CYBER SECURITY CHECKLIST

Enable 2-factor authentication for every site or app that offers it, in particular:

- ○ Google (use the “security key” option if you have a YubiKey 4)
- ○ Facebook
- ○ Slack
- ○ Your banking or financial institution

Passwords

- ○ Install a password manager (like LastPass or 1Password)

VPN (virtual private network)

- ○ Use a VPN (like ExpressVPN or NordVPN)

USB

- ○ Buy a USB condom or charge-only USB cable

Encryption & Locking Devices

- ○ Enable device encryption on your laptops (MacOS, Windows) and phones (Android)
- ○ Lock your devices (PIN, pattern, any are fine)
- ○ Mobile phones
- ○ PCs and laptops, so that they lock after some period of inactivity

Web, Messaging, etc.

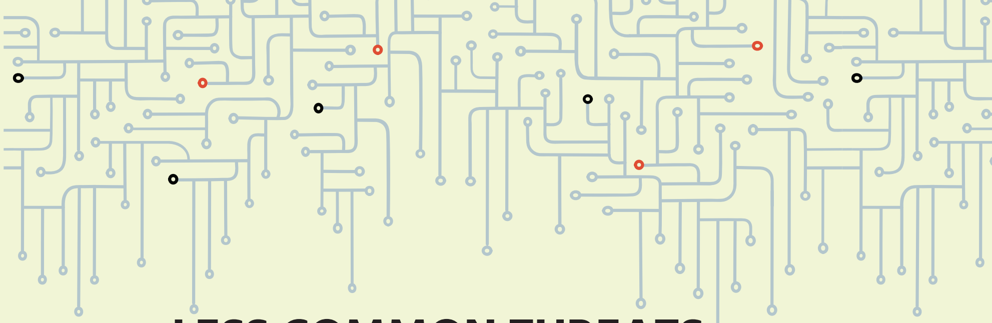
- ○ Use a well known browser like Chrome, Mozilla Firefox, or DuckDuckGo
- ○ Install Signal (Android, iPhone) or WhatsApp (Android, iPhone)
- ○ Enable “click to play” in your web browsers
- ○ Uninstall your virus scanner
- ○ Uninstall software you don’t use

RULES TO LIVE BY

- Never plug your phone into an untrusted USB port
- Avoid sharing USB devices between computers
- Buy a burner phone (and maybe laptop) when traveling to some overseas countries
- Turn off wireless technologies when you aren’t using them
- Use caution when following links in e-mail
- Use encrypted text messaging software instead of SMS
- Keep your software updated
- Consider a smaller, cheaper computer, like a Chromebook, if you just want to use the web

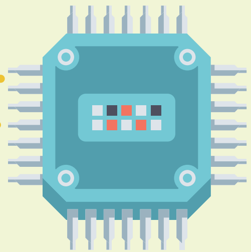
LGBT
TECH

IN DETAIL



COMMON THREATS

- **Phishing.** E-mail is not authenticated. Just because it looks like it came from your bank, or your best friend, doesn't mean that it did. "Your account was locked due to suspicious activity. Give us your account number to get it unlocked."
- **Your Facebook friends.** Even if your account is well-protected, how many of your friends use 2-factor? "Hi, I'm stranded in Rome and my credit card is frozen! Can you wire me some cash?"
- **Identity theft.** Few organizations protect data properly, and sufficiently determined attackers can exfiltrate it even when they do. PII and password databases are compromised all the time. Even if you get your account back, the things it contained might be unrecoverably lost (e-mails, documents, money). This can also occur through theft of your own devices.
- **Password re-use.** Without 2-factor, and given all of the password database compromises, using the same password on multiple sites basically guarantees that someone out there knows the username and password to many of your other accounts.
- **Software vulnerabilities.** Sometimes even legitimate, HTTPS-protected web sites are compromised, such as through ad networks. If a new exploit is discovered and your browser has not yet been updated to address it, your computer can be compromised. Any other software that can be accessed over the network (including many virus scanners) are at a high risk of remote exploitation.



LESS COMMON THREATS

- **Spear phishing.** Imagine "Hi, so-and-so! Had a great time at the lake last weekend. Remember that site I texted you last week? This one is actually better: ..." except that every part of that sentence was true because that's how much research they've done. And so of course you click the link.
- **Man-in-the-middle.** Never trust the network. If a web site doesn't have a green "https" indicator, every network element between you and the web site has the opportunity to intercept or change what you see or send.
- **Wireless.** Every method by which you can remotely interact with your devices is a method that an attacker can do the same: WiFi, mobile (baseband), Bluetooth, NFC
- **Wires and connectors.** Everything you connect to your computer can potentially infect your device with malware, and vice-versa: USB devices of any type, ethernet, even DisplayPort/DVI/HDMI and conceivably even VGA (DDC).
- **Physical access.** It takes just a second for a well-equipped attacker to compromise a device they have physical access to.

LIVE YOUR BEST LIFE

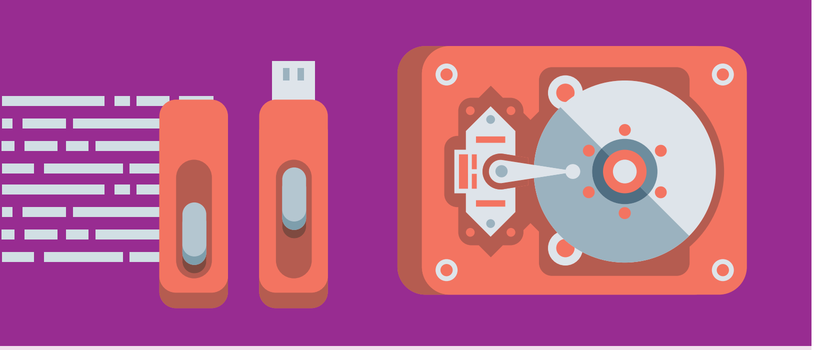
USE 2-FACTOR AUTHENTICATION

Enable 2-factor support for all sites that allow it right now, especially Google, Facebook and GitHub. This often involves installing the Google Authenticator app, and using it to scan a secret barcode on the web site to link the two together. You'll then use the one-time password supplied by this app, or an SMS message, to log in to the site in the future.

For maximum security, buy a YubiKey 4. Enable the 2-factor "security key" option where it's available (Google, GitHub, Dropbox, and probably others). This renders your account immune to phishing. If you get the NFC-capable YubiKey and have an Android device, you can also use the YubiKey Authenticator app instead of Google Authenticator to keep your 2-factor secrets even secreter (and more portable).

✓ **Enable 2-factor on Google (security key)**
✓ **Enable 2-factor on GitHub**

more info on YubiKey on page 3



USE A PASSWORD VAULT

Install LastPass or 1Password in your web browser and phone. This gives you unique passwords for each site, and applies reasonable protection of those passwords even though they're ultimately stored in the cloud. LastPass supports YubiKey for 2-factor. Your master password should be very strong (consider a sentence or passphrase).

NEVER PLUG YOUR PHONE INTO AN UNTRUSTED USB PORT

Always use your own wall charger to charge your phone. Never plug your phone into a random USB port, such as those found at airports or taxi cabs. Only charge your phone from your computer's USB port if you're confident it doesn't have malware. (That's a trick. Your computer probably has malware.)

If you must plug your phone into an untrustworthy USB port, buy and use a USB condom, or use a charge-only USB cable. Newer Android devices default to "charge only" USB port behavior, which may or may not have the same effect. Certainly don't change this default if you want to engage in risky behavior.

✓ Amazon: Charge-only USB cable (doesn't support fast charging)
✓ Amazon: USB condom (supports fast charging)

AVOID SHARING USB DEVICES BETWEEN COMPUTERS

USB devices of any kind can become malware infection vectors. This is especially true for USB thumb drives, but is often true for complex peripherals like printers, and can even be true for devices like keyboards and mice. Remember: you're not just interfacing with the device, you're interfacing with every device that device has ever interfaced with. If you're going to replace your computer, consider replacing cheap peripherals at the same time.

✓ "badusb"

SECURE AND ENCRYPT YOUR MOBILE DEVICE

Secure your mobile devices with a PIN, pattern, etc. Whether you use a PIN, password, pattern or fingerprint doesn't really matter much.

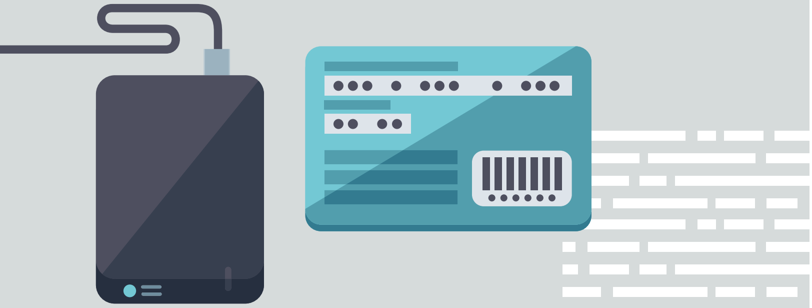
Newer phones encrypt by default. Do this for your laptops. Consider doing it for your desktop as well, if you have one.

Both of these options are chiefly there to protect you and your data against theft. Neither measure will do anything against a well-funded state adversary, but they will effectively stop most all routine thieves.

BUY A BURNER PHONE (AND MAYBE LAPTOP) WHEN TRAVELING OVERSEAS

There are still 70 countries that criminalize being LGBTQ+, if you are traveling to one of these countries it is recommended that you use a burner phone for safety purposes. Don't log in to important or identifying accounts such as email, social media, dating apps, financial apps, etc. Additionally, it's a lot easier for an adversarial nation-state to hack into your phone when you travel to their home turf, where they probably own the mobile infrastructure and know who you are. If you're worried about your phone number changing, use Google Voice. We don't recommend bringing a phone or laptop if you are traveling to one of these countries:

- China
- Russia
- Israel
- Cuba
- Iran
- North Korea
- Ukraine
- Belarus



TURN OFF WIRELESS TECHNOLOGIES WHEN YOU AREN'T USING THEM

Wireless technologies like Bluetooth have been targets for exploitation in the past. Leaving Bluetooth and NFC turned on all of the time increases the chances that someone might discover and exploit such a vulnerability.

BE CAUTIOUS FOLLOWING LINKS OR OPENING ATTACHMENTS IN E-MAILS

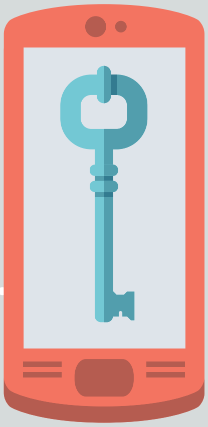
Even if you believe the message is legit, assume every message is a spear phishing attack. Be cautious before following links in e-mails, and consider navigating directly to the web site yourself. If you aren't expecting an attachment from someone, verify with them before you open it.

USE SIGNAL OR WHATSAPP FOR ENCRYPTED TEXT MESSAGING

SMS can be snooped on by anyone that controls the mobile infrastructure you're connecting to. This includes other nation-states, but it is also possible to trick your phone into connecting to someone's fake mobile tower and you'd never know it. This also implies you can't necessarily rely on the phone number as proof that the other person is who they say they are.

Use end-to-end messaging apps for personal communications where you want some assurance of privacy. Signal is great, but WhatsApp has recently incorporated Signal-like features.

✓ Signal (Android, iPhone)
✓ WhatsApp (Android, iPhone)



KEEP YOUR SOFTWARE UPDATED

Prefer software that auto-updates. When an update is released (for instance, monthly OS security releases), take the time to apply the update as quickly as possible. Once word gets out that a vulnerability exists, there is a rush to exploit that vulnerability on systems that are not yet patched. Every time you "remind me tomorrow", you leave yourself open to exploitation for one more day.

Uninstall software that you don't use. Vulnerabilities discovered in software that you don't have installed can't hurt you.

ENABLE "CLICK TO PLAY" IN YOUR WEB BROWSERS

In Chrome, this is in your Settings, under Advanced Settings, Privacy, Content Settings, Plugins. Choose "Detect and run important plugin content" or "Let me choose". This reduces the chance that a compromised site or ad network will invoke an arbitrary plugin with the intention of exploiting a vulnerability in it.

✓ How to Enable Click-to-Play Plugins in Every Web Browser

DON'T USE VIRUS SCANNERS

If you don't engage in risky behavior to begin with, virus scanners are probably more of a liability than a benefit. Virus scanners, by their nature, are extremely privileged pieces of software running on your devices, and they have bugs like any other software. While they can be effective at spotting viruses and other malware, there are viruses and malware that target the virus scanners directly.

LGBT TECH