Be Internet-Smart

A Privacy and Security Guide

of Best Practices

2020

Adam Greenberg
hello@AdamGreenberg.com

THIS PAGE INTENTIONALLY LEFT BLANK
(EXCEPT FOR THAT… AND THIS.)

Contents

INTRODUCTION **4**

PROBLEMS AND EASY SOLUTIONS **4**

Public Computers 4
Shared-Computer Etiquette *4*
Internet Browsers *5*
Unsecure Networks 8
Unsecure Passwords 9
Password Managers *9*
Two-Factor Authentication *11*
Settings 13
Mobile *14*
People 14
Physical Security *15*
Financial Security *15*

RECOMMENDATIONS **16**

Worthwhile (and Free) Apps and Services 16
- *LastPass – Password Manager* *16*
- *Authy – Two-Factor Authentication* *16*
- *ProtonMail – Secure Email Service* *16*
- *ProtonVPN – Virtual Private Network* *16*
- *Brave – Internet Browser* *16*
- *HTTPS Everywhere – Browser Extension* *16*
- *Ghostery – Browser Extension* *16*
- *DuckDuckGo – Search Engine, Browser Extension, and App* *16*
- *FindMyDevice – If lost, this is one Google app you could be glad you had* *16*
- *Malware Bytes – AntiVirus Software* *16*
- *CCleaner – Computer Cleaning Defragmenting Software* *16*

Helpful Websites 17
- *HaveIBeenPwned.com* *17*
- *EquifaxBreachSettlement.com* *17*
- *SpreadPrivacy.com/tag/device-privacy-tips* *17*
- *Panopticlick.eff.org* *17*
- *TOSdr.org* *17*
- *myActivity.Google.com* *17*
- *Switching.Social* *17*

CONCLUSION **18**

ACKNOWLEDGEMENTS **18**

INTRODUCTION

This concise and practical guide points out oft-overlooked problems regarding Internet privacy and security, AND offers ***easy-to-implement, secure, and free solutions.***

Initially, I created this guide as part of a larger conversation that – ideally – would be happening throughout all government departments and federal agencies. Actually, I created this guide specifically pertaining to Peace Corps volunteers and staff abroad, but I now see it as relevant to nearly any company, organization, entrepreneur, or family too. It is an inventory and personal assessment of Internet behavior that any individual can use to be more secure across the web on both a mobile phone and a computer.

Here, I have adapted it from its original form for you, so if a section doesn't quite seem relevant to you, jump around, of course. It's short and I hope you find it useful.

No incentive has been made to the author in recommending any of the following applications.

PROBLEMS AND EASY SOLUTIONS

A few of the following topics are quick fixes from a macro or company Admin perspective. But ultimately, the responsibility of all of this can fall only on you, dear Reader. Let's jump in.

Public Computers

Shared-Computer Etiquette

Keep the Desktop Clean

The Tragedy of the Commons dictates that public computers have a way of becoming a cluttered mess of forgotten documents strewn across the Desktop. This is just an unpleasant thing to be greeted with upon logging in. It's sloppy, it looks terrible; we're better than that.

Save all your files to one dedicated, personal, organized folder and keep the Desktop clean.

Everyone else thanks you.

Deleting Files

Our office computers previously had nearly a thousand documents (many surprisingly sensitive) just hanging out in the Recycling Bin.

> Don't forget to empty the Recycling Bin.
> *Because you haven't actually deleted anything.*

Internet Browsers

Saving Passwords by Default

By default, Internet Browsers save passwords automatically.

Intended to be convenient, sure; *but* what happens when individuals (or family members) share the same computer – and more specifically, the same login?

(Not often really a problem at companies. And ideally, not within families either.
But between teenage siblings? Who are we kidding?!)

…Well, the potential issue is completely obvious. And completely avoidable.

With even only the very password used to log in to the computer itself, anyone can see ALL the passwords and personal information – saved by default – from any website by any other user of that computer in the 'Passwords' settings page of your Browser (Google Chrome?).

*In particular, that usually inevitably includes *email* logins (and thus also, personal cloud storage access, private photos, and yes, sometimes even financial information).

All just waiting for the next unscrupulous person.

> EASY SOLUTION:
> **Change Your Internet Browser's Default Password-Saving Setting to OFF**

(And delete currently saved login information.)

Your Choice of Browser

While we're on the subject, and perhaps before you go changing only this default password setting in Google Chrome (the preferred browser of most; maybe you too?), you might first consider switching to another Internet Browser altogether.

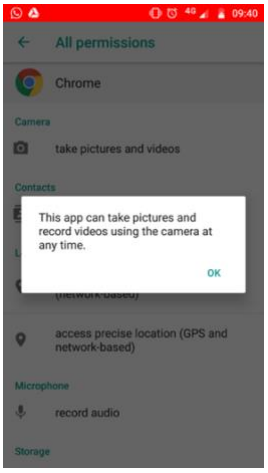
While it is convenient to connect one's Internet life to one service provider (same email address, same browser company, same search engine, *I get it*), Google Chrome often drastically slows down a computer's performance speed by consuming a lot of RAM – significantly moreso than other browsers, actually. See for yourself by looking at the Memory usage in **Activity Monitor** on Mac (or CTRL-Alt-Del -> **Task Manager** on PC)

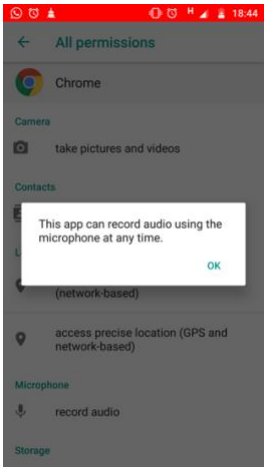
At least Google Chrome *is* more secure than Internet Explorer.
Please don't tell me you're still using Internet Explorer.
(Actually, if you are, do tell me; that's hilarious: hello@AdamGreenberg.com.)

But perhaps the more egregious violation is that Google Chrome also tracks absolutely everything you do across the Internet.

After all, Google's money does come from showing you personalized ads. (And yes, we could even say personalized ads might be preferable to the alternative. Who wants *irrelevant* ads? Again, I agree.)

But Google's privacy issues go further than just tracking for the purpose of targeting ads. As just one example, here are two screenshots found deep within the Google Chrome settings on my phone (before I deleted the app):





To be fair, these issues aren't limited to Google.

RECOMMENDATION: **Brave** www.Brave.com

Maybe consider giving **Brave** a try?

Its clean, minimalist interface and quick load time will not disappoint, while making your security and privacy its priority.

To beef up the security of your current Internet Browser, consider downloading the free extensions, **Ghostery** and **HTTPS Everywhere**. (Brave includes HTTPS Everywhere already.)

www.Ghostery.com

www.eff.org/https-everywhere

*Also, before you replace your current browser, don't forget to export your bookmarks so you can import them into another.

*And do first still manually delete all those saved passwords anyway.

Incognito Mode

Don't Browse Confused.

Incognito mode is not *private* browsing.
Incognito mode also does not make your browsing more secure.

Incognito mode only deletes your local search and browsing history – that is, just the URLs.

Websites, search engines, Internet service providers, and governments can still continue to easily track you, **as they do**.

Through your IP address and Cookies.

IP address – Your device's unique address on the Internet.

Cookies – Not to be had with a glass of milk, these cookies are bits of code that websites automatically install on your computer any time you visit most *(read: all)* websites. Arguably, some may be useful like remembering your login username (though this *is* a less secure practice), while other cookies only benefit the website in their desire to identify you and consistently track your browsing with ads all across the Internet.

It's not just ads however; many websites sell your information to third-parties.

Remember when you just clicked "I Agree" on … everything? Yea, that's it.

(And on that note, check out TOSdr.org for summaries of the rights we've given up across most services.)

Thus, this information forms what becomes your browser *fingerprint*. And believe it or not, in all likelihood, you *can* be uniquely identified. In fact, you can test this out and see your current browser fingerprint here: www.Panopticlick.eff.org.

All of this is not to suggest that you have anything to hide; it's only to give you back control over what information – if any – you freely, and often unknowingly, give to companies that want to track you and sell to you. Or – just as often – sell *of you* to others.

RECOMMENDATION: **DuckDuckGo** www.DuckDuckGo.com

If you really want to be search secure, DuckDuckGo is the Search Engine for you, which tracks nothing.

Unsecure Networks

Virtual Private Networks

Now, unlike Incognito mode, VPNs are a tool that actually do block your activity across the net. A VPN masks your identifying IP address, presenting the VPN server's IP address as yours. Combined with the meta-activity of many others connected to the same server from across the world, your activity is securely privatized.

RECOMMENDATION: **ProtonVPN** www.ProtonVPN.com

Unsecured, Public Wi-Fi Networks Requiring No Password

Tempting as they are, don't use them.

Everything done on an unsecured, public Wi-Fi network can be seen *by anyone* through an easy-to-implement hack called a "man in the middle" attack.

Just don't allow yourself the headache. Don't use unsecured, public Wi-Fi networks.

Instagram can wait.
(And if Instagram can't wait, you have another problem. *Hey, no judgement.*)

Password-Protected Wi-Fi Networks

An improvement on the above, sure. And on a positive note, password-protected networks do seem to be a more common practice among organizations, but even password-protected Wi-Fi is *often* still not as secure as it might be, because…

Wi-Fi Network ADMINISTRATION Requiring No Password

Because with a quick download of a free app (to remain unnamed), I – for example – was able to assume administrative access of my company Wi-Fi. There was just no admin password.
I could read all the unread SMS messages from the phone company to the account (thousands), and – more to the point – if I wanted to, I could easily switch off (and permanently block) access for any device currently connected to the network of any fellow employee.

EASY SOLUTION:
IT will implement an Administrative Access Password on the company Wi-Fi network by _____ [date].

Unsecure Passwords

Using the one, same, short password (or even a handful of its variations) on over 100 personal accounts across the web – as I did for the past 20+ years, up until last year – was never a good idea. To say the least. (*You too?*)

I just assumed it was all I could do. *How could I keep track of different passwords for all my accounts? A different password for every site? Fuhgedaboutit! Let's be real; that's asking too much.*

But ironically, the more variations of the same, simple password I kept trying to use, the more difficult it became to mentally keep track of them all anyway.

Password Managers

Password Managers have emerged as important and easy-to-use tools in the arsenal of anyone intending to be smart online in 2020. Contrary to common initial misconceptions, a good password manager does not actually have to be inconvenient. In fact, a good password manager is incredibly convenient. And it is just a far better way to keep all your accounts actually organized and secure.

For one, built-in random password generators make it easy to create, save, and update long, unique passwords that are difficult-to-crack for every account you have across the whole Internet.

And you never have to remember a single one of them. **Ever again.** Well, that's not true; you do have to remember this ONE, good password. You ought to make it great, actually; one you've never used for anything else before, but that you're sure to remember.

Take some time to think about it. It should include numbers and maybe a few random symbols that COULD substitute for letters. (Think @ for a; 8 for B; 1 for i; or I; or l; or L; (Is it an i or an l?! Or is it a showpoint, |?); 3 for E; 5 for S; etc… or a long poem or song lyric you won't soon forget, you get the point.)

I mean it. This MASTER PASSWORD should be a completely NEW password. One that you've never used for anything, nor previously told anyone any derivation of; something that no one you wouldn't want to would ever have any reason to guess – that this strange and difficult combination of keystrokes is the sole barrier between them and your entire online life.

"Now, wait a minute", you say – thinking critically – "how can having only one master password for all my passwords possibly be more secure? If someone gets access to this one, they have access to all. And websites get hacked all the time."

Good question. Four points: first, I will grant you that – while unlikely – sure, that **is** plausible (and that's why this master password will be new, unique, and memorable only to you). Second, activating Two-Factor Authentication on this account will **significantly** boost that security. Third, I'd like to return your question with a snarky question, "*What alternative system are you already using right now to keep track of all your accounts (sharing this same, old password)? Paper? A notebook on your desk? A Post-It note on the monitor? An Excel or Google Sheets file in Google Drive on a Google account that uses said same, old password – the one you've used across the web for 15 years? With no 2FA? And is that document read-protected? Or are you just bumbling them all around in your head?*"

And my fourth point… *my actual point*… we'll come to that in 30 seconds.

Additionally, downloading a simple-to-install browser extension of your preferred password manager will further make signing in to all your accounts rather painless (*and dare I say, maybe even a little… fun?*), while improving your security and peace of mind many-fold.

Password managers allow you to rest easy knowing that a potential breach on one account (unlikely as that even is when you're now using such a strong, random password) does not mean all your accounts are now at risk because you had been using that same, simple password all over the web. A breach on one is just that; a breach on one, not all.

RECOMMENDATION: **LastPass** www.LastPass.com

LastPass is a free phone app, desktop app, and website that always ranks among the top of such a list. LastPass uses "zero-knowledge encryption" (here's my fourth point) which means even if the company was hacked, they can't leak your passwords, because they actually never even *have* your passwords; your passwords are decrypted locally on your device each time you log in.

Aside from its genuinely awesome infrastructure and the aforementioned random password generator, LastPass also has additional 2FA security options, shared emergency access, automated, bulk password-changing capabilities (it'll change your password *for you*, while you watch!), an easy browser extension, a security score and ranking test, and a slew of other nice features worth your time that I won't get into right here (*hey, this isn't an ad; it only reads like one*). They also have premium plans you could pay for, but their free service is excellent in its own right and more than sufficient for the average person. (*Sorry, you're not average… but you are.*) Don't buy it.

Two-Factor Authentication

You've probably heard of Two-Factor Authentication (or 2FA, *as us cool kids call it – over at the water cooler** – and as I've already mentioned above thrice now). And maybe you've even been forced to use it on a few sites? Maybe your bank required your phone number, so they can send you a text message to confirm every time you log in? You might appreciate this security. Or you might consider this all a complete hassle. *It doesn't have to be.*

But there's no denying: 2FA does take security to a whole new level, because it requires two conditions to be met in order to access an account: the combination of something you *know* (your password) and something you *have* (your device displaying a code).

It really is a near-genius innovation in security. *Yes, I said 'genius'. Nearly.*

Most 2FA apps today are *TOTP* – Time-Based, One-Time Passwords – a time-sensitive system of issuing a new 6-digit code every 30 seconds. 30 seconds is a very slim window for any hacking attempt to deduce your password, making your account quite secure, *particularly* if you use 2FA in combination with LastPass' random string of long passwords. (Apparently, just 1,000 individual words comprise 91% of all passwords! Also apparently, it would take modern computers nearly some billion years to break the cryptography of a password that looks like *h7SGqJar*!09kE^FQw*. *…Not my password, don't get any ideas*.)

<u>One Important Caveat</u>:
An app-based 2FA is significantly more secure than 2FA connected to the SMS of your phone. Recently, hackers have been calling up phone companies (or even just walking into phone stores), answering even only a few, easy-to-deduce identification questions, and then re-directing (or "porting") a targeted phone number to their own SIM card. Then they use the 'Forgot Password?' option on a website to receive an SMS-based 2FA code to reset your password and gain access to an account. (Particularly, to steal Bitcoin.)

RECOMMENDATION: **Authy**	www.Authy.com

Authy is perhaps the best of all the 2FA apps. Like most others, Authy also uses TOTP, but what sets Authy apart is that it also syncs an automated, cloud-based backup of your account across all your registered devices. (They also have a desktop app.) So even when you inevitably break or lose your phone, you need not worry that you also just locked yourself out of all your accounts. I couldn't believe it but Google Authenticator does not do this; to me, that's a DEAL BREAKER. *This relationship is over, Kevin!*

For Advanced Security, An Important Warning:
Now, if you want 2FA on your Gmail account (definitely recommended as – let's be real – that probably is your most sensitive account, second to money stuff), then you're going to want to register your Authy account with ANOTHER email address. Because – think about it – if you lost your phone (and for argument's sake, your computer with the synced desktop app also), you will need to be able to login to the email address registered to your Authy account to regain access. Obviously, you can't do that if your Authy account is also registered to your 2FA-locked Gmail account.

That is very important. *So important I'm going to CTRL+C / CTRL+V it again.*
That is very important.

RECOMMENDATION: **ProtonMail**	www.ProtonMail.com

It's advisable to use a secondary email to register Authy, and also as the security backup email on your LastPass account (under Advanced Settings). (Yes, this means you can make your Gmail address your primary login username for LastPass.)

ProtonMail is a secure, free email service that is also "zero knowledge encrypted" and utilizes two passwords to login: one to access your account, and the second to actually decrypt your mailbox. Because it requires two passwords, you could safely use this account WITHOUT any 2FA activated (in fact, to set this all up correctly, you must), making it the best choice for registering sensitive accounts like LastPass and Authy.

Now, you didn't hear this from me – but you *could* even use the same, rare, long, memorable new master password (or better, a slight variation) for each of your LastPass, Authy, and ProtonMail's two account passwords.

The Bottom Line:
ProtonMail is ideal for this, but *whatever* email address you use to register your Authy account, DO NOT enable 2FA there. I'd also recommend just not telling anyone the email address of your new ProtonMail account and also just generally not even really using it for anything else.
Why risk it?

*You can also even 2FA your LastPass account. (Again, only if your security backup email (under Advanced Settings) is registered to an account that you don't need LastPass to get into… i.e.; ProtonMail without 2FA.)

Settings

Phew, that got heavy for a moment. Advanced stuff there from page 12.

(If all of this was just very confusing to you, I'm happy to personally walk you through your situation. Feel free to message me; again: hello@AdamGreenberg.com.)

Here are some more settings to consider:

Evaluate your Google Activity
If I may be so forward, allow me to make a weak assumption: you have a Google account.

If you haven't already, it's a good idea to take an inventory of your Google record. You can see your history across many of its platform services, delete entries, and alter default settings at https://myactivity.google.com. I will say, it is nice that they even make this available.

Did you know that if you just generally kept your location access on and your settings as defaulted, there is a time-based GPS map of everywhere you've been?

Mobile

Turn off Background Data

When you download a new app to your phone, the use of your data "in the background" (i.e., when you're not even using the app) is often enabled by default. This is a terrible setting for most apps, and especially so if abroad and paying for data.

> Take account of each app and ask yourself if this one *needs* to have access to using your data in the background. 97% chance it doesn't.

On Android: Generally found in: Settings > Network & Internet > Mobile Network > Data Usage. Then scroll each app individually and turn off "Background data".

*Remember to do this after downloading any new app.

People

Here's some more good news: **People, you are both the problem and the solution.**

A lot of these problems arise as the result of being just a little bit *uninformed* about basic Internet security.

And a lot of these solutions arise as the result of being just a little bit *intentional* about Internet security.

And now that you know… you know.

> SO, TO RECAP:
>
> - Log out of your accounts before jumping up from a public computer. (*And don't save them by default*.)
> - At least save your files to a dedicated folder, not to a public computer's Desktop. (*Must you save anything personal there anyway?*)
> - Empty the Recycling Bin. *Or you didn't actually delete anything*.
> - **Use a password manager and enjoy knowing you're significantly more SECURE.**
> - **Enable 2FA on (at least) your most sensitive accounts (carefully).**
> - Consider browsing through a VPN.

But wait, there's more!

Physical Security

Phones in the Back Pocket?!

Don't keep your phone in your back pocket. Big as they are and small as we know pockets often are (women's pants pockets especially *[Why is that? Huge business opportunity there, btw*]), your phone in your back pocket is nearly always half-exposed. An easy target for opportunistic theft. *And opportunistic theft is the most common theft.* Just don't make it easy.

Riding a bike?

Do you like music or podcasts while riding? *Me too.*

Annoying as it may be, better though to be in the habit of listening with only one ear-bud, so you can still safely hear the sounds of oncoming traffic.

Financial Security

Banks and Credit Cards while Abroad

Notify any banks or credit card companies that you're traveling abroad, so that transactions are not pre-emptively denied. Also, some banks have apps that allow you to turn off the use of your card if you've just lost it.

Recommendations: *Capital One* offers a credit card with no foreign transaction fees.
Charles Schwab offers a debit card that refunds all worldwide ATM fees.
Together, these two cards are terrific for traveling / living abroad and are the secret financial combo of most digital nomads / travel hackers.

RECOMMENDATIONS

As an overview, below are the previously recommended apps and websites of this guide, plus additional AntiVirus and Defragmenting (maintenance cleaning) programs.

Again, no incentive has been made to the author in recommending any of these:

Worthwhile (and Free) Apps and Services

- LastPass – Password Manager
- Authy – Two-Factor Authentication
- ProtonMail – Secure Email Service
- ProtonVPN – Virtual Private Network
- Brave – Internet Browser
- HTTPS Everywhere – Browser Extension
- Ghostery – Browser Extension
- DuckDuckGo – Search Engine, Browser Extension, and App
- FindMyDevice – If lost, this is one Google app you could be glad you had
- Malware Bytes – AntiVirus Software
- CCleaner – Computer Cleaning Defragmenting Software

Helpful Websites

- HaveIBeenPwned.com
  Quickly check your email against a database of known security breaches.

- EquifaxBreachSettlement.com
  In light of their 2017 breach of 248 million Americans' personal financial data and credit records (?!), Equifax is now offering 10 years of free credit monitoring. Take advantage. Don't delay. *How long do you think this offer will realistically remain accessible?*

- SpreadPrivacy.com/tag/device-privacy-tips
  Short Privacy and Security Guides for your specific devices.
  Take a quick look and implement.

- Panopticlick.eff.org
  Test your browser fingerprint. *Surprised it's unique?*

- TOSdr.org
  Terms of Service; Didn't Read.
  Brief summaries on the rights you've given up when you clicked "I Agree."

- myActivity.Google.com
  Evaluate your Google records, delete entries, and alter the default settings.
  Seriously, take a look.

- Switching.Social
  Ethical, easy-to-use, privacy conscious alternatives to the most common social media sites.
  Okay, yes no one uses these.

CONCLUSION

Only you can prevent forest fires and only you can be smart on the Internet.

But if you take *just one thing* away from this guide, please make it to secure at least your most important accounts with a long, random, strong password and a password manager.

Now, if you're using both the long, randomly-generated, unique passwords of a password manager like **LastPass** for every website account you have, AND the TOTP codes of a 2FA app like **Authy** on top of those passwords (#CouplesGoals!), AND your Authy account and LastPass Backup Email are registered to a secret **ProtonMail** email (allowing your **Gmail** and your LastPass accounts to also both be safely 2FA-protected), AND you connect to the net through a VPN on a more privacy-focused browser, well then… consider yourself now among the very most secure people on the Internet in 2020.

I would have welcomed you to a truly small club of nerds, but security like this just is more mainstream today. Because unfortunately, it's necessary. Still, you are – no doubt – ahead of the curve. And at least for now – until quantum computers beef up – no one is drinking your milkshake. Your security level is **Beast Level**. You could pat yourself on the back, if you so fancy.

ACKNOWLEDGEMENTS

This guide is the result of going down a rabbit hole.

And it still really only just scratches the surface. *We didn't touch on phishing emails, identity theft, backing up your files, or being smart on Social Media.*

*If you're talking 2FA at any water coolers, I want to be there.

Do you have feedback? Has this guide motivated you to take action? *Let me know.* Can you recommend another security topic that should be here? Personal questions about safely setting up your own 2FA configuration? Or strong, adversarial opinions about an app herein recommended? Do you work at Google and want to correct my *obvious* misunderstanding of *your* privacy issues? Thanks!

hello@AdamGreenberg.com

And thank *you* for reading. Go make some changes; your passwords are showing.