Title: Best Security Practices for Protecting Self and Tendies - Monthly Repost
Author: FordicusMaximus
Created 2022-04-21 00:30:21 UTC
Permalink: /r/DDintoGME/comments/u8armf/best_security_practices_for_protecting_self_and/
Url:
https://www.reddit.com/r/DDintoGME/comments/u8armf/best_security_practices_for_protecting_self_and/

Alright, you beautiful internet-dwellers, listen up!

I'm reposting this since I just scrubbed my account. So hopefully it can help refresh some of you old-timers that have already seen it, or be of use to you newcomers.

Many of you smooth-brains are just that and understand online security even less than you understand that your wife's boyfriend isn't really your friend...

Online security is something you should absolutely work on NOW and not WHEN you get those stacks and stacks of tendies. Not only is this paramount to your physical safety, but also helps keep your money, identity, family relations, etc... secure and safe from prying eyes. Let's face it, these rich f*ckers aren't going to be happy when this is all over and will very likely try to enact some form of retribution. Don't worry about some brute coming in to smash your kneecaps, but think more along the lines of lawsuits for some bullsh!t that keeps you in court for years and bleeds your money dry. And out of pure spite no-less.

So what's to be done? Well, it's fairly easy with modern tech to protect yourself and your family, BUT it does take *discipline*. Below, I'll show you some of the best tools and practices that I myself incorporate in personal and business life and have had zero incidents with identity theft, hacks, malicious software, or any other crazy stuff happen.

Let's start with practicing the art of mouse hovering (or copy/pasting if on mobile). On most websites (including Reddit), a person can insert pretty much any link anywhere. So BEFORE you click on those pretty little blue words below, take a second to hover your mouse over the words to verify that the link that is hyperlinked reflects what's being said. You'll see the address it links to in the bottom left corner of your screen. If it looks suspicious, don't click on it. If on mobile, simply long press to copy and then paste into a browser (but don't hit enter right away) to verify URL. You can also use tools like this [redirect checker](https://wheregoes.com/), or this [URL scanner](https://vms.drweb.com/online/?lng=en).

#1 Password Manager \- [Bitwarden](https://bitwarden.com/) (did you hover over the link to verify before clicking?)

\- It's FOSS (free and open source) with a super cheap paid option.

\- Works beautifully on Windows, Mac, Android, and iOS. It even has browser extensions.

\- E2EE (end to end encrypted) locally on each device and has all of the features like autofill, MFA (multi factor authentication), biometric locking, password generator, etc...

Please, for the love all apekind, use this in your everyday life! **NEVER** reuse passwords. Create a solid and unique password for your Bitwarden account and remember that single password/phrase. This will be the *only* one you'll ever need again, so make it good. As a side note, it's easier to make a memorable [PASSPHRASE vs password](https://protonmail.com/blog/protonmail-com-blog-password-vs-passphrase/). Auto generate a random password/phrase for literally every other account you have or make in the future for anything. This helps protect you in case some website has a data breach (like Facebook for the umpteenth time this year). Using a combination of letters, characters, capital letters, and special characters creates a virtually unbreakable (through brute force or guessing) lock.

#2 Email Forwarding/Aliases

\- Huh?

\- This is where you generate specific email addresses for individual accounts. For instance: I create an account for Reddit. But instead of using [*smoothbrain@gmail.com*](mailto:smoothbrain@gmail.com), I create an email through one of the below providers that looks something like smooth-brain-reddit@pm.com. This way, I know exactly what account it's to and no other account has it. It also protects my actual email address from these websites I create accounts on. It's simply acting as a buffer before it hits my inbox.

\- If you're just looking for a *hit-it-and-quit-it*, use the FOSS tool of Guerilla Mail. No emails are attached and you can send/receive mail to the random generated address. All mail is only held for 24 hours and then deleted.

Some of the providers I personally use are: [Protonmail](https://protonmail.com/), [Mailbox.org](https://mailbox.org/), [AnonAddy](https://anonaddy.com/), Guerilla Mail and [SimpleLogin](https://simplelogin.io/).

SimpleLogin is $15/yr if you are a student and have access to an .edu email. But these are all fairly inexpensive services to pay for IF you want to upgrade. They **ALL** have a free tier as well.

Side note: It is also wise to have separate email accounts specifically for finances! Don't use that email for anything else aside from your banking, credit cards, brokerages, and so on.

#3 MFA/2FA (Multi/Two Factor Authentication)

\- This can be a slight pain to use, BUT, it is super important. Especially when it comes to finances!

\- My two choices for convenience are [Aegis](https://getaegis.app/) for Android and [Tofu](https://apps.apple.com/app/tofu-authenticator/id1082229305) for iPhone.

\- Both are FOSS, E2EE, and can be backed up to store elsewhere.

\- Enable MFA whenever possible. This will add an extra layer of security to your accounts that necessitates a person to have access to the random and temporary code before being able to log in.

\- Do note that some websites have their own proprietary app for these codes or do 2FA through text messages. Text 2FA is not nearly as secure, so stay away from that if possible.

#4 Cloud Storage

\- Did you know that Google, Microsoft, Dropbox, and many of the other cloud providers can literally see all of your dirty pictures, read the text of your documents (including finances), and see every file, date created and edited, and files "trashed"? Apple claims they can't, but they also don't have a public code and don't like outside audits...

\- What's one to do?

\- First, I would utilize a FOSS program like [Cryptomator](https://cryptomator.org/). What this does is create an encrypted space where you can throw in anything and everything and then lock it. This space can also be stored in a Google Drive account (or any online storage really), while actually remaining encrypted. Create and store the random-gen password in your Bitwarden account. And guess what?! This is also available for all major devices.

\- If you want a native encrypted cloud storage, one of the better priced ones is [Sync](https://www.sync.com/). The free tier gives you 5GB to use. Here's a referral [link](https://www.sync.com/?_sync_refer=a17b9e030) if you want extra free storage a well. It's still E2EE, but not open-sourced. They do, however, have an audit on their encryption and source codes. I use this for backing up photos, business docs, and keeping a backup of one of my [Cryptomator](https://justchecking.org/) vaults here.

#5 Online Tracking Prevention

\- Since most of you probably couldn't use a rock to break open a coconut, we're going to stay *simple* for this one as well (KISS style). Download [Brave Browser](https://brave.com/) and set that as your main browser.

\- I've seen wayyyy too many screenshots with ads spammed through on their screens. [Brave](https://geekprank.com/) has native ad blocking and anti-fingerprinting measures built in to it without the need to download extra extensions. This is plug-n-play privacy.

\- Ad companies (think Facebook, Google, Microsoft and the likes) have so much more info on you than what you can even imagine. They know your Age, marital status, location, work relationships, overall psychological health, financial status, what foods you like, and so much more seriously invasive sh!t.

\- This browser can help reduce much of that information collected, as well as help spoof and provide incorrect information about you.

\- And please, please, please STOP using Google. Use ~~Brave Search, SearX, Qwant, Ecosia, or Presearch~~ as your primary search engine. They're mostly just as good as Google and don't censor or track you. To change on pretty much any browser for mobile or desktop, go to Settings > Search Engine > Selected Search Engine. Easy as that.

\- *Edit: Recently with the whole Russia/Ukraine situation, DDG (DuckDuckGo) took a stance and decided to censor and omit "Russian Propaganda" from their indexers. Regardless of your thoughts on their stance, it is a form of censorship and has been removed from the recommendations.*

This is it for the *main* concerns. But I will go into some details below for a little more in-depth security \[just the\] tips and practices.

\- Lock down your phone plan accounts with only specific users allowed to have authorized access. This will help prevent sim swapping. If someone manages to get into your account and you have SMS 2FA enabled for finances and important accounts, they can more easily gain access to those accounts. While different for each provider, you'll want to call and ask them to place a "port freeze" or similar on your account. This can be done through settings on some provider's websites. Some will send you generated codes each time you want to make a change, while others will require proof of verification before major changes can be made.

\- For those of you involved in crypt0, get yourself a [hardware wallet](https://www.securities.io/the-best-hardware-wallets-to-keep-your-crypto-safe-in-2021/) (or multiple) and back those seed words up in both a physical copy stored in a safe or lockbox, and also in a well protected encrypted account like Cryptomator. Delete and use those seeds to recover your wallet BEFORE you transfer funds to that wallet to ensure you have them recorded correctly!

\- If you're looking for more privacy friendly and secure computers/OS, Linux is super easy to install and use now days with very strong security built in. [Ubuntu](https://ubuntu.com/download/desktop) and [Mint](https://linuxmint.com/download.php) are probably the most user friendly ones to use. Simply look up videos on how to install and you'll be up and running within 20 minutes or so. Personally, I use [PopOS](https://pop.system76.com/) as my daily driver.

\- For mobile devices, Apple is the go-to for most people. But as I said earlier, their privacy promises are based solely on their own word and we've all seen how self-regulating bodies act behind the scenes. I use [CalyxOS](https://calyxos.org/) (Android minus Google) myself on a Pixel device.

\- For communications... Hands down, use [Signal](https://signal.org/) messenger for all important communications between friends and family. It's FOSS, has the same functions as Whatsapp, is E2EE and privacy focused, and you can send pretty much any file type to any other person using Signal. This also replaces SMS/MMS on Android. If you still use email, [ProtonMail](https://protonmail.com/) is a very good (and secure) email provider.

\- While online and contactless payments are becoming more popular, the tech to hide our personal info is still lacking. For those of you in the EU, you have more options through your banks, but for those US apes, if your bank doesn't offer temporary card numbers, use the [Privacy.com](https://privacy.com/) service for online purchases, and use Google/Apple pay if using NFC (contactless) payments in stores. This will keep your real credit (or debit) card number hidden and therefore reduce the chances of identity or financial theft.

\- Another discipline to work on is to **ALWAYS** go to the official site of whatever software you're trying to get and download it from their downloads page. Also, check for the "https" in the address. A general rule is to stay away from antiquated "http" addresses as they don't offer the same kind of protections. For instance, navigate to https://bitwarden.com/download/ and then click on the desired device you want to download it for. That will lead you to the correct and *official* publishing of the software.

\- VPNS? Sure. They can be useful. Don't just download and use any free VPN though! They can steal/collect just as much data as an unprotected WiFi network. [ProtonVPN](https://protonvpn.com/) is a newer service offered by the world class ProtonMail team. It has a free tier and is easy to use. Even if you don't pay for one, definitely use it whenever you're on **any** open WiFi connections such as sitting at Starbucks or the airport. You'd be amazed at how easy it is to collect data packets from those networks and potentially get the login info of others.

\- If you want to see who sells your info when you create an account or contact someone, enter your name as their business/name. If you get an email from someone else with that entered name, you'll know exactly who sold and who to black list. For example: I make a Netflix account and enter my name as "Netflix Test" and use a one-off alias email for this specific account. A few days later, I get an email from Grubhub addressing me by the name of "Netflix Test". I'll know exactly who sold it and to whom. And with the alias email, I can also disable this account's emails easily.

\- Condoms and birth control! Please, for the sake of all apekind and humanity alike, utilize this! If you're happily married or with kids, don't have more heirs than what you can spend time with and raise correctly. See ol' Ken boy for how children who aren't loved enough turn out when they're older. You don't want your offspring to become the very thing we're up against. For those of you without children, you don't want to knock up or get knocked up by some random person and become embattled in lawsuits and lose those precious tendies. There have been many instances where someone will sleep with you to get a chance at your money. It's not that uncommon!

\- Visit \[r/ NukeRedditHistory\] for a lovely little extension that will replace old comments/posts and then delete them. Not only should you do this currently every now and then, but especially post squeeze! I use this often.

\- You can also check out the [Redact](https://redact.dev/) software that allows you to remove old content from [multiple platforms](https://redact.dev/services) (FB, Twitter, Reddit, etc).

\- Make sure to frequently check [HaveIBeenPwned](https://haveibeenpwned.com/) to see if you have any breached accounts!

For more security tools and practices, head over to ~~\[r/ privacytoolsIO\] or~~ [~~privacytools.io~~](https://privacytools.io/) (now deprecated) \[r/ PrivacyGuides or [PrivacyGuides.org](https://privacyguides.org/)

This is all I can think of for now. The coffee in my veins has ran out and it's now time to replenish. I hope you have found this helpful and if you have any questions, let me know. I can go into more details on specifics if they come up, or I can answer questions about cyber security in general. But please, use these measures and keep yourself, your family, and your finances safe!

Edit #1: Just read [THIS](https://cybernews.com/security/rockyou2021-alltime-largest-password-compilation-leaked/) to understand the importance of having different PWs for every account, as well as MFA/2FA on top of that.

Edit #2: Updated the privacy subreddit info/website and added some links to new services.