Open Resource for Personal Online Privacy

What is this document?

This is a public resource doc for anyone who is trying to learn more about protecting their passwords, identity, credit card information, webcam access, or other personal information online.

This is free for you to share/steal/contribute to. If you'd like to make an edit or contribute, just comment anywhere in the document.

I hope this helps you and your loved ones protect yourselves online.

TABLE OF CONTENTS

Why do I need to worry about my security online?

TL;DR
Like it or not, your information is everywhere on the internet. That fight is lost. It's best to think of online security as a bike lock: if someone really wants to get your stuff, they're going to get it. Yes, you could go off-grid and live like a hermit, but that's not practical. What we can do is take enough precautions that we are not easy targets and avoid major problems.
—---
There's a lot of information out there and it's confusing. Securing your information online is probably something you feel like you know you need to do, but haven't really figured out how to take action. In fact, this behavior is reinforced by the idea that, probably, nothing bad has happened to you so far.

No matter what your situation, the first step is realizing that you've got lots of valuable information online.

There's personally identifying information like your address and social security number, but there's also high-risk information like your bank account numbers or bank logins. You might think, yes, but I don't have my bank account number on my website for everyone to see, so I'm fine, right? Maybe. But hackers know that most people use the same password for most of their accounts online–so, if they hack a weak organization, like that random app you downloaded last week and made an account for, they know that there's a chance that they can use the same email and password for your Bank of America login. You can see the problem.

On top of that, there's also information out there about you, like your email address, that might not sound so bad if it gets into the wrong hands. Who cares if someone wants to randomly email me cat gifs, right?

Even your email address alone can pose a problem. For instance, there are many people who are happy to pay money to acquire your email address so they can sell it to marketers who can solicit you. If you've ever gotten an email and said, "I never signed up for this. Why am I getting this email?" That's because your email was found and aggregated into what marketers call a "compiled list." If you're not into junk mail, then keep reading.

Watch this video:
What Happens When You Dare Expert Hackers To Hack You? (Real Future, Episode 8)

In this resource document, we're going to take a tour of some of the kinds of information and some of the kinds of threats that exist out there. Buckle up.

8 Simple Ways To Protect Yourself Online?

1. Enable Automatic Updates On Your Devices

Software is constantly changing. Typically, as software ages, it becomes easier to hack. Having up to date operating systems on all your devices helps remove a layer of vulnerability.

As soon as a new update arrives, hackers begin working on how to identify weaknesses and exploit them. In general, newer software is safer. This does NOT mean you should click on every pop-up you see on your machine. In fact, this is a common way hackers will get unknowing users to download malware or viruses.

See below about trusting pop-ups.

2. Use Antivirus & Anti-Malware Software

This doesn't apply as much for Mac systems, since most viruses and malware are written for Windows machines. Still, having software that constantly

How-To Geek recommends Avira or Kaspersky if you need something "heavy-duty." Additionally, Malwarebytes is a well-regarded tool for malware detection.

3. Use A Password Manager

I shouldn't have to say this, but you absolutely need to have a password (fingerprint password) on your laptop or phone. If you lose your phone, you are in big trouble. Probably the scariest part of identity theft is that you may or may not be able to tell if it's happened.

Most people use bad passwords. Bad passwords are things that are easily guessable or have a predictable format. *YourLastName2009!* or someone's birthday are both easy to "phish." Phishing is more "social" hacking than technical. It's when someone solicits information about you using social tactics like a phone call to your cell phone company. With just a little bit of information about you, like a birthday or other info you might have on Facebook, phishing hackers may be able to "verify" your identity with a service provider and get much more information, like emails, passwords, or credit card info.

Here are some password managers that will help you create better passwords, change them on a regular basis, and also keep them safer than you can keep them on your own:

- 1Password
- Dashlane

- LastPass

Here's an open resource for generating passwords if you need one right now and can't install a password manager yet: PasswordsGenerator.net

Just in case you think you're the only one who is behind on this, here's a picture of Hawaii's Missile Alert Center with passwords written on post-its stuck to their computer monitors.

> *"[The Hawaii Emergency Management Agency] issued an erroneous warning of [an] impending ballistic missile attack. And apparently, it was a poorly designed system that was behind the faux pas — including passwords stored on Post-it Notes."*
>
> - Associated Press

Photo Cred: Associated Press

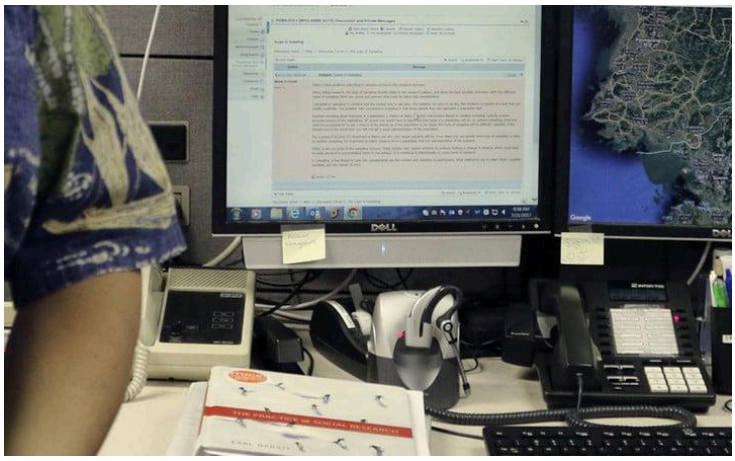


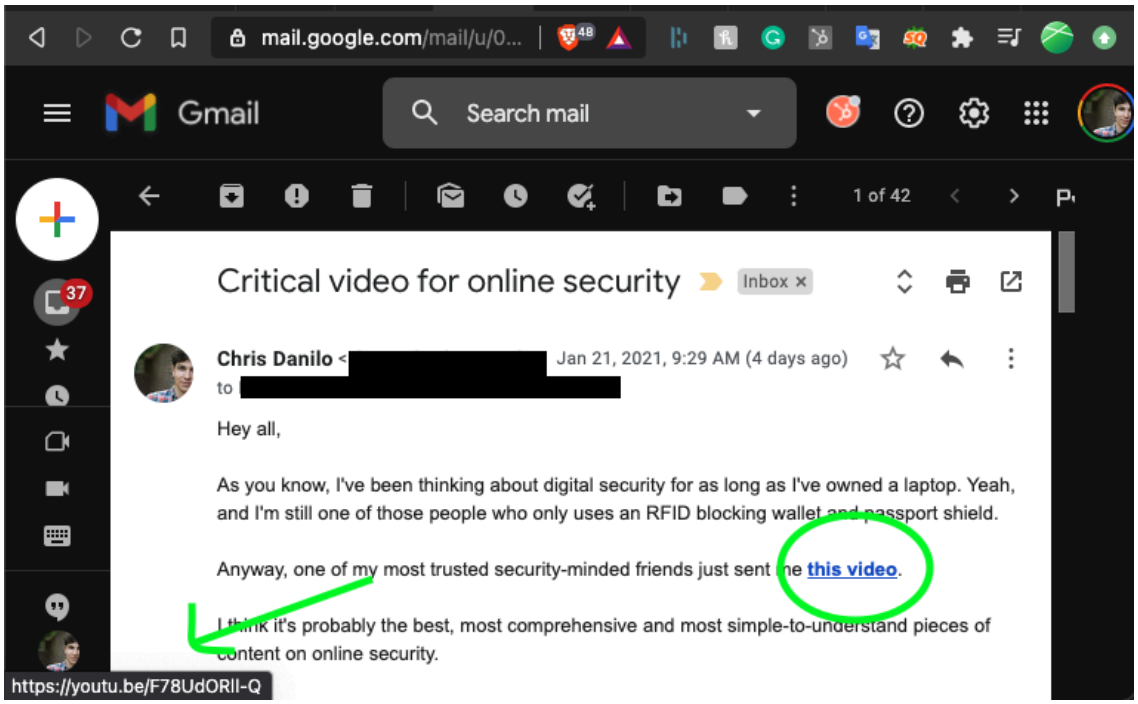
Photo Cred: Associated Press

4. Be Skeptical Of Links In Emails

Somehow, this is still the most common way for a hacker to get something installed on your computer. Nothing bad will happen if you open an email. Bad things can happen if you click a link in an email.

If you want to check to see where the URL will actually take you, most browsers give you a link preview in the bottom left corner of your screen.

Here's a screenshot of what I mean:



Just hovering over the link in the email will show you the URL it will take you to.

If the link text says CapitalOne.com but the preview says CapitalOne.oneclickyougo.com you have just found that the link is not what it says it is. This is called a subdomain and though it looks like it's CapitalOne's website, it's not. Whatever comes right before the .com part is where the link will take you.

5. Don't Trust Pop-ups

I know, I know, it looks like the pop-up is from your computer. That's part of the design. It's supposed to look like a system alert that you would normally expect to see from your computer.

The best example is Flash and Java updates because they're so common on Windows machines.

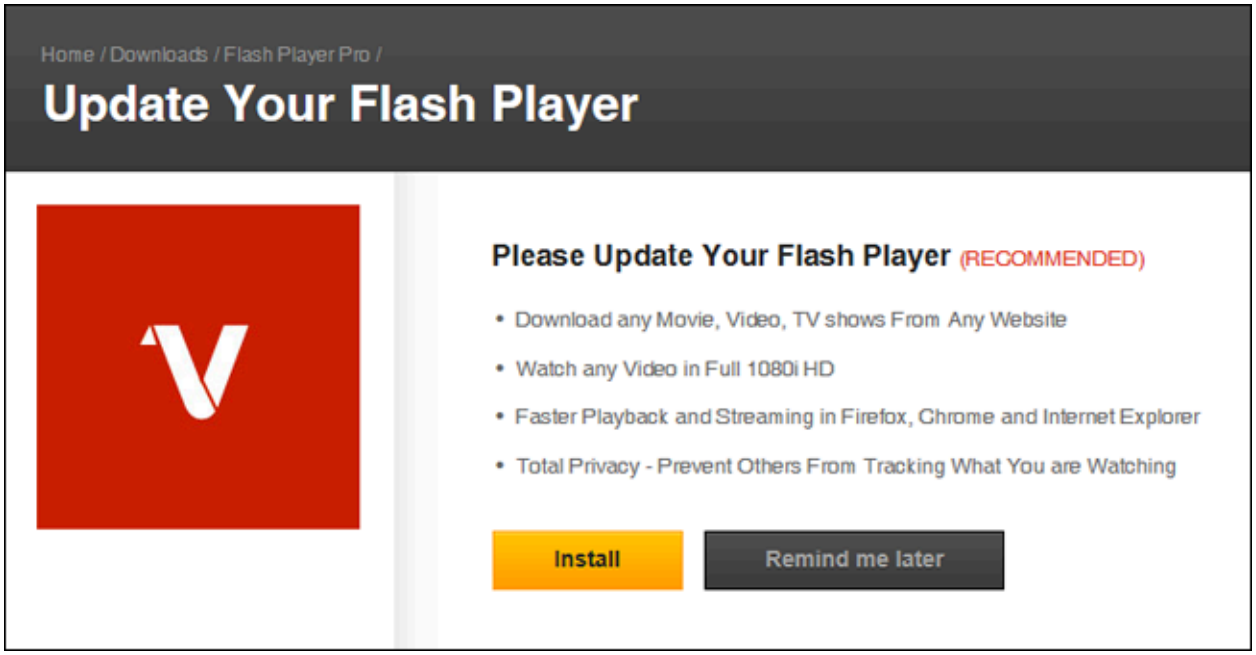


Photo Cred: How-To Geek

Here's what How-To Geek says about them:

"A site may give you a warning you need the latest version to get that cat video to play. Instead of clicking the link (or button) to update, do a search for "adobe flash" and get the update from Adobe's official website—not the popup from catvideos.com.

This applies to "tech support", too. Don't believe any site that says it's detected a virus on your system (or any calls from Microsoft). If a popup says you have a virus on your computer, don't click on it. Instead, go to your Start menu, open your antivirus program of choice, and run a scan from there instead."

6. Use A VPN if you need to use public Wi-Fi

A VPN is a Virtual Private Network. They often come packaged in as services with Password managers like Dashlane mentioned above. It's basically an encrypted channel carved out between you and the internet router. It means that you're not literally broadcasting your IP

address or personal information to everyone around you. This is called “packet sniffing” and it’s a way for hackers to see what information you’re sending to and from the router. It’s not hard to do this and you are welcoming attacks if you don’t have a secure and private network in public spaces.

If you travel a lot and find yourself in need of public Wi-Fi, you will definitely want to use a VPN.

These are solid recommendations:

- NordVPN
- ProtonVPN
- MozillaVPN (From Firefox)

But there’s a catch. Not all VPNs are created equal. Plus, since the Snowden trial, many governments have decided that it’s not ethical to spy on their own citizens. This means there is now incentive for governments to collaborate with other governments by sharing data. If you’re researching which VPN to use, just make sure you find one that is well-reviewed but also not part of the 5 Eyes Agreement, the 9 Eyes Agreement, or the 14 Eyes Agreement.

Here’s an article that ProtonVPN wrote about these agreements if you want to dive more deeply into the details.

7. Use A Browser That Doesn’t Sell/Store/Use Your Data

Browsers like Chrome are ubiquitous, and you may have noticed that they hog a lot of your computer’s speed. That’s because about half of the activity that Chrome has running in the background is advertising surveillance. This means they’re tracking your clicks, keystrokes, and serving you ads from marketers.

There are plenty of other browsers out there with better security and will allow you to “opt-out” of the surveillance economy.

Try these:

- Safari
- Firefox
- Brave

Brave is my personal favorite. It’s built on Chromium, which is the original core of Chrome. It will do everything Chrome does and will let you keep/import all your Chrome extensions and bookmarks--and it will do it at twice the speed because it’s not using your computer for ad surveillance.

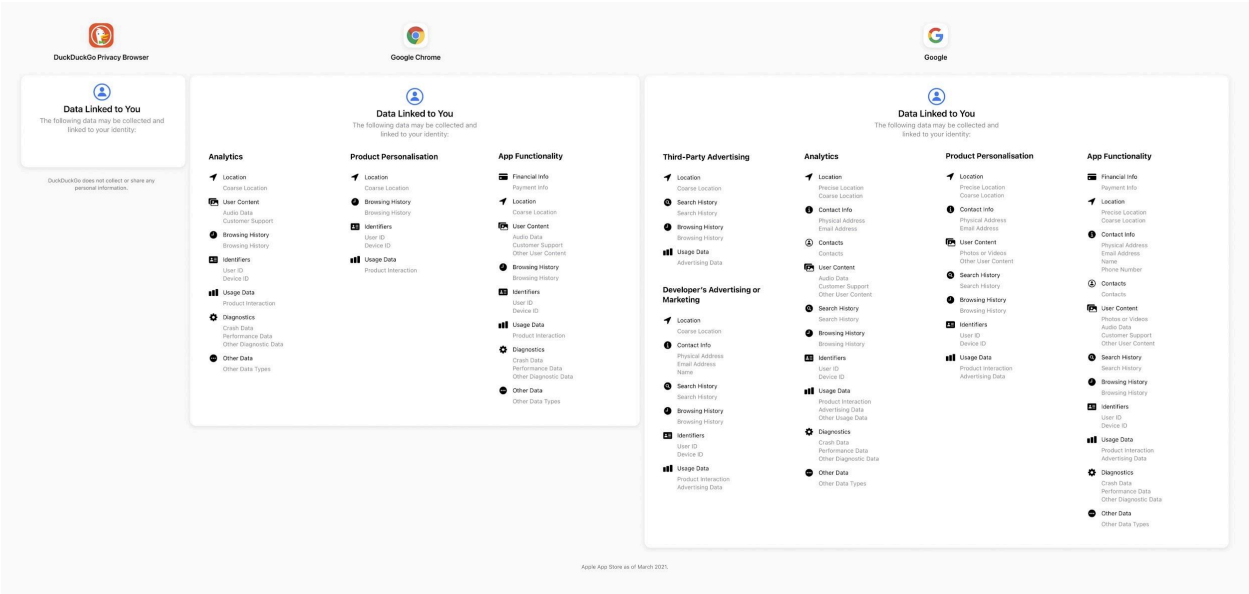
Google Is Tracking You

Outside of Google's web browser, Google Chrome, tracking is still happening. Google.com is the #1 most used search engine, but that doesn't mean it's the best. I prefer DuckDuckGo. They provide great search results, and they proudly advocate for web privacy.

Here's a tweet from DuckDuckGo revealing some basic info about Google that most people don't realize:

DuckDuckGo's Tweet

Here's the image of everything that Google tracks and knows about you:



What Google Tracks

8. Use 2 Factor Authentication

2FA is the process of using 2 devices to authenticate your identity before logging you into an account. If you've ever tried to log into your bank account and you get a text message with a code, that's 2FA.

In general, 2FA using phone numbers isn't that secure. It'll be okay for most personal things, but if you're locking up bank info or identity info, you'd be better off using a YubiKey or something similar.

Just Do Those 8 Things

If you just do these 8 things alone, you'll be better off than the vast majority of internet users. Remember, the goal isn't to store all your information in Fort Knox, that's impractical and would be a huge pain if you needed to check your bank account or upgrade your Verizon account. Instead, you'll be a darn tough bike lock that deters most thieves from messing with you.

Basic Laptop Security

Laptops are great because they allow us to take our office with us. Of course, there are still downsides. If you need to use public wifi networks or access the internet through any other network that you don't own, you'll want to read the section above about VPNs. These are mandatory. You are a target if you access wifi at the airport and don't use a VPN.

Outside of wifi access, there are some things you can do to set up your laptop to be more secure. Here are some things you can do to increase your physical laptop's security.

Don't share accounts

If your friends, family members, or colleagues need to use your laptop, don't allow them to use your account. Either give them access to the "Guest" account, or create a separate login for them under User Preferences. With fast user switching, this is convenient for everyone.

Data encryption

All of your hard drives (disks) should be encrypted. This includes both your startup disk, and backup disks (Time Machine, etc.). If you're on a Mac, you'll want to encrypt with MacOS' Filevault using a strong password. A strong password is not one that you make up. It's one that is generated by a password manager like 1Password or Dashlane. See the password management section above to learn about this.

Strengthen Your System Preferences (for Mac Users)

Go through these steps for your Mac's System Preferences (from the Apple menu in the upper left hand corner of your screen):

- Under "Users and Groups":
    - Set a strong Mac login password. Don't make one up! That's not secure enough.
    - Delete any other unused accounts other than the guest account.
    - Under Login Options, turn off automatic login.
- Under "Desktop & Screensaver":
    - Turn on the screensaver with a reasonable timeout like 5 minutes.
- Under "Security & Privacy" Settings / General:
    - Require password after sleep or when screen saver begins. It's handy to add a short delay (say 5 seconds).
- Under "Security & Privacy" Settings / Firewall:
    - Enable the firewall.
    - Under Firewall Options, block incoming connections for all apps listed.

        - Uncheck the box to automatically allow signed software to receive incoming connections.
    - You may need to unblock your development server, say to allow for mobile development. Do this on an as-needed basis, and only expose as much as is necessary.
- Under "Network":
    - Under "Advanced", remove any generic preferred networks, e.g. "linksys".
    - Uncheck the "auto-join" box for any network that you don't use frequently.
- Under "Sharing":
    - Set a reasonable Computer Name to use as the hostname.
    - Turn all sharing services off.

What Is Identity Theft?

Identity theft is when someone steals information that is used to verify your identity to an authority. This could mean your driver's license, social security number, passport, credit card, or your fingerprint. If someone has your identity, they can pretend to be you and withdraw money, sign up for a new line of credit, or do other shady black market things.

According to Javelin Strategy & Research, identity fraud resulted in $16.9 billion lost in 2019, and impacted 5.1% of consumers. If someone said there was a 5% chance that someone would steal your credit card every day before you left the house, would you be worried? You should be. Because that's what this means.

If you suspect any part of your identity has been stolen, follow these recommended steps by Experian.

How Can I Prevent Identity Theft?

When someone steals your identity, they often try to use your name to open new accounts.

One of the easiest things you can do to prevent this from happening is by placing a "freeze" on your credit. Since a bank has to run a credit report on your identity when you open a new account, placing a freeze on your credit will mean that the account won't be opened without your personal authorization.

Here's a great article from American Express on how this works. You'll have to place a "freeze" on your credit report with all three credit bureaus individually and this AMEX article does a great job of walking you through this (with links).

Placing a "freeze" on your account does not impact your credit score or your ability to rent an apartment. It will require that you "unfreeze" your credit when you open a new loan, like a car loan, or a new bank account–which is precisely the goal.

FAQs

My kid has an iPhone. How do I set them up?

Here's a great article by Malware Bytes. It walks you through which features they should and shouldn't have access to, how to set up "Find My" so you can locate them in an emergency, and definitively says to set them up with their own Apple ID.
https://www.malwarebytes.com/blog/news/2022/08/how-to-set-up-ios-for-your-kids

Can the FBI subpoena my SMS messages?

The answer is: they can, and they can see much of what you're saying if you use certain apps like iMessages or What'sApp.

Here's a great article by Malware Bytes on just what they can see:
https://blog.malwarebytes.com/privacy-2/2021/12/heres-what-data-the-fbi-can-get-from-whatsapp-imessage-signal-telegram-and-more/

My assessment: stick to using Signal as your primary SMS message platform.

Is Google Drive HIPAA Compliant?

The short answer is yes, but that doesn't mean you should use it like it is. The real question is whether or not you trust Google to honor their promise to not look at your data and whether or not you trust Google to never get hacked.

Here's a third party review of Google's HIPAA compliance:
https://www.hipaajournal.com/is-google-drive-hipaa-compliant/

Here's Google's comments on HIPAA Compliance:
https://cloud.google.com/security/compliance/hipaa-compliance/

Should I stop using GMail?

GMail isn't encrypted, but even if you used an encrypted email, the person you're emailing would also have to use encryption in order to keep your email safe. This end-to-end encryption is hard to find and to make things harder, Google Workspace's suite of tools are full featured and convenient.

Here's a great article from the Guardian about the details that may help you make this decision.

https://www.theguardian.com/technology/2021/may/09/how-private-is-your-gmail-and-should-you-switch

What are .Onion Sites?

Basically, Onion sites are part of the “dark web.” It means that the site isn’t accessible as part of the normal, public web. It means that you need a special, private browser to access it. The upside is that onion sites allow for oppressed populations and freedom fighters with governments who have blocked certain sites to access the rest of the world. The downside is that it is a channel for nefarious activity, too.

Here’s an article from CyberGhostVPN that explains them pretty well.
https://www.cyberghostvpn.com/privacyhub/what-are-onion-sites/

What actually makes a secure password?

The idea is to pick something that is easy to remember but also:

1. Hard to guess
2. Hard for a computer to figure out
3. Not the same as your bank account password

Here’s an article on what really matters in a password:
https://gatsby.iandunn.name/what-really-makes-a-password-strong/

Here’s a tool to help you create a secure password that you can actually remember:
http://www.egansoft.com/password/

Here’s a nerdy comic from xkcd on how we’ve spent a lot of time making passwords that are “hard for humans to remember but easy for computers to guess.” https://xkcd.com/936/

References/Resources

Not Even Close: The State of Computer Security (with slides) by James Mickens
(FYI: This is for nerds.)
https://vimeo.com/135347162

Real Future, Episode 8
“What Happens When You Dare Expert Hackers To Hack You.”
https://www.youtube.com/watch?v=F78UdORll-Q

How-To Geek
“Important Security Practices You Should Follow”
https://www.howtogeek.com/173478/10-important-computer-security-practices-you-should-follow/

VICE Documentary in HBO
“This Is How Easy It Is To Get Hacked”
https://www.youtube.com/watch?v=G2_5rPbUDNA

Associated Press
Hawaii’s Missle Alert Agency Stored It’s Passwords On Post-it Notes
https://www.digitaltrends.com/computing/hawaii-emergency-management-agency-stored-passwords-on-post-it-notes/

Experian
The Hidden Costs of Identity Theft
https://www.experian.com/blogs/ask-experian/the-hidden-costs-of-identity-theft/

Experian
What Are The Unexpected Costs Of Identity Theft?
https://www.experian.com/blogs/ask-experian/what-are-unexpected-costs-of-identity-theft/

NordVPN
“What is a VPN?”
https://nordvpn.com/what-is-a-vpn/

ProtonVPN
“The 5, 9, and 14 Eyes Agreements (Explained)”
https://protonvpn.com/blog/5-eyes-global-surveillance/

Personal Cybersecurity Checklist | Morgan Stanley
“Maintain Good Cybersecurity Habits”

https://www.morganstanley.com/what-we-do/wealth-management/online-security/personal-cybersecurity
PDF:
https://www.morganstanleyclientserv.com/publiccontent/assets/online-security/documents/CRC2203658_MSCyberSecurityChecklist.pdf

LifeHacker
"How Secure Are You Online: The Checklist"
https://lifehacker.com/how-secure-are-you-online-the-checklist-5938980

MalwareBytes Labs
"Here's what data the FBI can get from WhatsApp, iMessage, Signal, Telegram, and more"
https://blog.malwarebytes.com/privacy-2/2021/12/heres-what-data-the-fbi-can-get-from-whatsapp-imessage-signal-telegram-and-more/

The Guardian
"How Private is Your GMail and Should You Switch?"
https://www.theguardian.com/technology/2021/may/09/how-private-is-your-gmail-and-should-you-switch

American Express
"How to Freeze Your Credit"
https://www.americanexpress.com/en-us/credit-cards/credit-intel/how-to-freeze-your-credit/?linknav=creditintel-home-article

CyberGhostVPN
"11 Best Onion Sites To Safely Visit on the Dark Web"
https://www.cyberghostvpn.com/privacyhub/what-are-onion-sites/

Ian Dunn
"What Really Makes A Password Strong?"
https://gatsby.iandunn.name/what-really-makes-a-password-strong/

Egansoft
Word-Based Password Generator
http://www.egansoft.com/password/

xkcd
"Password Strength"
https://xkcd.com/936/

Malware Bytes

“How to set up iOS for your kids”
https://www.malwarebytes.com/blog/news/2022/08/how-to-set-up-ios-for-your-kids