or hours.

You may also want to consider a hardware firewall option, though this is less important with MacOS than with Windows. Also consider enabling stealth mode in the MacOS firewall options, as this will prevent your computer from responding to unsolicited ping requests.

MONITOR YOUR MAC'S CAMERA & MICROPHONE

The OverSight gives notification anytime your Mac's microphone or camera are activated. If an application is attempting to covertly listen in or watch you, you'll be alerted. Another option is to cover your Mac's camera with a sticker, but this doesn't solve the microphone issue. The cameras on Macs are hard wired to turn on a green indicator light anytime the camera is activated, though there are unconfirmed reports that this has been remotely bypassed on certain models.

MINIMIZE USE OF CLOUD STORAGE

We recommend generally limiting the information you store in the cloud. When storing your data on a cloud server, it is connected to the internet 24 hours a day, 365 days a year. In the event that the cloud provider's servers are breached, your data could be compromised. Think of storing information in the cloud just the same

as storing information on someone else's computer. Would you trust someone else to protect your most sensitive data?

If you do use cloud storage, consider encrypting the data independent of the type offered by the cloud provider. For example in Microsoft OneNote, individual tabs can be protected, and in Apple's Notes app, individual notes can be password protected. When this is done, additional encryption is added, increasing, but not perfecting security. Other independent encryption options are available for ZIP and PDF files.

SECURELY BACKUP YOUR COMPUTER

If your computer is stolen, the hard disk fails, or you forget your password, you'll want to have a backup. Backups should be regular, but introduce a new vulnerability. If you don't encrypt the backup disk and it is stolen it's just as if your computer itself went missing. Using MacOS's built in TimeMachine application you can enable encrypted backups. We suggest using a backup disk that can be unplugged from the computer and stored in a fire/theft resistant safe when not in use. Imagine if you are on vacation and your home or office burns down, destroying both your computer and backup disk.

UPDATE SOFTWARE OFTEN

Consider updating your version of MacOS between one week and one month from the release of a new version. Most updates include security fixes that prevent your computer from local or remote compromise. Postponing updates at least a week after release helps you avoid detrimental software bugs sometimes found in versions prematurely distributed to the public.

REDUCE ATTACK SURFACE - NO FLASH, NO JAVA, DISABLE AIRDROP

There are numerous ways that a computer can be compromised. Best practice to lower your risk is to reduce something called "attack surface". This essentially means closing vulnerabilities, and making yourself a more difficult target. Two

major vulnerabilities that exist on many systems are the presence of the Flash player and Java (not to be confused with JavaScript). Both applications are historically known for poor security. Most users do not need either one of these applications and it is recommended to uninstall them if they are present.

You should also turn off AirDrop when it is not in use, as this makes your computer less visible on networks. We would suggest turning off Bluetooth, but this is impractical to users of wireless keyboards and mice. As another measure of reducing network visibility you should change your computer name to read something other than "Joe's MacBook". This could lead to you being specially targeted due to your identity or platform.

DON'T RUN AS ADMIN

None of us plan to get a virus, but it still happens (just less often on the Mac platform). If you use one account as your administrative account, and another account for your daily activities, you make it more difficult for a virus to fully control your system. The only downside to this method is that you may have to type the admin account's username and password to authenticate when executing certain system-level tasks.

BEWARE OF MALWARE IN DISGUISE

Websites are able to determine what operating system you are using and present targeted ads. These ads may appear to be local operating system pop-ups claiming that your system has been compromised or needs a "tune up". If you download and install this malware in disguise your system may begin to experience all sorts of issues. One of the most common examples of this malware is MacKeeper - a product that purports to make your Mac run better, yet it does just the opposite.

Aside from the software and tips that we mention here in this blog, MacOS includes just about everything your system needs to be secure, right out of the "box". If you do mistakenly download malware or spyware, we recommend Malwarebytes Anti-Malware as a cleanup tool.

BEWARE OF EMAIL PHISHING & ATTACHMENTS

A common way both Mac and PC users are compromised is through email. Sometimes they are sent nefarious attachments which they open and become infected, but in an increasingly common type of attack, they are phished. Phishing is where a malicious actor sends an email that looks like it is coming from a reputable service provider such as FaceBook or a bank. In the email the recipient is informed that they must click a link and enter their username and password for a seemingly legitimate and urgent reason. For example, the email will state that the user's account has been compromised and they must log in immediately to rectify the issue. When they log in, their credentials are sent to the attacker, and the user's account is now compromised. The attacker often uses this initial attack as a springboard for a broader one. The following are some signs that an email may not be legitimate:

- *ANY* request for you to click a link in your email and enter your username/ password or provide banking/credit card information
- Hovering over links show that they go to a site not associated with the alleged service provider, or the domain name seems abnormal
- Variations of a familiar web address (e.g. FaceBoook.com, City8ank.com, twitter.FB500.com)
- Poor use of the English/local language (many phishing attacks are conducted by foreigners residing in countries where they are less likely to be successfully prosecuted if caught)

CONSIDER ENCRYPTED COMMUNICATION OPTIONS

Ensure your home and office networks are either wired or encrypted with WPA2. The original WPA is decent, but if you are using WEP encryption or nothing at all, your network is vulnerable to abuse.

You may also want to consider a virtual private network (VPN). Deployed properly, a VPN can help protect your identify when browsing from home or work and boost the confidentiality of your communications while on public wifi networks.

ANTI-VIRUS & OTHER CONSIDERATIONS

You may want to consider installing an anti-virus application. Anti-virus software used to be considered unnecessary when the Mac platform had less marketshare, but times have changed, and the MacOS platform is now being targeted more than ever. There are many anti-virus options available for Mac, including Avast, Sophos, ESET, Bitdefender, Avira, and Kaspersky.

Beyond the above, there are additional ways to make your Mac more secure, but they are generally more complex or costly. We suggest starting by implementing most or all of the steps we outlined -- your Mac will be relatively secure at that point. If you need additional support, contact us for a personal or business security consultation.

Original Document Source: https://www.discernum.com/library/mac-security-tips