R.A.C.K: Risk Aware Cybersecurity and Kink - Changes You Can Make Now

Written by SubNate reviewed by Mistress Mara

DISCLAIMER: the information presented here, while based on research and experience, are the opinions and recommendations of SubNate. Cybersecurity is a complex and ever-changing field. Please be sure to research the solutions mentioned to make sure they fit your needs.

Keep accounts separate

Websites, companies, and institutions build online profiles for you based on your online activity. If you want to make this more difficult, keep your online accounts separate, so they can't be linked to each other and back to you. Have work accounts separate from your personal accounts. Never link them to each other in any way. Use a different name and username for each account.

To help keep things compartmentalized, there are a few different steps you can take:

- Use two different browsers, one for work, one for personal life.
- If you're not using different browsers, log out of your account and close the browser tabs/windows before switching to your other account.
- Do NOT rely on incognito tabs, they don't provide privacy, they just tell your browser not to save your history.
- Create a 2nd user account on your computer, one for work, one for personal. Log out and back in based on workflow.
- It is also possible to install browser extensions that create "containers" for different user profiles. These are useful tools, but due to human-error and possible software exploits, they are not as reliable as the methods described above; It's easy to forget to switch.

Use a Security Conscious Browser

On the subject of browsers, don't use a mainstream browser for work. Except for Mozilla Firefox, most modern browsers usually default to Google Chrome (including Microsoft Edge). While Google is working hard to keep you safe online, they aren't working as hard to keep you safe from them. Google's main source of revenue is from data analytics and advertising. This is a built-in conflict of interest when it comes to keeping you truly private online.

Mozilla is in a similar situation, but they have a cleaner track-record of respecting user-privacy. For this reason, I would recommend the following Browsers (other good options also exist):

- Mozilla Firefox (with some hardening extensions)
- Brave Browser
- UnGoogled Chromium
- Librewolf (stripped down version of Firefox).
- TOR Browser (best for specific uses).

Use a VPN/TOR

Virtual Private Networks (VPNs) are designed to route all of your internet traffic through the servers of a 3rd party provider before reaching the internet. When done well, the connection

is encrypted, and hides the specifics of your web-browsing from outside eavesdroppers like your internet service provider (ISP), or anyone monitoring an open network.
VPNs are an important part of internet security, but they have to be used correctly. VPNs don't hide you from the VPN provider, they hide you from everyone else. VPN providers may or may not log your traffic. The best, most reliable VPNs don't keep logs of your browsing, and they charge for their services. VPNs may offer free tiers, but if a VPN is totally free, they are probably tracking and selling your data. **Don't trust them.**

Some recommended VPNs are (in alphabetical order):

- Mullvad
- ProtonVPN
- TOR

The TOR Network, or (The Onion Router) is similar to a VPN; it routes your internet traffic through a series of servers before reaching the open internet. The main difference is that instead of a VPN company owning and operating the servers, TOR is run by a combination of companies, individuals, and institutions. The servers are provided through a P2P (peer to peer) network. The data is sent in encrypted pieces through the network in layers, which is where TOR gets the "onion" part of its name. Because of the number of "hops" your traffic takes through different countries and servers, the TOR network is very good at maintaining anonymity, since it's very difficult to tell which country the connection originates from. However, the number of hops also means that the connection will have more "lag," so TOR is not good for moving large amounts of data (lots of photo or video).

VPNs and TOR can be used together or separately, but there are different reasons to use each. Mainly, TOR is useful for hiding your location in a more random, distributed fashion, not trusting any one party. If you have a VPN you trust, it's good for hiding your internet traffic from your ISP, and other trackers, but the VPN service provider needs to be trustworthy. They shouldn't keep any logs, they should have their software source code available (open-source), and/or they should be being audited by third-party security firms. If the VPN allows you to purchase your subscription via cryptocurrency or mailed cash, even better.

Passwords

Nobody likes passwords. Nobody likes creating them, remembering them, or resetting them. The passwords that are easy to remember, are not strong, and the passwords that are strong, are not easy to remember. What makes a password strong is how random it is, and how long it is; the longer and more random a password is, the harder it is for a human or computer to guess.
To solve this problem, we created password managers: programs that create complex passwords and store them for you in "vaults," or databases. These databases are encrypted with one password that *you do* need to remember, called a "master password," or "vault password." It's much easier to remember one complicated password than many.

Use a Password Manager

Pick a password manager (see below), and start using it for every new online account you create. Gradually update your existing accounts to longer, stronger passwords. Pick a password manager that has the ability to sync between multiple devices, this way you can always have a backup of your logins.

Use 2FA/MFA

Whenever possible, add Two-Factor Authentication (2FA) to your online accounts. 2FA or MFA (Multifactor Authentication), is based on the premise combining something you know (a password) and something you have (a phone or second device to hold or receive the code). You can only access your account if you have both. So if someone learns your email or username, and even if they compromise your password, unless they have the second device, or "factor," they won't be able to get into your account. Apple and Google are both aggressively promoting or requiring 2FA, which is good for account security.

Password managers can also manage 2FA for you by scanning a QR code or entering a link from your profile. When you open the manager, and select a login, you'll see a 6-digit code, on a timer, refreshing itself. This is a much more secure way of receiving 2FA codes than getting a text-message or email.

Use Strong Passwords / Change Them

Another advantage of password managers is that they can save multiple complex passwords per login. If you sign up for an account with security questions, the website doesn't actually care what your answers are, it's only matching a selected question with the provided answer. Instead of actually entering your mother's maiden name, etc., generate another strong random password and enter that instead. Just be sure to save which question you chose as the name of the "password."

Some password managers will also keep track of the date the login was saved and when it was last updated. Passwords that haven't been updated in a while should be changed out. How often is a matter of opinion, and depends on how important the account is. It's probably a good idea to rotate passwords at least once a year. This also ensures you catch accounts using outdated information like previous phone numbers or email addresses that you may want to update.

The complexity of passwords created by a password manager means they're much less likely to ever be guessed; however, if you accidentally reveal a password, or if an online account is breached, that password should be updated **immediately**. Since the password is created and remembered by the password manager, changing a password often will not make it any harder to manage or remember.

Recommended Password Managers:

- Bitwarden
- 1Password
- KeePassXC

Disable Voice Assistants,

Alexa, Siri, Google, turn them off. Unless you need to use voice controls for accessibility reasons, avoid using voice or AI assistants. While there are reasonable precautions taken to keep voice processing data on the device, unless you're using an open-source solution, you have to take the developer's word that they are not sending or selling your data.

Further, for any kind of voice activated technology to work, your device's microphones have to be on some, or all of the time. This is necessary for these assistants to respond to voice

commands like: “Hey, Siri,” “Okay, Google,” “Alexa,” etc. They have been known to misfire and record sensitive conversations by accident. If your device allows it, have the voice assistant triggered by a button-press, instead of a command phrase.

Encryption

In a nutshell, encryption uses the math of large numbers to scramble your data. It uses a created key as the solution to decoding the data. The use of complex numbers means it’s almost impossible to unscramble the data, unless you know the answer ahead of time (the key). There are various ways encryption keys are generated and managed, which is outside the scope of this article, but just know that you can manually create your own encryption keys, or trust an app to do it for you.

The *key* to using encryption safely is to know A) who controls the keys, and B) to maintain those keys safely. Many popular and respected messaging platforms advertise that they are encrypted. The risky part is that they are managing the encryption keys and the servers for you. Meaning that you have to trust them, to trust the encryption. If you don’t control the keys, you don’t control the data.

Encrypt your Communications

Stop using text messages for anything sensitive. Although there have been recent efforts to send text messages with encryption (a good thing!) the trouble with SMS (traditional text messages) is that they are/were often not encrypted at all. Even if SMS messages are encrypted, in some cases the contents of the text messages, and the metadata surrounding them, are visible to the cell phone carriers. These factors make SMS vulnerable to both government requests, and malicious actors at the cell phone companies.

Instead, use trusted, open-source, end-to-end encrypted messaging clients like Signal, Session, Element or SimpleX (see table below).

Encrypt your Devices

Always encrypt your devices with strong passwords. Don’t use drawn patterns or passcodes lower than six digits; alphanumeric passwords are better than passcodes. This doesn’t mean that you’ll need to enter these passwords every time you use your device; there are ways to set timers/other conditions to strike a balance between security and convenience.

Encrypting your device’s storage means that if your phone or laptop is stolen, while the thief could erase your device and resell it, they would still need to erase it to do anything with it. Your data wouldn’t be compromised, it would just be gone. And if they tried to recover the data from the wiped drive, it would still be gibberish because it hadn’t been decrypted. Keep backups of your important data so that if you’re in this situation, you can restore from a backup.

Side Note: There have been laboratory studies showing that encryption keys can be withdrawn from where they are temporarily stored in computer memory; this is known as a side-channel attack (presumably because it gets at the data through a sidelong method). These kinds of attacks typically require special equipment, know-how, and hands on time with the device. A good rule-of-thumb is: *if someone has physical access to your device, they can compromise it given enough time.* Don’t leave your devices unattended around strangers! Even with these theoretical risks, an encrypted device is much more secure than an unencrypted one. It is ***trivially easy*** to reset your user password on your computer if your drive is not encrypted.

Encrypt your Data

While it's important to encrypt your drive/Operating System, it's also possible to encrypt specific files or folders in software vaults. This is sometimes handled by the OS through password protection of a file or folder, but there are also programs that create vaults with specific characteristics, like VeraCrypt.

VeraCrypt can be used to create a virtual drive (folder) which is protected by strong encryption, locked with a password. VeraCrypt can also be used to hide files in such a way that if you enter one password, it shows one set of files, but if you enter a different password (like if someone is looking over your shoulder) it will show a different set of files. It will also make it difficult to see how much of the vault space is used for actual files, and how much is random.

Backup Important Data

There are two (2) important rules to remember when backing up your files.

1. Data that is not backed up, does not exist!
2. Data is not backed up unless you have three copies of the data, and one copy of the data is off-site.

An off-site backup could be a cloud storage solution that you trust, or it could involve copying data onto a drive and mailing it to a friend or family member. Off-site backups are very important in the case of burglary, fire, or some other emergency that removes or destroys both local copies of your data. Another important benefit of backups is that when data is backed up and stored separately, if data is lost, stolen or encrypted without your permission, you can switch to another backup, and continue on with life.

Change Your Software

While hardware certainly is an attack service, most of the privacy risks come from the software we run on our devices. The operating systems installed, and the programs we use every day, especially web-browsers. Changing to free, open-source alternatives can help protect your data, save money, and secure your systems.

Prefer Open-Source Software

Wherever possible, use only open-source software. Open-source software makes its source code available for anyone to review and to suggest improvements. It can be audited and has nothing to hide. Typically, anyone who wants to change the code can, but they have to give credit to the original, and they have to transparently tell future reviewers what they changed. This transparency means that that security flaws are caught quickly by the community, and if a program or operating system is trying to do something shady, everyone will see the changes and stop using the software. Although the next parts of this document are targeted toward Linux and Android, many open-source programs are available on Windows or macOS too. If you get into the habit of using open-source, cross-platform software on your current operating systems, then switching to another operating system is less of a hassle.

Examples of this in practice would be: use Firefox, or a de-googled version of Chrome (Brave is a good alternative); prefer LibreOffice, or OnlyOffice, over Microsoft Office; instead of Photoshop use GIMP, etc. In the "Further Reading" section, we provide resources for finding alternative software.

This preference for open-source should include your operating system on your computer and phone. Switch to Linux and Android, respectively. More specifically, use a modified version of Android like LineageOS or GrapheneOS. More on these options below.

For Computers – Linux

You may have heard of Linux. Probably, though, you have some preconceived notions about what it is and who uses it. Maybe you've heard it's what hackers prefer, or that you have to be a huge geek to understand how it works, or that your software won't run on it because no one writes software or games for Linux. While it's true that many in the IT field use Linux, and it is a favorite among geeks, it's not nearly as difficult or inconvenient to use as people think, and it's getting better every day. You also have probably used something running Linux without even knowing it. Android phones run a version of Linux, so do many smart TVs and appliances, and *most of the servers that run the internet.*

So what is Linux? Linux is a free and open-source operating system introduced in the early nineties. It was heavily inspired by UNIX, and its tools and functions are structured in a very similar way. It started as a research/hobby project and was intended to give people a free alternative to the expensive, proprietary operating systems of the time. Because it is free, and because the code is open-source (available to anyone), anyone can learn it, and make suggestions to improve it. Because of its flexibility and transparency, it was quickly adopted by IT professionals and is actively developed and improved to this day. Eventually, certain companies and institutions wanted to make Linux easier for average computer users. This led to the development of "flavors" or "distributions" of Linux with graphical tools and familiar layouts included on the CD (or USB drives now). The most popular of these flavors would be Ubuntu, Fedora, and Arch. There are sub-flavors of each of these, but they all aim to make Linux more convenient and accessible for regular computer use. Unlike macOS or Windows, no company owns Linux. Anyone can download and install it on their computer, and it is compatible with the hardware from most laptop and desktop manufacturers.

All you need to install Linux is:

1. A copy of your distro (flavor) of choice, e.g. Ubuntu. This is an ISO file, and it's free to download.
2. A flash drive you don't mind erasing.
3. A computer to install Linux on (which can replace Windows, but doesn't have to).
4. About 15–20 mins to complete the installation.

There are many tutorials on how to install Ubuntu or other Linux Distros on your computer, but we may create one of our own if there's interest.

Android

Most people know what the Android mobile operating system is, but not as many know that Android uses a Linux kernel at its core, and that much of the operating system is open-source. Google has been the maintainer of the Android operating system for years now, but due to the nature of open-source licenses, many of the components of the operating system have to stay open-source. You can install a completely functional version of android on your phone without using any of Google's software (an AOSP install - Android Open Source Project). Installing Android in this way does require some sacrifices. For example, the Google Play Store will not be included, so apps will have to be installed manually or from a different app store like

F-Droid or Aurora. Likewise, Google Play Services, which controls things like push notifications, won't be present and so these features won't work properly either. Not ideal, but depending on how limited the use of your phone is, this may be enough. Phone, contacts, web-browser, etc. are still included in AOSP.
Most Android phones ship with Google's software included, though, so deciding what and how to install on an Android phone is only necessary if you're installing an Android variant on your phone.

Comparing factory installed Android to iOS, there aren't drastic differences. Both have reasonable security measures in place, but both also require you to place a large amount of trust in Google/Apple/The phone manufacturer. iOS is arguably more secure than Android, but requires you to place most of your trust and control of the device in the hands of Apple. Android on the other hand has more control and customization options. If you leave it stock, you are trusting Google, Samsung, etc. with your data, and some of the control over the device.

What Android devices have that iPhones do not, are the options to install software from sources outside their main app stores, a wider variety of hardware to choose from, and the ability to install alternative operating systems. For these reasons, we advise against putting trust in one corporation (Apple), and choosing an Android device instead, which will allow you to make changes, or not, as you choose (more on that in the hardware section below).

A stock install of Android still allows you to do the following:

- Install free and open-source apps.
- Install software from alternative app stores, or your browser.
- Enable a 2nd user account on your phone.
- Use privacy respecting apps that don't use Google Play Services.
- Have more control over the look, feel, layout and settings of your device.
- Unlock the bootloader to install alternate Android operating systems (**erases device!**)

Android (Rooted)

Rooting Android involves modifying the software so that you gain admin privileges over the OS. The user with complete control in UNIX/Linux is called the "root" user. Not all Android hardware manufacturers make this easy to do. Samsung, for instance, doesn't generally allow this, and in cases where it can be done, sometimes features of the phone stop working as a result. Google and OnePlus are examples of manufacturers that typically do not prevent rooting.

Some may argue that rooting an Android phone reduces its security. From some perspectives, this is true, however there are added benefits to having total control of the software on your device. For example, having root access allows you to remove software installed by the carrier or manufacturer in order to save space, or prevent unwanted surveillance. Having a rooted phone also allows you to install apps which control the networking of the phone at a granular level, or spoof hardware information, making it's harder to fingerprint your device.

Having root access is not required to install an alternative Android OS like LineageOS, but the two aren't mutually exclusive. Accessing and changing the features of the phone that allow root access does require unlocking the bootloader, which will erase the device. Unlocking the bootloader is also necessary for installing an alternative OS. Rooting and installing alternatives to stock Android article subjects of their own. Just know that there are difficulties and advantages to both.

LineageOS

LineageOS (formerly Cyanogenmod) is an alternative mobile OS based on Android (AOSP), with some helpful tweaks and modifications and a focus on security. There are ways to install Google apps if you want, and LineageOS is updated as new versions of Android come out.

CalyxOS

CalyxOS is similar to LineageOS, but they have taken a special interest in privacy and security by including some curated apps as part of the OS image, saving some steps for the user.

GrapheneOS

GrapheneOS is an OS designed around hardening Android, while including Google apps but isolating them from sensitive parts of the operating system. It tries to strike a balance between convenience and security while taking an aggressive stance toward improving and securing Android.

Change Your Hardware

Choose hardware that respects your privacy and is easily serviceable. Don't rely on Apple. You have to trust Apple for your phone or computer to be secure, and they are notoriously hard to repair, meaning you have to trust someone else with your hardware. No matter how reputable a company is, there's always the possibility of things being lost or stolen if you have to ship off your device for repairs. If you want to use Apple products for your personal, nonwork devices, that's your choice, but you should treat them as completely separate.

If you really want to commit to the change, wipe your current devices and sell or donate them to a friend or loved one. Then buy two mid-to-high-range phones and computers (suggestions below). Think of one as your main work device, and the other as a burner/backup.

For Computers

Anything with readily available parts. Dell, HP, Lenovo, Asus. These can often be bought "certified refurbished" online with refreshed batteries and limited warranty. They usually don't require special tools to repair (most iFixit kits will work fine), and most have replaceable batteries/drives. The goal here is that you're not purchasing a luxury device, you're investing in a tool you can control and keep to yourself, performing your own repairs or upgrades.

If you're handy-tech inclined or want to learn, building your own desktop PC is an excellent way to control your hardware, and is often more economical because you can replace/upgrade parts as you desire/can afford.

NOTE: A relatively new computer company, Framework, makes quality laptops with fully replaceable/upgradable parts. If you choose to go the route of purchasing a new computer, I would recommend them. Otherwise, recycle/upcycle common hardware. **Full disclosure**, I (SubNate) know people who own this hardware and who work at the company. They are in no way sponsoring this article, nor do they know I'm writing it. I get no financial benefit from recommending them. That said, some of this article was written on a framework, and my next laptop is also going to be a Framework.

For Phones

The best choices are main-brand Android phones, Google Pixel, Sony, Motorola, and sometimes Samsung. Samsung makes high-quality hardware, but their phones are typically more in the "luxury" phone category, and are often "locked down" similar to Apple hardware (as noted in the previous section).

If you're lucky enough to live outside the US, the most repairable phone on the market is the Fairphone. They don't currently ship to the US, so if you're in the states, you'll need to either import the device(s), or choose another option.

My recommendation for availability and control over the device would be the Google Pixel line. At the time of this writing, the latest models are the Pixel 7 line. Although there are many reasons to distrust Google (like any big tech company), they have a strong track record of making reliable, customizable phones with years of software/security updates. They also don't stop people from installing their own operating systems on their hardware. If possible, buy the phones used or outright. Don't enter into contracts for financing plans with carriers. This allows you to own the device immediately. If you buy the device unlocked, you can use it with any carrier. Carriers are also required to give you unlock codes for your device (to use with another carrier) if the device is paid off or a 12-month contract is complete.

Social Media

Switch to social media platforms that don't ban you just for posting adult content. Porn has always been a strong driver of adoption for new technology. The shopping cart mechanic on websites was started by porn sites. The adult industry has been quick to adopt video hosting, streaming, video chatting, VR technology and yes, cryptocurrencies. This is probably a story you've experienced personally, or will: platforms often gain users because of adult content. Then, once the platform has grown large enough that they have investors and advertisers to please, they ban the adult content and the accounts that share them. Tumblr is a prime example of this. So is OnlyFans, which threatened to ban adult content (basically the reason the site exists) because credit card companies didn't like that it was a porn site. Other social media sites also have strict but unevenly applied terms of service regarding things like nudity, or promoting adult content on other sites. So creators are caught in a catch-22, where the largest numbers of viewers and engagement take place on platforms like Instagram or Snapchat, which can ban your account on a whim. If we abandon these platforms for more democratic, decentralized options (see below), there will be fewer disruptions in business, and a strong message will be sent to these puritanical, patriarchal platforms that we don't need them.

To be realistic, though, we understand that a lot of business generation comes from these mainstream platforms. Our suggestion is to gradually start educating your audience about better alternatives. Your devoted fans will follow you anywhere, and people will always search for porn. Using SFW or "vanilla" accounts on mainstream platforms to recruit users to these safer, more accepting platforms is the ideal long-term strategy.

Alternative Social Media Platforms

The table below lists some alternative, up-and-coming social media platforms that are all free to use, open-source, privacy respecting, and have NSFW servers, or are relaxed about NSFW content.

Here are some key-terms to keep in mind while learning these new platforms:

- Decentralization - whether a group of servers that share data (federation), or devices that connect directly to each other (P2P), data is **not** centralized on servers owned by one company or person. This makes the platform hard to shut down or censor.
- Federation - A process/technology that allows servers to connect to each other and share data to keep the network running. Instead of one company owning all the servers and hosting all the data, the groups of servers work together to make the data accessible where appropriate. Mastodon, Diaspora, Pixelfed, PeerTube and Friendica all use this technology, and can all talk to each other if they want.
- Peer-to-Peer (P2P) - A type of network where individual users' devices establish connections to each other directly over the internet, or through a P2P network like TOR. This doesn't involve a centralized set of servers. Data is stored on the devices rather than online.
- End-to-End Encryption - a strong form of encryption which means that data is stored encrypted on your device, is sent encrypted over the internet, and is stored encrypted on the other device or server.
- Instance - Another word for "server;" if people host or run servers for Mastodon, Pixelfed, etc. each server is an "instance." The advantage of these platforms is that you can sign up for any server (like one that allows NSFW) and that server can still connect you with users on another server. Pick a server/instance that you like and sign up for that one. You'll still get access to the federated network.

These alternatives can be a bit intimidating at first because they work differently. But the buzzwords and fancy tech aside, here's what you need to know. The social media platforms are designed to be privacy respecting, but they should still be treated as public forums. Pick a server that aligns with what you want (allows NSFW for example), and sign up. Unless a server or group of servers are being assholes, and have been blocked by everyone (which is another benefit of federation), the servers will talk to each other. You can look up and follow users from other servers. This website helps you pick servers from across the "fediverse."

The messaging clients listed below (Element, Signal, Session, SimpleX, Jami, Tox) all allow for E2E encryption, and are either P2P or decentralized as well. These platforms are meant for one-on-one or group conversations and can be considered private as long as you trust the participants.

Mainstream Solution	Alternative(s)
X (Twitter)	Mastodon, Nostr/Iris
Facebook	Friendica, Diaspora*, Hubzilla
Instagram	Pixelfed
Snapchat	Signal, Session, SimpleX
Skype/Discord	Element, Jami, Tox
YouTube	LBRY, PeerTube
Reddit	Lemmy

Alternatives/Honorable Mentions:

- SecureScuttlebutt (SSB) - A P2P Social Media app. Connect to your friends' phones/computers when you meet in person and update your newsfeeds!
- Nextcloud - Self-run/self-hostable alternative to Google Drive.
- Cwtch - Activist created, privacy respecting app similar to Signal or Session. Sex work friendly.

Further Reading:

Switching Software - A site listing privacy/ethics focussed software alternatives.
Prism Break - A site targeted at apps and platforms private enough to help slow/prevent government surveillance. "Hardcore" but still accessible and useful.