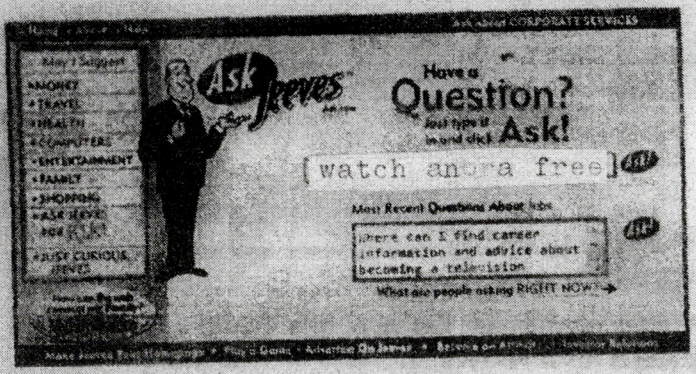
Staying Safe

on the Information Superhighway

Nathan Powell

Contents



Introduction

The information superhighway, or "Inter-Net", is a global network of computers for file-sharing and other communications. It is the public-facing successor to the U.S. Department of Defense's ARPANET, which facilitated the rapid sharing of information for defence contractors and academics. The Internet is not a single platform, but rather, a series of discrete services and "pages" that construct a global community.

My earliest memory of the internet is using my family's Compaq Presario, a PC running Windows 95 with a dial-up connection. At the time, a computer lived in its own room, separate from our daily lives. The only websites I knew about were the official Lego page and some Zelda fan art sites. Though the internet felt like a relatively frivolous platform, these early websites would often contain malicious files and other hazards. A common expression was "don't download anything".

The modern web bears little resemblance to the email forwards, Flash games, and BBSs of yesteryear. For one thing, we can never fully "log off". The internet is a daily necessity in modern life, required for job-hunting, education, healthcare, and hamburger delivery apps. Our lives are increasingly lived "online", and thus, the stakes of digital security are higher than ever.

Though modern PCs and smartphones are relatively well-equipped to prevent basic malware attacks, there are newer concerns related to social engineering: doxing, online harassment, phishing, surveillance, and others. I can confidently say that the internet is far more dangerous place than it was for a young Nathan playing Lego games in the late-90's.

In writing this zine, my desire is to produce a document that will someday become obsolete, once lawmakers and tech companies address the structural issues that cause harm to the world's most vulnerable populations. Unfortunately, that day feels very far away, though I remain hopeful that a better world is always possible. Until then, let's look out for each other. Stay safe out there.

-Nathan Powell, McMaster University, 2025
MA Program in Communication and New Media

Key Terms and Definitions

Data Autonomy

Data Autonomy refers to a user's control and ownership of their data. The myriad web platforms available today have radically different approaches in this regard: Amazon, for example, operates a web portal for law enforcement to download audio/video recordings from inside users' homes [1]. In asserting your data autonomy, it is important to consider the specific practices of any companies storing your data.

Cloud Storage

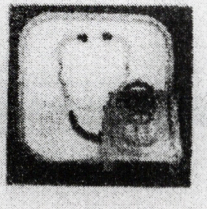
A growing number of consumer-facing technology products incorporate "cloud" functionality in some way. This offers several benefits, as your data is theoretically safe from localized disasters, like flooding or hard drive crashes. It also enables users to access their files from any geographical location.

As a marketing metaphor, "cloud" implies an immaterial, distant object that hovers in the sky. However, these cloud services exist in physical locations, often spreading user data across multiple continents to save a few bucks. The cloud is just someone else's computer[2], with data stored on the same 3.5" hard drives as a standard PC.

Safety

This zine aims to instruct you, the reader, on the best available practices for managing one's files and information. However, the dangers of hacking and social engineering are becoming more sophisticated every day, and there is no guaranteed method of staying safe online. As well, it is occasionally outside of your own control. If your co-worker falls victim to a phishing scam, for example, this might compromise your data in addition to theirs. Even the most cautious among us are susceptible to data breaches.

File Encryption FAQ



"What does file encryption *do*?"

Encryption takes ordinary, readable information and converts it to gibberish[3]. This conversion requires the use of an *encryption key*, a password that allows users to both encrypt and decrypt (ie. recover) the data. Much like your internet accounts have passwords, file encryption allows users to "log in" to access private data, such as documents and images.

"Isn't this just for hackers and criminals?"

Encryption is completely legal, and is currently used in many aspects of everyday life. For example, Blu Ray Discs and Netflix streams both use encryption to ensure that media is only viewed with approved hardware, so you can't watch *Anchorman 2* without using encryption in some way[4]

The social connotations of encryption are perhaps unwarranted, but worth considering. People on the bus might look at you weird if you start talking about 256-bit encryption keys. Someone might offer you a tin-foil hat. However, if you're reading this guide, then you probably have a general feeling that privacy is important.

"But what if I live in a *good country* and I trust the government?"

You don't, and you shouldn't! Nation states change their laws constantly, and this is particularly dangerous for marginalized groups within society. As well, there are other groups who may wish to access your data for malicious reasons, such as harassment and stalking.

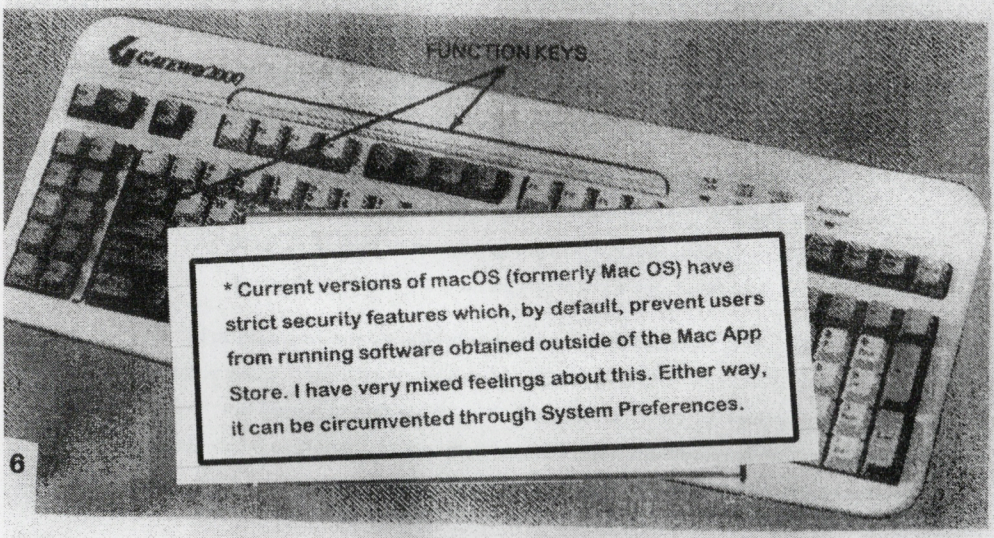
If your laptop has unencrypted data, then your information is accessible to anyone with a screwdriver and some patience. Even under the most "normal" circumstances, a PC might contain scanned tax documents or employment contracts, which contain sensitive information. Keeping your files safe is *always* a worthwhile endeavour.

Comparison of Operating Systems

The available operating systems vary wildly in their security features, and as a result, no individual OS is "the safest". In the chart below, I have compiled some of the OS-specific features as they relate to the topics of this guide.

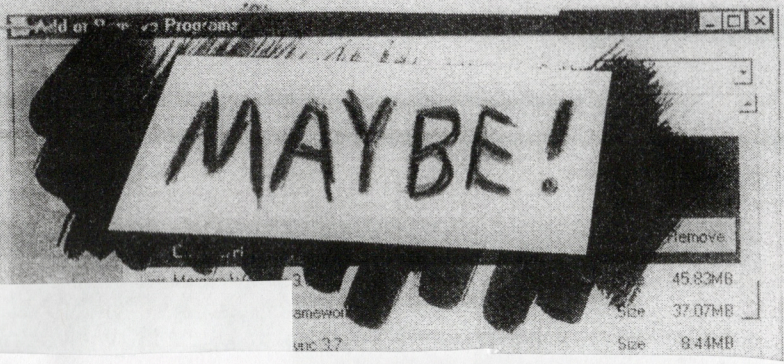
Also, while I have your attention, I must point out the horrible choice by Microsoft to paywall their encryption functionality in Windows 10 and 11. It's an unfathomably bad move.

	Windows 10/11	macOS	iOS/iPadOS	Android	Chrome OS
Built-in virus scanner	✓				
Built-in file encryption	Paid Upgrade	✓	✓		
Law-enforcement backdoor	✓				
Runs third-party software	✓	*	App Store only	✓	App Store only
External disk sync/backups	✓	✓			



* Current versions of macOS (formerly Mac OS) have strict security features which, by default, prevent users from running software obtained outside of the Mac App Store. I have very mixed feelings about this. Either way, it can be circumvented through System Preferences.

Should You Use a Virus Scanner?



Windows 10/11

- All modern Windows systems include Windows Defender, a free antivirus suite maintained by Microsoft, which earned a "nearly perfect rating" [5] from the AV-Test Institute in 2019.
- Microsoft has been commended by security researchers for their fast response to reported bugs and exploits. [6]
- However, Windows has greater compatibility with legacy software (relative to macOS), which potentially makes modern PCs susceptible to decades-old vulnerabilities. [7]

macOS

- Throughout the 2000's and early 2010's, Apple claimed that their computers "don't get PC viruses" [8].
- They dropped this claim in 2012, following an increase in Mac-specific malware and the vulnerabilities of Bootcamp partitions (ie. Windows on Mac). [8]
- Following the release of macOS Catalina (2009), Apple increased their restrictions on third-party software, requiring apps to sandbox their access to OS permissions and files [7].
- Modern macOS installations run a daily check for malicious software, using Apple's "XProtect" database [9].

Mobile (Android/iOS/iPadOS)

- Due to the sandboxed nature of Apple's mobile platforms, there is no practical method for third-party antivirus apps to scan for malware.
- Wired has called Android AV apps "garbage", due to the influx of fake antivirus software on the Google Play store [10].
- The best defence against mobile viruses is to keep your software up-to-date, as annoying as that sounds.

Conclusion:

Modern versions of both Windows and macOS offer sufficient built-in protections against malware. However, it is always possible for users to manually install trojans and other bad software. Do a quick Google search before installing any mysterious apps.

Ad Blocking

Some of the advice in this guide is situational, such as the use of a VPN. Other subjects, however, are more clear-cut, such as the potential threat of scams in online advertising.

Use an ad blocker. Always, always, always.

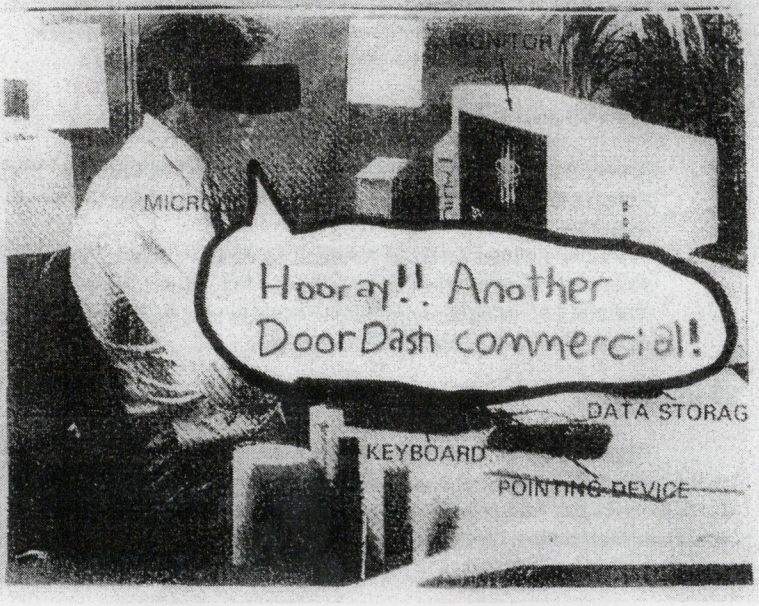
I don't care if this means your favourite YouTuber loses out on ad revenue. In my experience, you get around 0.7 cents per view anyway. This is a small price to pay for extra security, considering the risks.

The FBI recommends it. Really.

You won't often see me enthusiastically quote a state surveillance body, particularly an American one, but here we are anyway. In 2022, the FBI encouraged the use of ad blockers in avoiding scams and other malicious search results [11]. For example, some groups will advertise trojan software using sponsored search placement, which means actual viruses can show up when a user is looking for legitimate software.

Some ad blockers are sketchy.

In the past few years, we've seen several ad blocking programs fall into malicious hands, such as tracking/surveillance companies. Do some research before installing a browser extension. Personally, I only ever recommend *uBlock Origin*. It's the ad blocker so good, Google keeps trying to shut it down [12].



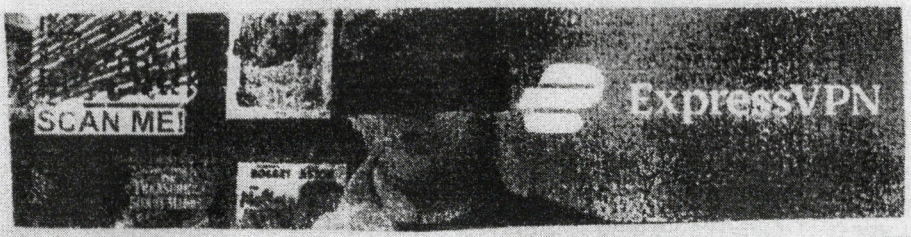
Select Settings

- [x] Endpoint
- [ ] Midpoint
- [x] Center
- [ ] Node
- [ ] Quadrant
- [ ] Intersection

Should You Use a VPN?

Not necessarily! VPNs route your internet traffic through a separate location, which disguises your IP address from websites and other applications that might track such things. This could be used to disguise risky political discussions from the prying eyes of nation-states and surveillance. However, a VPN service could record your browsing data just as easily as an ISP or government agency.

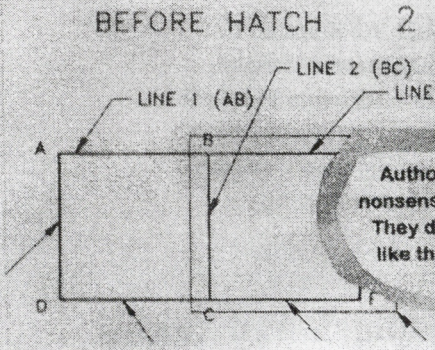
Be wary of VPN services that invest heavily in sponsored content and influencers!



There are several activities that warrant the use of a VPN:

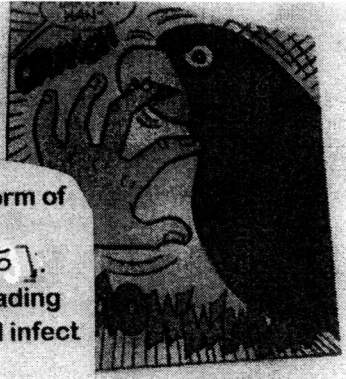
- Hide web activity from ISP and law enforcement
- Piracy! Downloading copywritten movies, television shows, and software.
- Accessing the American library of Netflix content in another country, like Canada.

Based on an external audit by Deloitte, Private Internet Access does not keep logs of user activity [13] This protects users from potential subpoenas from government agencies. According to Wired, ProtonVPN does not keep logs either [14]



Author's note: *Private Internet Access* is a no-nonsense VPN, and my personal recommendation. They don't have promotional pricing or anything like that, so you aren't as likely to end up with a surprise credit card charge.

Malware Overview



Trojans

Likely the most commonly-understood form of malware, trojan horses ("trojans") are standard computer programs that run malicious tasks [15]. Trojans may disguise themselves through misleading file names, such as "linkin_park_numb.exe", and infect the host computer upon running.

Best defence: don't run any executable software without verifying its source, such as the website from which it was downloaded. Do a quick Google search of the file name before opening.

Viruses

Viruses are malicious computer code which infect legitimate software on the host machine. This form of malware spreads through MP3 files, images, and other documents [15] Unlike trojans, viruses cannot run on their own.

Best defence: keep your software up to date. Modern productivity software and media players have built-in safeguards against infected files, with their databases regularly updated to include new threats.

Worms

As the name suggests, worms are slightly more animated than other forms of malware! Worms will infect new computers by scanning local networks in search of vulnerable machines [15]

Best defence: be mindful of the devices on your network. All it takes is one outdated machine, such as a legacy PC running older software, to infect a whole network. Other risky devices include low-cost "IPTV" boxes, particularly those sold under obscure brand names for the purposes of media piracy.

Historical Malware Examples

MyDoom (2004)

As the fastest-spreading virus of 2004, MyDoom infected machines through malicious email attachments and Kazaa downloads. [16] MyDoom's network of infected computers launched a DDoS attack on SCO, which brought their website offline for multiple weeks [16].

Stuxnet (2010)

Though most viruses target as many computers as possible [17], Stuxnet had a very precise goal: damaging the Natanz nuclear facility in Iran [18]. This malicious code marks the first major state-sponsored malware attack against another nation [18]. It is estimated that up to 100,000 computers may have been infected by Stuxnet at some point [17].

CryptoLocker (2014)

CryptoLocker was the first major case of "ransomware", a virus which encrypts files and documents on target machines before demanding money for the recovery key. Thankfully, the original group behind CryptoLocker was shut down by cybersecurity firms, with the 500,000 keys made public [19]. However, ransomware remains a concern in daily life, as the City of Hamilton faced a ransomware attack in 2024, causing over $7.4 million in damage [20].

Dangerous PDFs

I hate to be an alarmist, but there is much to be alarmed about, and I spend most of my days feeling a little bit scared. The frightening new malware exploit of our time, and the one that has caused issues for even the most tech-focused among us [2]], is "session hijacking".

Put simply: a malicious PDF or application can steal your browser cookies, which allows hackers to access your internet accounts and bypass usernames, passwords, and two-factor authentication (!). These attacks have become more visible in recent years [2!], and are difficult for web companies to detect and prevent.

What can you do?

1. Don't click on any strange links
2. Screen all URLs before opening

Don't scan random QR codes! They could literally send your phone to **any website**.

Be careful when typing URLs

Malicious emails, like those containing session-hijacking scams and dangerous PDFs, often contain salacious subject lines like "is this you?" and "i remember you, do you remember me?". They prey upon the reader's sense of curiosity.

Personally, I'm relatively immune to such appeals, as I have zero interest in being contacted. Hackers beware: I simply cannot be bothered. The Powell method is, thus far, undefeated.

How Safe is Cloud Storage?

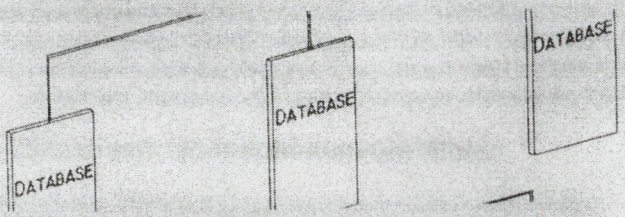
Cloud storage is an appealing proposition: a user's files are safe from local disasters like hard-drive crashes and home flooding, and companies like Backblaze offer "unlimited" storage plans for low monthly fees [22]. However, "the cloud" is a nebulous and immaterial metaphor for what is, more accurately, a series of high-performance computers located in server farms around the world [23]. Here are some general considerations regarding cloud storage.

Account Deletion

Internet accounts are terminated/deleted every day, and for a host of reasons. Some platforms auto-delete accounts after a period of inactivity. Some platforms are just evil; Apple once terminated the developer account of a game dev who criticized Apple at a public event [24].

Service Changes

If you store all your personal files on the cloud, there's always the risk of a particular platform changing their pricing model. This was the case with Google Photos, who lured in users with free, unlimited photo storage [25], only to reverse that decision once their competitors went out of business. Be cautious of cloud storage plans that are simply *too good to be true*.



The CLOUD Act (and Canada)

The CLOUD Act is an American federal law, enacted in 2018, that allows the American government to subpoena the data of U.S.-based companies, regardless of server locations. This mainly evolved from a dispute between Microsoft Ireland and the U.S. government [26].

Canadian citizens should be greatly concerned about this legislation, given the presence of American technology companies in Canada, and our general reliance on American corporations. Companies like Apple, Microsoft, Alphabet, and Shopify, among many others, are legally required to give their data to U.S. government agencies upon request.

Basically: the U.S. government can access the data of any technology company that does any business within the United States. The FBI could download your doorbell camera videos! Be very, very careful about the data you share with these companies!

Password Management

Creating secure, complex passwords is an important aspect of digital safety. You're probably familiar with "password meters", the helpful graphics through which websites tells you if a password is sufficiently complex. However, these meters have unfortunately led to predictable patterns, wherein users often place capital letters at the start of a password and add symbols onto the end [27]

Instead, I would argue that dedicated password managers are far better suited to generating secure passwords, as they produce totally arbitrary sequences of numbers, letters, and other symbols. Here are some examples of local software and online services for managing account passwords:

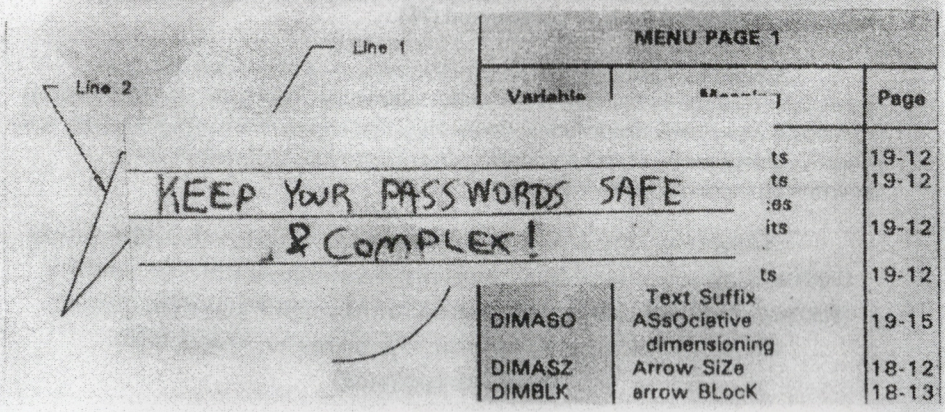
Bitwarden **Dashlane** **1Password** **KeePassXC**

App/Online Recommendation: 1Password

1Password allows users to generate complex account passwords, then synchronize them across multiple devices. They also keep track of which sites have experienced data breaches and will notify users accordingly. The service costs $5 CAD for a basic, monthly plan, which is slightly higher than some competing services. However, their advanced client-side encryption makes for a compelling product.

Local Recommendation: KeePassXC

Rather than syncing your passwords through a dedicated online service, which often requires monthly subscription fees and significant trust in third-party servers, KeePass is fully offline. It's free and open source software, and the password database is stored locally, as a database file [28]. You can even sync the database with your other devices through existing cloud-storage options, if that's your jam.

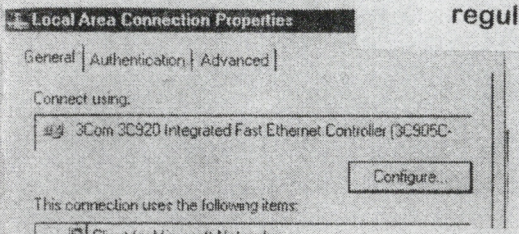


Local Network Safety

By default, computers will communicate with one another on local networks. If you have a compromised machine that connects with the same router as everything else, it can cause issues for the entire network. Issues of ransomware, worms, and data leaks abound. Here are some simple prevention strategies.

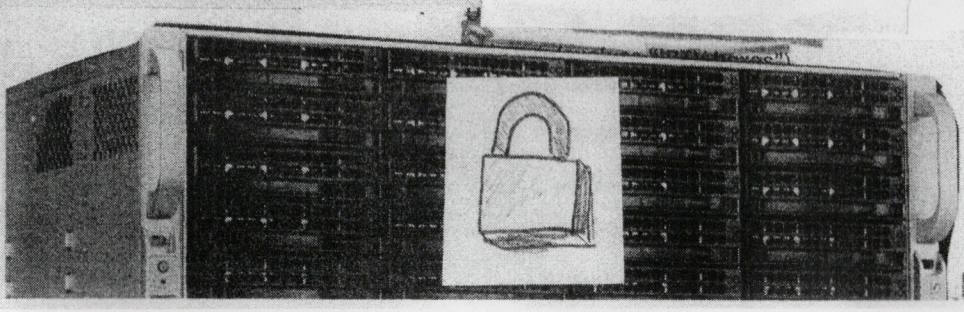
Do:

- Keep all devices up-to-date
- Set complex login passwords on all machines
- Use a VPN for any torrents, legal or otherwise
- Update your Wi-Fi password on a regular basis, make it complex

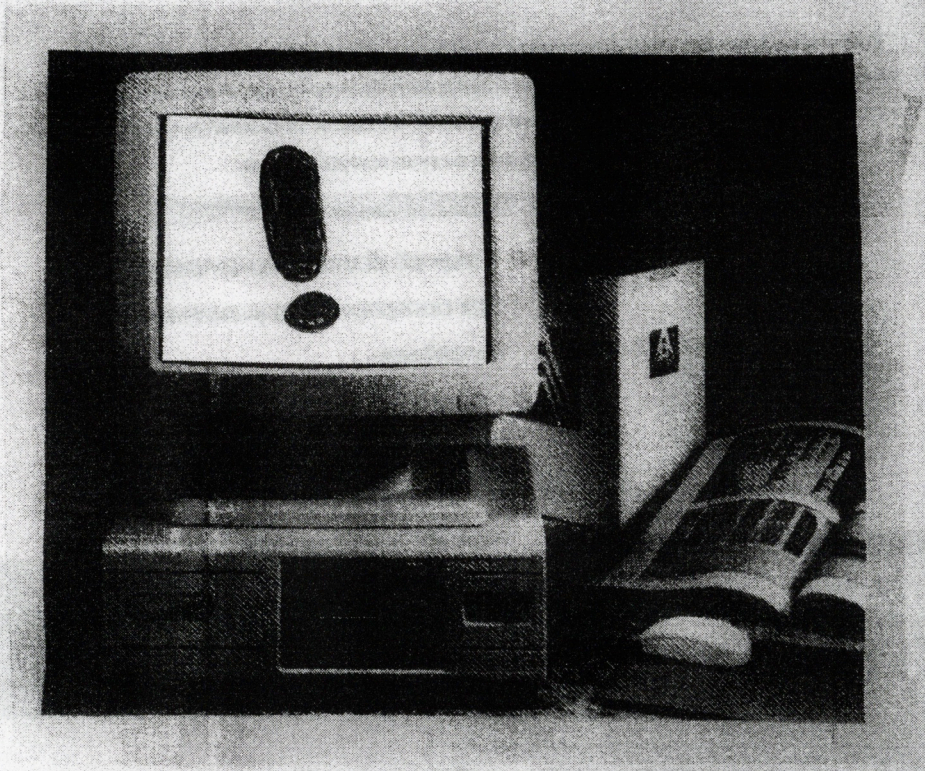


Don't:

- Add your entire hard drive to the local network share
- Use questionably-sourced devices on your network (such as "IPTV boxes")
- Plug a "legacy" machine into the same router as everything else



Limitations of Security



Ideally, this guide has outlined several important concepts in data security, online privacy, and everyday computing.

It is my hope that readers of this zine will consider adding password managers and VPNs to their regular lineup of software. However, since this guide provides general-purpose advice for those with an existing familiarity with personal computing, these overall "best practices" will not suffice in extreme cases of harassment and doxxing.

Complex fonts

The quick brown fo

The quick brown fo

The quick brown fox jum

Τηε ψυιχκ βροων φο

Уэд рфивк бсощн е

the next big cyberattack will be even harder to crack.

AbB123

Limitations of Security

Pierce et al. coined the term "differential vulnerabilities" in discussing the effectiveness of cybersecurity toolkits, such as this one [29]. Basically: we are not all equally vulnerable to the dangers of the modern web. As Zoe Quinn discusses in *Crash Override,* even the most technically proficient among us can be victimized by structural issues of the modern web [30]. Online harassment is only exacerbated by the intersection of marginalized identities, such as gender, sexuality, race, and disability [21].

In discussing this zine's issues of safety on the modern web, we must be careful not to overemphasize the effectiveness of individual software tools or browsing habits. The Internet is a dangerous place, and all the world's social ills exist here in some form. The previous sections provide important recommendations for staying safe(ish) on the information superhighway, but they are not guaranteed. As a result, one should not feel ashamed (or at fault) when their data is compromised, whether by old-school hacking or social engineering.

Additional Reading

Tyson, J. (2001, April 6). How Encryption Works. *Howstuffworks.*

https://computer.howstuffworks.com/encryption.htm/printable

In this detailed article, Tyson explains the mechanics of online encryption, including SSL, hashing, and checksums. This article links cryptography back to its earliest recorded days in analogue communications, including ancient Spartan battles. It's important to remember that encryption is not a *new* feature in the information age, particularly when encryption-based software is challenged by government agencies.

Why I'm Having Second Thoughts About The Wisdom Of The Cloud. (2011, January 10). *TechCrunch.* https://techcrunch.com/2011/01/10/why-im-having-second-thoughts-about-the-wisdom-of-the-cloud/

This article dates back to the earliest days of "cloud" discourse, at a time when Google Wave was still operational. The (unnamed) author notes several concerns relating to cloud computing that remain relevant today: government surveillance, unreliable syncing between devices (iOS still doesn't have a "sync" button), and the high stakes of storing tax/banking information online.

Works Cited

[1] Whittaker, Z. (2020, September 27). This is how police request customer data from Amazon. *TechCrunch*. https://techcrunch.com/2020/09/27/this-is-how-police-request-customer-data-from-amazon/

[2] Brock, D. C. (2017, August 31). Someone Else's Computer: The Prehistory of Cloud Computing. *IEEE Spectrum*. https://spectrum.ieee.org/someone-elses-computer-the-prehistory-of-cloud-computing

[3] Loshin, Pete. (2013). Preface. What Is This?. In *Simple steps to data encryption: A practical guide to secure computing* (1st edition). Syngress.

[4] Lee, K. (2012). Researchers crack Blu-ray encryption. In *PC world* (Vol. 30, Number 2, pp. 38-). IDG Communications, Inc.

[5] Top scoring in industry tests. (2024, April 24). *Microsoft Learn*. https://learn.microsoft.com/en-us/defender-xdr/top-scoring-industry-tests

[6] Baraniuk, C. (2017, May 9). Microsoft makes emergency security fix. *BBC News*. https://www.bbc.com/news/technology-39856391

[7] Purdy, K., & Klosowski, T. (2020, April 21). You Don't Need to Buy Antivirus Software. *NYT Wirecutter*. https://www.nytimes.com/wirecutter/blog/best-antivirus/

[8] McMillan, R. (2012, June 26). Apple quietly drops its claims that its computers don't get viruses. *Wired*. https://www.wired.com/story/macs-get-viruses/

[9] *Protecting against malware in macOS*. (2024, December 19). https://support.apple.com/en-ca/guide/security/sec469d47bd8/web

[10] Barrett, B. (2019, March 16). Most Android Antivirus Apps Are Garbage. *Wired*. https://www.wired.com/story/android-antivirus-apps-bad-fake/

[11] Kan, M. (2022, December 22). FBI Recommends Installing An Ad Blocker To Dodge Scammers. *PC Mag*. https://www.pcmag.com/news/fbi-recommends-installing-an-ad-blocker-to-dodge-scammers

[12] Yee, A. (2025, February 25). uBlock Origin is officially dead for Chrome, but ad blockers live on. *PCWorld*. https://www.pcworld.com/article/2595287/ublock-origin-is-officially-dead-for-chrome-but-ad-blockers-live-on.html

[13] Singleton, S. (2024, September 11). Private Internet Access: A lowprice, high-value VPN for everyone. In *PC world* (pp. 48–53). Foundry. https://www.pcworld.com/article/403379/private-internet-access-vpn-review-4.html

[14] Gilbertson, S. (2025, January 14). The Best VPNs to Protect Yourself Online. *Wired*. https://www.wired.com/story/best-vpn/

[15] Brain, M., & Fenlon, W. (n.d.). How Computer Viruses Work. *Howstuffworks*. https://computer.howstuffworks.com/virus.htm

[16] MyDoom shakes SCO with DDoS attack. (2004). *Computer Fraud & Security*, *2004*(2), 1–1. https://doi.org/10.1016/S1361-3723(04)00022-3

[17] Chen, T. M., & Abu-Nimeh, S. (2011). Lessons from Stuxnet. *Computer (Long Beach, Calif.)*, *44*(4), 91–93.

[18]Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, *22*(3), 365–404.

Works Cited 2

[19] Ward, M. (2014, August 6). Cryptolocker victims to get files back for free. *BBC News.* https://www.bbc.com/news/technology-28661463

[20] Peesker, S. (2024, August 16). Cyberattack has cost Hamilton $7.4M so far, says city. *CBC News.* https://www.cbc.ca/news/canada/hamilton/hamilton-cyberattack-cost-1.7296868

[21] Peters, J. (2023, March 24). How hackers took over Linus Tech Tips. *The Verge.* https://www.theverge.com/2023/3/24/23654996/linus-tech-tips-channel-hack-session-token-elon-musk-crypto-scam

[22] Personal Computer Backup. (n.d.). *Backblaze.* https://www.backblaze.com/cloud-backup/personal

[23] Monserrate, S. G. (2022). The cloud is material: On the environmental impacts of computation and data storage. *MIT Case Studies in Social and Ethical Responsibilities of Computing.* https://doi.org/10.21428/2c646de5.031d4553.

[24] Totilo, S. (n.d.). Apple Bans Game, Days After Developer Publicly Trashes App Store. *Kotaku.* https://kotaku.com/apple-bans-game-days-after-developer-publicly-trashes-5497459

[25] Bohn, D. (2020, November 11). Google Photos will end its free unlimited storage on June 1st, 2021. *The Verge.* https://www.theverge.com/2020/11/11/21560810/google-photos-unlimited-cap-free-uploads-15gb-ending

[26] Brier, T. F. (2017). Defining the Limits of Governmental Access to Personal Data Stored in the Cloud: An Analysis and Critique of Microsoft Ireland. *Journal of Information Policy (University Park, Pa.), 7,* 327–371. https://doi.org/10.5325/jinfopoli.7.2017.0327

[27] Paudel, R., & Al-Ameen, M. N. (2025). "It's Definitely New and Different...It's Really Engaging": Understanding the Power of Storytelling Towards Secure Password Creation. *International Journal of Human-Computer Interaction,* 1–21.

[28] Gilbertson, S. (2025, March 26). The Best Password Managers to Secure Your Digital Life. *Wired.* https://www.wired.com/story/best-password-managers/

[29] Pierce, J., Fox, S., Merrill, N., & Wong, R. (2018). Differential Vulnerabilities and a diversity of Tactics: What Toolkits Teach Us about Cybersecurity. *Proceedings of the ACM on Human-Computer Interaction, 2,* 1–24. https://doi.org/10.1145/3274408

[30] Quinn, Z. (2017). *Crash override : how Gamergate (nearly) destroyed my life, and how we can win the fight against online hate* (First edition.). PublicAffairs.

Quick Reference Guide

Should I purchase a virus scanner?

Nope. Windows Defender is free, and macOS scanners are basically snake oil.

Which VPN should I use?

Proton or *Private Internet Access*, since neither company keeps logs of user data.

Are ad blockers unethical?

They're essential for safe web browsing, according to the FBI [1].
Use *uBlock Origin*.

Do I need a password manager?

They're a good idea, especially with the dozens (hundreds?) of websites you might use on a regular basis.

What's the best computer?

It's a tie between the 2001 iMac G3 (Indigo), and the Commodore 64.

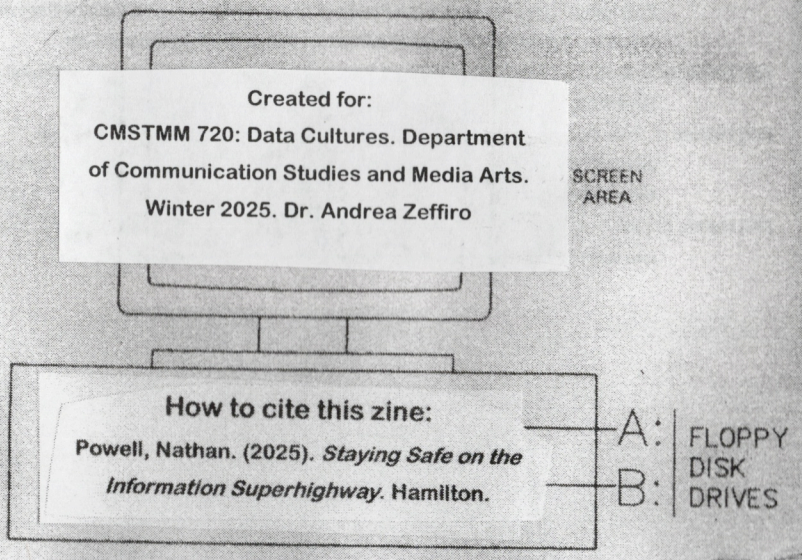


Fig. 2-1. Disk drive arrangements and their DOS names.