

PERSONAL DIGITAL SECURITY

A cybersecurity guide for solo practitioners and individuals

Revision 3.14.2



<https://TechFramework.com>

TABLE OF CONTENTS

The Importance of Personal Cybersecurity	2
Home Router Security	3
Firewalls	5
WIFI Security	8
Malware Protection	10
Online Accounts	11
Protecting Your Personal Information	14
The Risks of Public WIFI	15
VPNs	16
Strong Passwords	17
Passwords Managers	18
Two-Factor Authentication (2FA)	19
Secure Texting	20
Secure and Private Email	21
PC and Mac Patching	22
PC and Mac Full Disk Encryption	24
Identity Theft Protection	26
Backups & Recovery	28
Good Habits	29

Who Should Read This?

This book is for anyone interested in personal and home cybersecurity guidance without much industry tech jargon.

Disclaimer

Cybersecurity and Information Technology change at a rapid pace. This book is not intended as an instruction manual but to advise you on best practices. Technical Framework, LLC, is not responsible for outdated information, nor are we responsible for failure to use the information successfully.

Copyright

Technical Framework reserves all intellectual property rights. Redistribution of this book, all or in part, is strictly prohibited by copyright law.

Credits

This book was an effort by the entire team at Technical Framework.
<https://techframework.com>

THE IMPORTANCE OF PERSONAL CYBERSECURITY

FINANCIAL LOSS

You stand to lose a considerable amount of money if you are hacked. Some or all of those losses may be irreversible, even if you are insured. Furthermore, the losses may not be immediately realized but could happen over a long period.

LIABILITY

If you harbor information on other individuals, as do medical, financial, real estate and insurance practitioners, you bear the risk of a civil lawsuit and government fines. Every state has reporting laws and penalties for breach of personally identifiable information (PII).

REPUTATION

If you are a business professional, suffering a hack due to a lack of due diligence and having to report the incident to all clients, vendors, and other constituents is sure to affect your bottom line, if not sideline you completely.



HOME ROUTER SECURITY

First, let's clear up any confusion between an Internet modem and a home router.

Your Internet modem is the device provided by your Internet provider and links your home to the Internet, much the same as a phone landline connects a phone to your phone company.

In contrast, the purpose of your home router is to securely connect all your wired and wireless devices, such as computers, smartphones, and TVs, to your Internet modem. Common home router brands include Netgear, TP-Link, and Linksys.

Your home router should be set up and maintained by a trained professional.

Following are the most critical security practices for home router setup and the most common points of a cyberattack when not followed.

DEFAULT PASSWORD

The first step after connecting to your home router should be to change the default password.

OUTDATED FIRMWARE

Throughout its life, your router must undergo firmware (software) updates, which resolve security vulnerabilities and bugs, among other benefits.

BACKDOORS

Any intentional or unintentional bypass of your home router's security is a backdoor. Examples include connecting to WIFI other than your home router's, such as the WIFI of your Internet modem or your neighbor's WIFI. Another example is a wired connection from one of your devices to your Internet modem or another Internet link not protected by your home router.

GUEST VS. TRUSTED WIFI

A capable home router should allow you to enable "guest" WIFI. Unless you intentionally allow it through the router's settings, devices that connect to guest WIFI cannot talk to devices on the main (trusted) WIFI. Visitors and non-computer devices such as TVs and digital assistants should use the guest WIFI.



FIREWALLS

While firewall science is well beyond the scope of this book, it's worth knowing basically what they are and why they exist.

There are generally two types of firewalls: hardware and software. Both work as a barrier against hacks.

Hardware firewalls earn their name because they are part of a hardware appliance like your home router. Software firewalls come standard on PCs and Macs and are turned on by default. It's usually not necessary to change the default settings of your firewall(s), and doing so requires the services of a trained professional.

Why do you need both? Your hardware firewall works much like a guard at the outer gate, blocking threats before they enter your home network. Your software firewall is another line of defense barrier in case your hardware firewall is penetrated or when you are using your device outside your home where the firewall of your home router does not protect it.

Firewalls are necessary but not bulletproof and can be bypassed if you inadvertently download malware or click on a phishing link, among other ways.

WINDOWS FIREWALL MAIN SCREEN

Windows Defender Firewall

← → ▾ ↑

Control Panel > System and Security > Windows Defender Firewall

▾ ↻

Control Panel Home

Allow an app or feature through Windows Defender Firewall

Change notification settings

Turn Windows Defender Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

See also

Security and Maintenance

Network and Sharing Centre

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help to prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks

Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Defender Firewall state: On

Incoming connections: Block all connections to applications that are not on the list of allowed applications

Active private networks: Network

Notification state: Notify me when Windows Defender Firewall blocks a new app

Guest or public networks

Not connected

Networks in public places such as airports or cafés

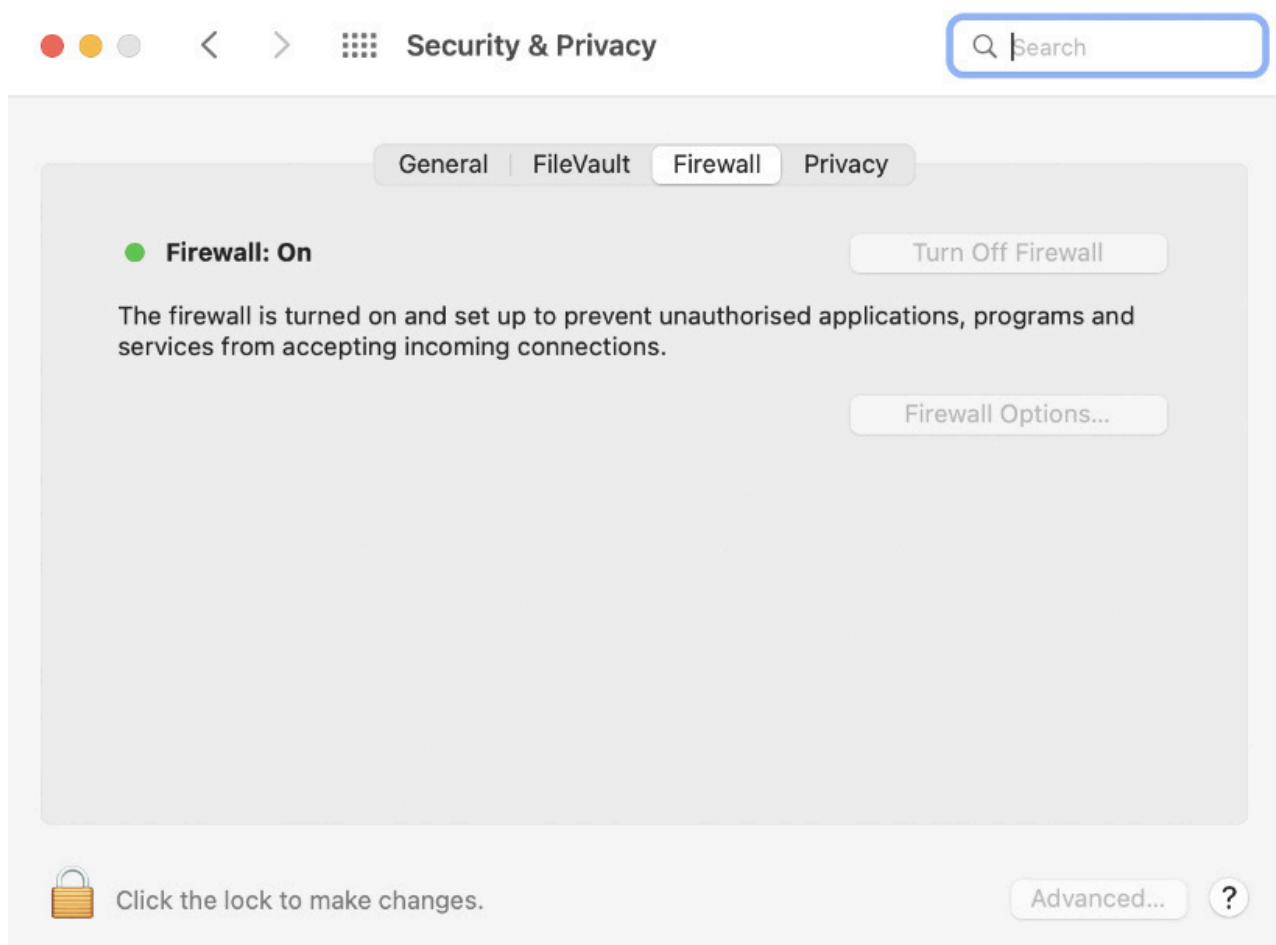
Windows Defender Firewall state: On

Incoming connections: Block all connections to applications that are not on the list of allowed applications

Active public networks: None

Notification state: Notify me when Windows Defender Firewall blocks a new app

MAC OS FIREWALL MAIN SCREEN





WIFI SECURITY

For the purposes of this book, WIFI security takes four forms:

- Encryption type
- Secure password
- MAC address filtering
- Hidden SSIDs

You do not need to be a WIFI network engineer to manipulate any of these settings, but you might get a headache trying to figure them out if you're not technically inclined, so do not hesitate to consult a trained professional.

Encryption is scrambling information between your device and your home router to prevent eavesdropping. At the time of this writing, the most secure wireless encryption is WPA2 and WPA3. WPA stands for "WIFI Protected Access," but like most technology acronyms, it's not helpful to know what the letters stand for.

WPA2 is compatible with more devices, but WPA3 is more secure. Both are secure enough for you to feel safe.

Length is more important than complexity when it comes to WIFI passwords.

So, make the password at least 15 characters, but there's no need to make it impossible to type. Ensure you use upper and lower case letters, at least one numeral, and at least one symbol (!@#\$, etc.)

Any device with wired or wireless network capability has a manufacturer assigned MAC (Media Access Control) address, essentially a unique hardware ID. You can set up your router to allow only specific MAC addresses, so even if a hacker discovers your WIFI password, they still cannot connect to your network.

Hiding your SSID means your WIFI will not show on a list of available networks, thereby making it invisible to all but specialized detection equipment. To connect devices to a hidden SSID, you must remember the WIFI name and type it in manually when establishing a connection.

MALWARE PROTECTION

Malware protection should be installed and continuously updated on phones, tablets, Macs, and PCs. While free products may be attractive, paid products almost always have more robust protection and advanced capabilities.

Reputable names in this area are BitDefender, Kaspersky, Avira, and Webroot. Set aside time monthly for you or your technician to review malware protection status and updates. If you're unsure how to evaluate and select malware protection, consult a trained professional.

Bitdefender®



Avast

Malwarebytes



WEBROOT®



ONLINE ACCOUNTS

If you're like most people, you've created countless online accounts, many of which you don't use or have forgotten entirely. Unfortunately, each abandoned account is another entry point into your digital life and should be closed. But how do you find them all and prevent losing track of accounts you create in the future?

Fortunately, there are several methods of abandoned account scavenging.

EMAIL SIGNUPS

For accounts you've created by "Signing Up With Google", you can head over to Gmail's security settings. You can review the list of connected apps to edit or revoke their access.

SOCIAL MEDIA SIGNUPS

You can also browse all the apps and websites you've logged into using

your social media accounts, as each has a privacy settings area. You can decide what you want to share or cut off on most platforms. For instance, on Facebook, you can stay connected to a third-party account while disabling its access to the pages you like.

INBOX CLUES

Another method is to hunt down the confirmation emails from each account creation in your inbox.

Search for common subject lines these services send you whenever you register for a new account. A few that work well include "signing up" and "thank you" and keywords like "confirm" or "confirming."

You can also use Gmail's search operators and keywords for filtering specific subject lines. "Subject: verify" will fetch all the emails with subject lines containing the word "verify," to name one example. This technique lets you discover roughly every app linked to your email address.

ACCOUNT DELETION

If you've ever wanted to delete your account from a website, but had no idea how to go about it, here's some help.

JustDelete.me is an easy-to-use tool that lets you search for all of your online accounts across multiple platforms in one place. It's free to use.

The website shows a grid of sites and links you directly to the page on the site where you can delete your account.

If you want to delete your account from a site, click on the Show Info link for that site, and then follow the instructions on the page. The links are also color-coded based on how easy or hard it will be for you to delete your account.

BROWSER SAVED ACCOUNTS

Whenever you fill out a form field on the Internet, your browser caches your input, so you don't have to type in your info manually the next time around. This applies to email addresses and passwords, too.

While this is a valuable feature that can help you populate forms quickly and effortlessly, it's a good idea to manage your autofill settings from time to time to double-check or update your information.

You can visit your browser's settings and go through the list to find any accounts associated with email addresses long past that you may have forgotten. Your success will depend on how long it's been since you cleared your browser's cache.

PROTECTING YOUR PERSONAL INFORMATION

You may feel that online privacy is a thing of the past. Advertisers and megacorporations seem to know almost everything about you! They don't have ESP, though. They're good at online profiling or buying data brokers' profiles.

These legal brokers scrape the Internet for the information they can package and sell. You can tell them to erase your data, and legally they have to comply, but there are so many! Services like Optery and Removaly handle the task of finding your data online, getting it removed, and verifying the cleanup. Both services give details about located profiles and make a free version available with practical DIY opt-out instructions.



Optery

 **REMOVALY**



THE RISKS OF PUBLIC WIFI

The most significant risk of public WIFI is the ability of the hacker to position himself between you and the connection point. So instead of talking directly with the public venue's WIFI system, you're sending your information to the hacker unwittingly. Think about the last time you were at a coffee shop, airport, or trade show. How do you know you connected to a legit WIFI access point? Remember that anyone can set up a WIFI system with any name to steal your data with minimal investment in time and knowledge.

Here's how to protect yourself from hackers in a public venue.

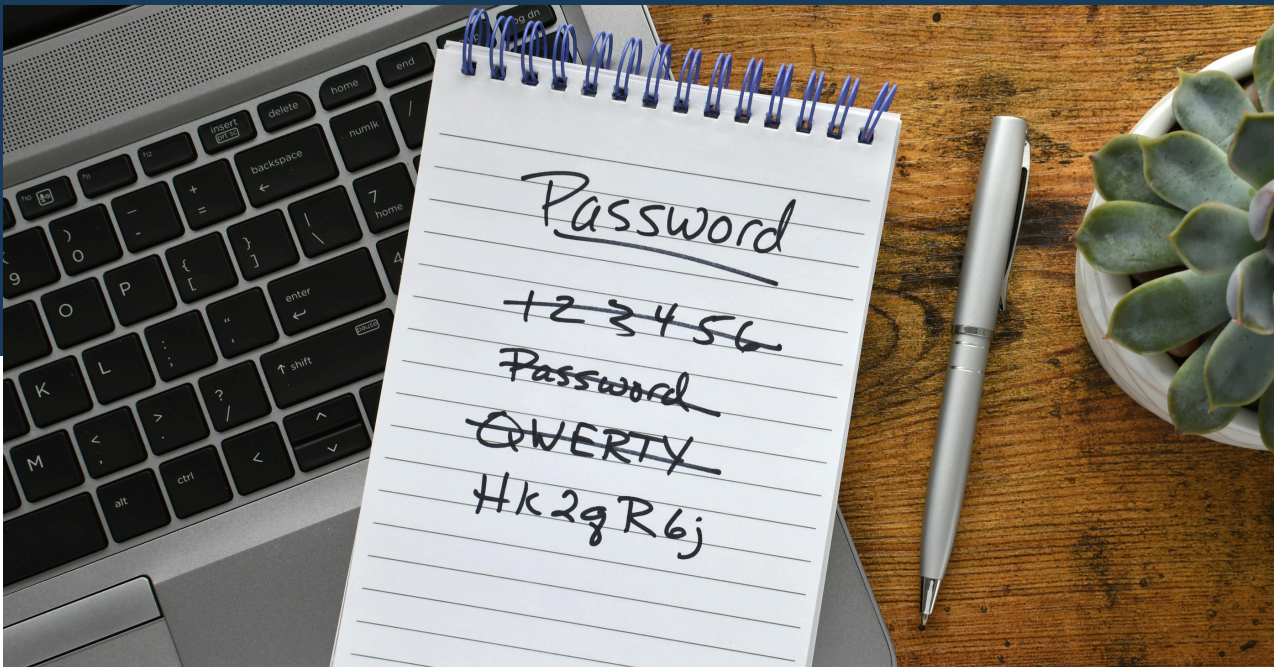
- Turn off the WIFI on your smartphone, and turn on the hotspot feature. Then, connect your laptop or tablet to your smartphone for Internet access.
- If you have no choice but to connect to the public venue's WIFI, use a VPN service such as NordVPN, ExpressVPN, ProtonVPN, or Private Internet Access to protect your communication.
- Remember to avoid transacting sensitive information if possible, while using the public venue's WIFI.

VPNS

A VPN (Virtual Private Network) service increases your information security and privacy and is especially useful when using public WIFI. Reputable providers include NordVPN, ProtonVPN, ExpressVPN, and Private Internet Access. While some providers offer "free" VPN services, paid subscriptions are worth the investment, especially if you travel frequently and find yourself using WIFI in airports, coffee shops, and restaurants. Once you subscribe to a VPN service, you'll be prompted to download the app for PC, Mac, or smartphone, all of which you can protect.

The caveat with VPN services is that you sometimes have to turn them off to access your desired website. For example, some financial institution websites will not allow you to log in if your device is connected to a VPN service. However, this issue should not deter VPN usage as the gains tend to outweigh the inconveniences.





STRONG PASSWORDS

By now, you've probably received a lecture from a tech about strong passwords, so this section will be to the point. Here goes:

- Use a unique, random password for each online account, consisting of 10+ characters.
- Include uppercase, lowercase, numbers, and symbols (!@#\$, etc.)
- Manage the passwords with a password manager.
- Change passwords for critical accounts, such as banking, investments, email, etc., at least once per year.

Why go through the pain of strong passwords, management, and frequent changes? Because member databases of companies from which you purchases services suffer breaches. Once hackers get hold of the database, they run cracking programs on the password list, exposing the simple passwords, which are then sold on the dark web along with other member information. So, if you use a simple, non-unique, old password for any of your accounts, you risk becoming a statistic.

PASSWORDS MANAGERS

A password manager is an app on your phone, tablet, or computer that acts as a digital vault to store, protect, and remember your passwords. Once you've logged into the password manager using a 'master' password, it will remember your passwords for any account. Many password managers can also automatically enter your passwords into websites and apps, so you don't have to type them in every time you log in.

Robust password managers such as 1Password and LastPass also store dozens of other types of information, such as lock combinations, ID numbers, serial numbers, and the like.

If you don't use a password manager, you're probably using a note file or spreadsheet to store your passwords, which means you're wide open to hacks.

Remember to use two-factor authentication to protect your password manager vault's master password.

1Password

LastPass...

DASHLANE

NordPass

RoboForm

KEEPER



TWO-FACTOR AUTHENTICATION (2FA)

2FA (also referred to as multi-factor authentication or "MFA") is an extra layer of security used to protect your account if your password is stolen. First, a user will enter their username and password. Then, instead of immediately gaining access, they will be required to provide another piece of information, such as a code received via a text message or from an authentication app.

There are more complex ways of implementing 2FA, but they are well beyond the scope of this book and don't necessarily apply to the mainstream. 2FA is no longer an option but a must. If you are not using it for your online accounts. Assume you have been compromised.

SECURE TEXTING

Text messaging is an inherently insecure method of communication. Besides storing messages on servers without your knowledge, cellular providers don't always encrypt communication between sender and receiver. If you want your messages to remain private and secure, use an app like Signal (Signal.org) or Telegram, both of which are free.

Signal provides secure texting and allows you to delete a message you have already sent with an option to delete on your end, the recipient's end, or both. Lastly, Signal also allows you to make secure voice calls as an additional bonus. Oh, and don't worry, you can use both Signal and Telegram alongside your existing texting app.



Signal



Telegram



SESSION

wire

SECURE AND PRIVATE EMAIL

One mode of communication that's here to stay is good old email. Unfortunately, the security and privacy of most email providers don't match that of Protonmail.

Protonmail, which at the time of this writing also offers contacts and calendars, is based in Switzerland and arguably provides the most secure emailing services for personal use. Among features are a password-protection option for each message and the capability to set a "self-destruct" timer, so emails disappear from the recipient's inbox – rather James Bondesque! Other notable mentions are Posteo, Tutanota, and Hushmail.



Proton Mail



Tutanota[®]



Mailfence

PC AND MAC PATCHING

Patching is the process of applying software updates (patches) that fix flaws, including vulnerabilities. Timely patching of operating systems and software applications such as Microsoft Office, Adobe products, and Quickbooks is necessary since vulnerability lists are publicly available and actively exploited by hackers.

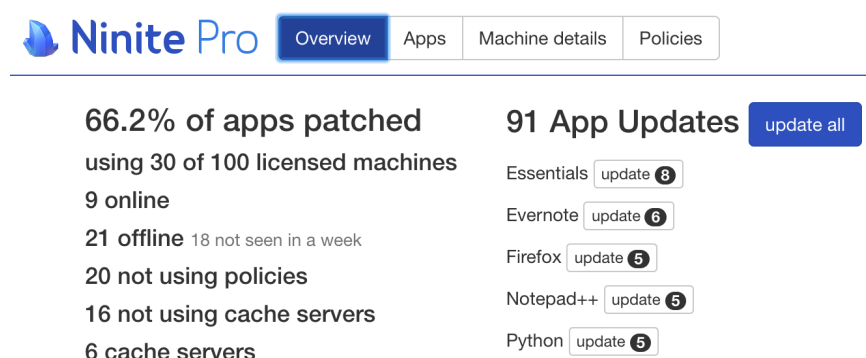
Here's one such list: <https://www.cvedetails.com>

Unfortunately, patching is not an easy process. While Windows and Mac OS download and install patches automatically by default, automation can fail and often does. More problematic are applications, which may never auto-update, creating a doorway for hackers.

The best solution is to consult a trained professional or IT service provider for monitored, systematic patching. If, however, you must do it alone:

WINDOWS PCS:

- Check the Windows update app to ensure you have the latest updates.
- Use a product such as Ninite Pro to update your software applications.

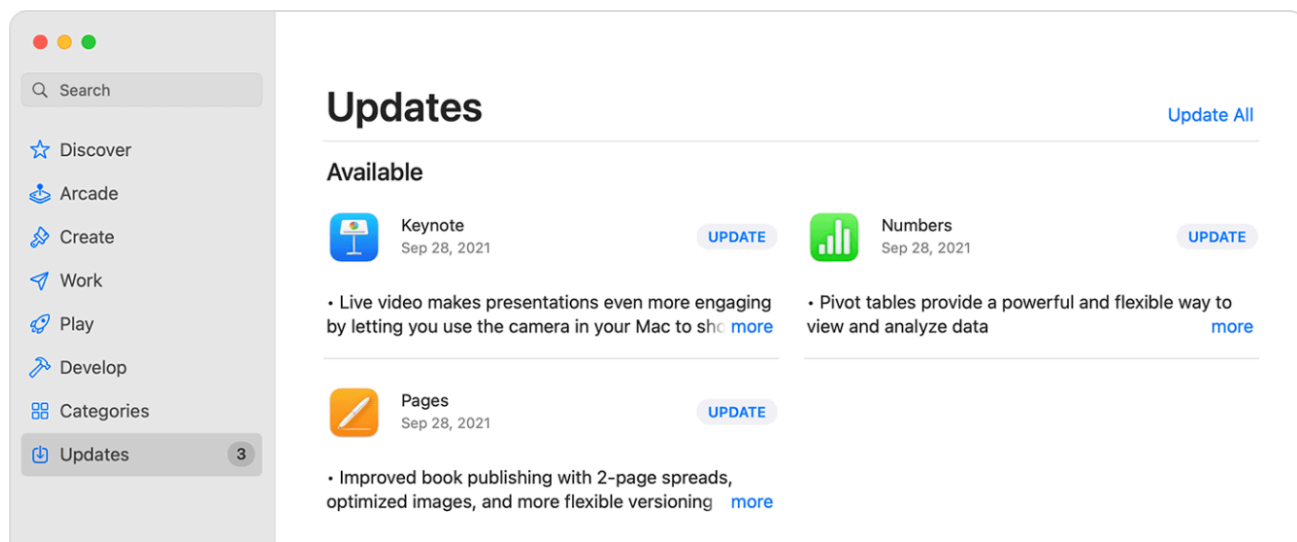


The screenshot shows the Ninite Pro web interface. At the top, there's a navigation bar with 'Overview' (selected), 'Apps', 'Machine details', and 'Policies'. Below this, the 'Overview' section displays machine statistics: 66.2% of apps patched, 30 of 100 licensed machines online, 21 offline (18 not seen in a week), 20 not using policies, 16 not using cache servers, and 6 cache servers. To the right, the '91 App Updates' section features a 'update all' button and a list of applications with their update counts: Essentials (8), Evernote (6), Firefox (5), Notepad++ (5), and Python (5).

Machine Status	App Updates
66.2% of apps patched	91 App Updates
using 30 of 100 licensed machines	
9 online	Essentials update 8
21 offline (18 not seen in a week)	Evernote update 6
20 not using policies	Firefox update 5
16 not using cache servers	Notepad++ update 5
6 cache servers	Python update 5

MACS:

- Check for Mac OS updates frequently, even if you think automation is doing the job.
- Use the App Store app to update software applications.



PC AND MAC

FULL DISK ENCRYPTION

Full Disk Encryption (FDE) is a free feature called "Bitlocker" in Windows and "FileVault" in Mac OS. FDE protects the data on your laptop or desktop computer if it is stolen by attempting to detect tampering. You must have the following ready to go if you activate FDE on your computer:

- 1) Your decryption code or password. This is not the same as the password for logging into your computer. If your computer requests this code and you or your technician do not have it, you're done. You'll have to wipe your computer of all software and data.
- 2) Have a full, recent, reliable backup of your computer so that if item 1 comes true, you can recover. If you have any doubts about what you're doing, you guessed it, consult a trained professional.

BitLocker recovery

Enter the recovery key for this drive

For more information on how to retrieve this key, go to
<http://windows.microsoft.com/recoverykeyfaq> from another PC or mobile device.

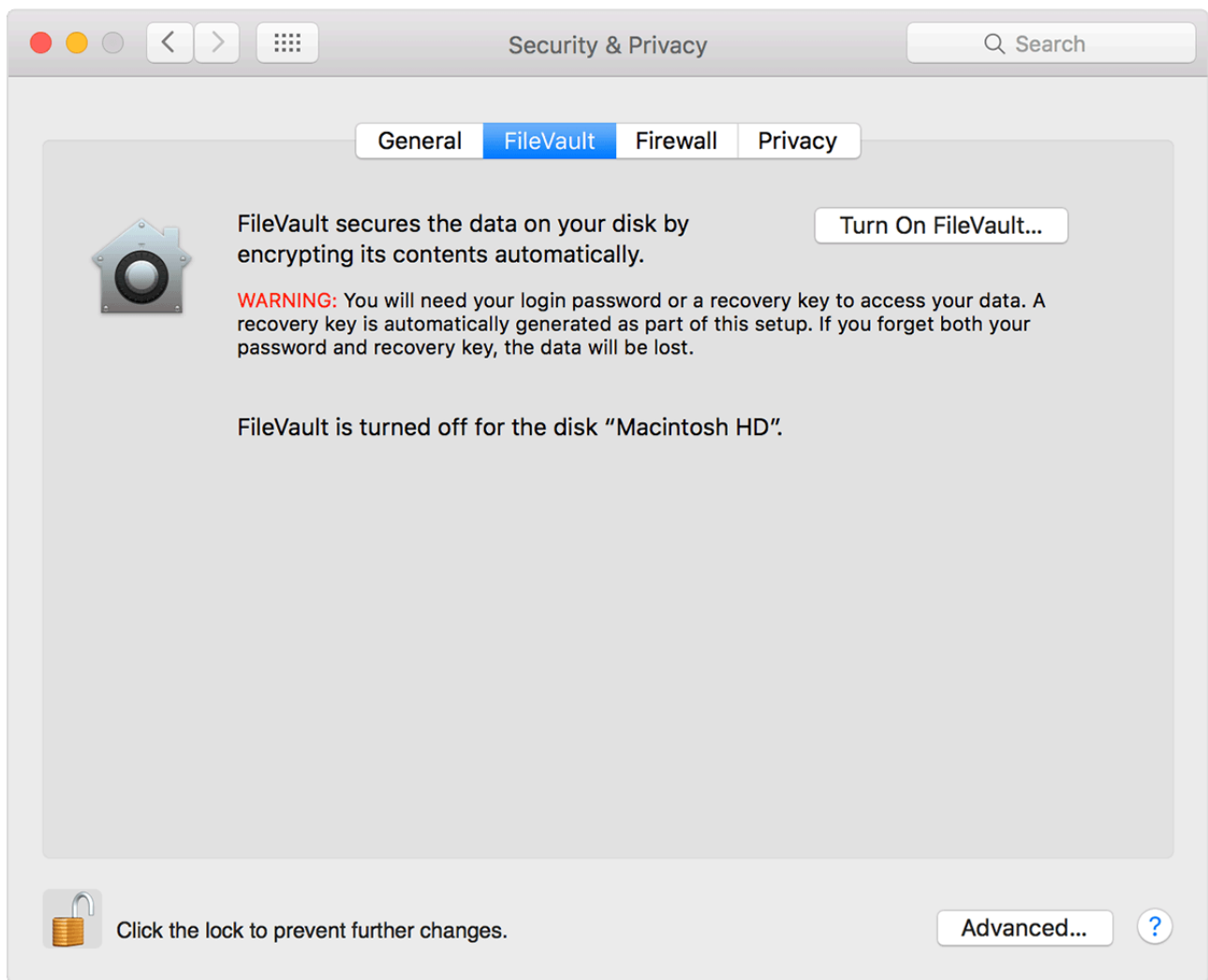
Use the number keys or function keys F1 - F10 (Use F10 for o).

Recovery key ID: 1837F52D-F48C-4d53-B6F5-83D6FCE67625

Press Enter to reboot and try again

Press Esc for BitLocker recovery

Press F11 to choose an alternate operating system





IDENTITY THEFT PROTECTION

In short, identity theft protection is a service that alerts you via phone, email, or text message, if someone is impersonating or attempting to impersonate you.

A good identity theft protection service should cover four areas of security:

CREDIT MONITORING

Credit-monitoring services examine your credit report at one or more of the major credit-reporting services (Equifax, Experian, and TransUnion) and alert you of any activity, whether it's a change of address or a new loan application. Some also track and disclose fluctuations in your credit score.

IDENTITY MONITORING

Identity monitoring services scour public records, such as property and arrest records, social media sites, the dark web, and more, for activity tied to your name, address, or other personal information. Signs of suspicious activity generate an alert to advise you to contact the monitoring services support desk for more details.

IDENTITY THEFT INSURANCE

Identity theft insurance helps a victim recoup the cost of recovering and restoring their identity. This process may include reimbursement of legal fees, phone bills, notary fees, mailing costs, and more.

ID theft insurance is sometimes included as a rider on a homeowners or renters insurance policy. It can be bought as a separate policy or as part of an ID theft protection package. Contact your insurance agency for details.

IDENTITY THEFT RECOVERY

A comprehensive ID theft protection plan will include recovery assistance. You may be assigned a dedicated agent to handle your case who can initiate phone calls, compose emails and run the legwork required to restore your identity. This type of support can save victims a lot of time and stress. Among popular services are Identity Guard, Identity Force, and Aura.



BACKUPS & RECOVERY

While security best practices vastly reduce your risk of being hacked, it can still happen, which is why backup & recovery are the single most crucial part of personal security.

Unfortunately, backing up your information is more than just installing a backup app and hoping for the best. You must ensure you can:

- Recover data successfully.

Periodically test restoration of random files and folders to ensure data is backed up properly and is recoverable.

- Recover data in a reasonable amount of time. (Recovery Time Objective)

How long would it take to restore all of your files or set up a new computer if yours is lost, stolen, or badly damaged?

- Recovery data of the required age. (Recovery Point Objective)

Do you need a version of your data from yesterday or six months ago? You'll need a backup app or service capable of archiving the required history.

For maximum privacy and security in cloud backup services, look for zeroknowledge encryption, which means not even the provider of backup services can see your data. Such providers include CrashPlan and iDrive.



Acronis



GOOD HABITS

The most critical element in cybersecurity is not hardware, software, or subscriptions but us. That's right—you and me. Human actions can counteract any technology-based protection. It's impossible to predict all the human reactions that may lead to a cybersecurity breach, but one root cause seems to be present in all of them, and that's a rush to action instead of pausing to evaluate the situation appropriately.

Sources:

<https://www.bankrate.com>

<https://usa.kaspersky.com>

<https://medium.com>

Contact Us



(970) 372-4940



155 Boardwalk Dr #400, Fort Collins, CO 80525



info@TechFramework.com