SKOUT
CYBERSECURITY

Cybersecurity Measures You Should Consider

(A follow-up handout to Tiedemann Advisors' cybersecurity webinar held on May 6, 2021)

Cybersecurity Measures You Should Consider

Three immediate steps to better protect your financial assets

How to increase your cybersecurity on multiple fronts

- ☑ Turn on two-factor authentication (2FAs)
- ☑ Enhance two-factor authentication
- ☑ Use a password manager
- ☑ Increase email security through anti-phishing technology
- ☑ Use a secure messaging app
- ☑ Block trackers and unwanted ads from your browser
- ☑ Use a “Big 6” cloud storage and backup your data to the cloud
- ☑ Increase your home cybersecurity
- ☑ Mobile device best practices
- ☑ Desktop and laptop best practices

Who can help with implementation?

3 immediate steps to better protect your financial assets

Recommendation #1:

Freeze your credit – with all three credit bureaus.

- TransUnion, Experian, and Equifax

Recommendation #2:

Create a new, dedicated email to access your financials.

- Use a dedicated email where you have direct access to your funds and only use this email in these circumstances, never elsewhere. For example, with Tiedemann Advisors, online banking, financial custodians (e.g., Schwab, Fidelity, etc.).
- Credit card companies have strong consumer liability protection, so it's less important to have a dedicated email there. Also, since you don't want to give out this email address to anyone, don't use the same dedicated email with your PayPal or Venmo account.
- Do not forward this dedicated email to your other email account(s), the two shall never meet.
- The goal is to keep this dedicated email address as hidden as possible so it can never be hacked unless the financial institution is hacked.

Recommendation #3:

Use a dedicated computer for your financial transactions.

- For increased protection against viruses and hacking, use a dedicated computer for checking your financials. Do not use this dedicated device for anything else.
- We recommend Chromebook over Apple and Windows computers. (Criminals don't target Chromebooks as much because they're not running on a popular operating system, and Chromebook's operating system also mitigates virus risk by disallowing the installation of traditional programs or applications.)

A **credit freeze** is a way to protect your credit reports from being used by scammers to open new accounts in your name.

Credit freezes are governed by Federal law, offer legal protections and it is free to freeze or unfreeze your credit. To freeze your credit, you will need to contact all three credit reporting agencies and process the freeze.

With each freeze you will get a PIN number. **Please be sure to keep this number as this is the number you will need to unfreeze your credit for any transaction you initiate that requires a credit check.**

Be aware that while freezing your credit is immediate, the process of unfreezing it may take up to three business days.

How to increase your cybersecurity on multiple fronts

SKOUT
CYBERSECURITY

Turn on two-factor authentication (2FA)

Passwords are the #1 course of compromise, and therefore one of the most important steps you can take to increase your protection is setting up two-factor authentication (2FA). This protocol requires you to type in a password and also provide one other piece of proof that you are who you say you are before you can log in to a service. One of the more common 2FA methods in use today employs six-digit verification passcodes that are sent to your phone via SMS (text message). When a unique scramble of numbers shows up on your phone, you type them into the browser along with your password at the login screen.

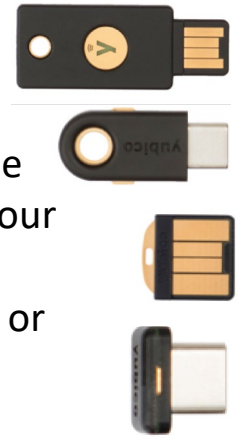
- Bias your choices to apps and cloud providers that support 2FA.
- If a site supports a “Security Key” or “Universal Second Factor,” follow instructions to set up your Yubikeys and Authy for added protection. (see side bar and following page).
- Google has the strongest support for a variety of strong authentication options.

Any 2FA security is better than none. However, 2FA through SMS codes are not without risk as they may be defeated by focused attackers.

Using Yubikeys for your desktops and laptops and a mobile 2FA app like Authy on your mobile device will provide added protection.

(see next page for more information).

Enhance two-factor authentication



Use a Yubikey for added 2FA protection on your desktop and laptop

For increased 2FA security, instead of having a code sent to you via SMS or generated by an app on your phone, use a ***YubiKey***. Each Yubikey device has a unique code built into it, which is used to generate codes that help confirm your identity. These types of keys are **phishing proof**. Even if someone tricks you into giving out your password and intercepts a 2FA code sent to your mobile device, they'd be hard pressed to snatch an actual key off your keychain or from your computer.

We recommend buying two or more Yubikeys: 1 large one to put on your keychain and 1 small to keep inserted in a USB slot.

Use a mobile 2FA app like Authy instead of having the code sent as an SMS

In cases where Yubikeys are not an option or if you prefer the convenience of using your phone, get your 2FA code from a two-factor authentication app on your mobile device rather than having it sent to you via SMS. Apps like Authy or Google Authenticator generate something called a Time-based One-Time Passcode (TOTP) directly within the app. So even if an attacker tricked your cell service provider into completing a SIM swap, they still wouldn't have access to your authentication codes. The data needed to generate those codes remains on your physical device, not within the SIM card.

While Authy and Google Authenticator are compatible and similar, we recommend ***Authy*** because it doesn't lock you into a single phone. (Authy can also be used wherever Google Authenticator is recommended).

Use a password manager

In addition to 2FA, to prevent compromised passwords from being so damaging, you should be using unique passwords on every website. These should also be strong passwords – long, unpredictable passwords that contain numbers and symbols. However, remembering so many complex passwords can be challenging, and this is why we recommend using a password manager like ***LastPass*** or ***DashLane.***

Best practices when you use a password manager:

- As you visit various sites you already use, allow the password manager to manage the password for you when it prompts you.
- If you are re-using the same password across multiple sites, have your password manager set a new / random password for you. **Having a machine-generated long and complicated unique password for every site that you never have to know should be your objective.**
- Start **lying** on account recovery questions (e.g., "What's your mother's maiden name?") for your accounts. Keep notes of your questions and answers in your password manager.
- Use the sharing feature in the password manager to share select passwords with family members and colleagues.

Setting up a password manager

Use a really long passphrase that you have never used anywhere else to get into your password manager.

Install the password manager as a browser plug-in and on your mobile devices so that it will automatically fill passwords into websites and apps.

If you are using Yubikeys, set up the password manager to work with all your Yubikeys.

If you are using Authy or Google Authenticator, you can set up the password manager to support a one-time token code.

Increase email security through anti-phishing technology

Since email is often used to reset passwords and to confirm your identity for many online services, protecting it against phishing attempts is a priority. Phishing is the most popular route to get access to your information. Phishing attempts have become so sophisticated that it's hard even for security professionals to spot them.

While major email providers integrate some anti-phishing technologies, you may still consider licensing anti-phishing technology like ***INKY*****.** INKY offers an automated installation called "Phish Fence" for both individuals and small businesses.

Phishing attempts usually trick you into giving your password out by:

Tricking you into logging into a fake website and as a result getting your password

OR

Tricking you into running an application, macro, etc. on your computer and then getting your password

Use a secure messaging app

Messaging apps make it easy to communicate and connect with people around the world. However, with new ways to communicate and connect via technology, there are also new ways for your privacy and security to be breached.

It is recommended to use a messaging app that has end-to-end encryption (E2EE) to protect your conversations and files.

Be aware that many apps don't have E2EE or you have to actively opt-in to them. (e.g., Facebook Messenger, Skype, Google Hangouts, Twitter, and with Snapchat only your photos and videos are protected).

While there are also many secured chat options available (WhatsApp, Viber, iMessage, Telegram), we recommend using ***Signal*** for the following reasons:

- It's open, free and written by pro-privacy hackers
- Balances strong cryptography with ease of use
- Use it for: chats, sending files, pictures, short voice messages
- Signal offers encrypted phone calls over data
- Messages can be set to auto-delete (cryptographically)
- Can be paired to a desktop app if you prefer to use a real keyboard and big screen

What is end-to-end encryption?

End-to-end encryption (E2EE) encrypts data and only allows the sender and receiver of the message to decrypt and read messages passed between them. E2EE also prevents apps from storing copies of your messages on its servers.

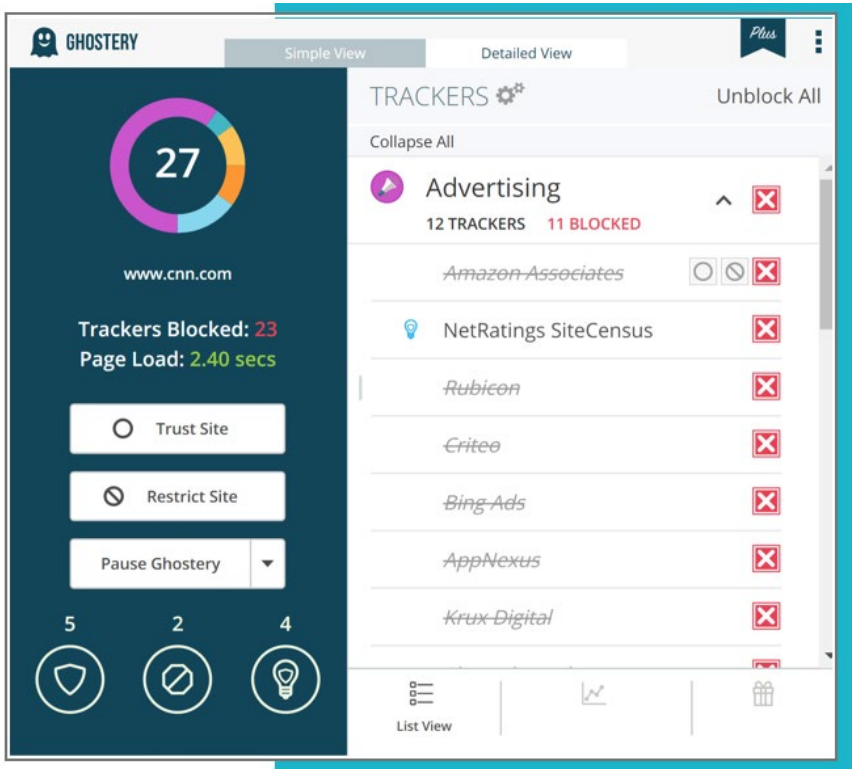
However, keep in mind that end-to-end encryption is not the catch-all security feature to protect yourself from surveillance. Even if you use a secure messaging app, an unsecured device will allow anyone access to your messages.

Block unwanted trackers and advertisements from your browser

Protect your privacy and improve the security and speed of your web browsing by blocking data collection tools (called trackers) and ads using ***Ghostery*.**

You will be amazed by the amount of tracking and advertising once visible. Many sites use trackers to collect information about your browsing habits and serve you ads that might be relevant to you based on this data. Invasive advertising may not only be an annoyance, but compromised advertising providers can be used by attackers to hack your browser.

While using a blocker is a way to protect your web browsing privacy, note that some sites may break when ads and trackers are blocked.



Use a “Big 6” cloud storage and backup your data to the cloud

For data storage and back up, use one of the “Big 6”: Google Drive, Microsoft Onedrive, Box, Dropbox, Apple iCloud, or Amazon AWS. The security capabilities of any single SaaS cloud provider are generally greater than all but the largest enterprises. Cloud storage is generally immune to ransomware wipes.

Best practice recommendations

- Know your security accountability as a customer vs. that of the cloud providers. They can protect you against hackers but can’t protect you against weak passwords or bad file sharing decisions.
- Be aware of where downloads go on your hard drive and use a tool like *BleachBit* to periodically wipe temporary files.
- Use file sharing functions in your cloud storage provider instead of emailing attachments. This may enable tracking as well as some content controls.

Protecting your data against physical loss or theft

As a best practice, you should back your data in case your device gets lost or stolen or if a system crash or hard drive failure occurs.

With cloud storage, backup is “auto-magical.”

In addition to backing your data up in the cloud, you should also protect it by encrypting your entire hard drive using ***FileVault*** (Mac), ***BitLocker*** (Windows), or ***Veracrypt***. Note – this will only protect your data against physical loss, theft and forensic analysis.

Increase your home cybersecurity

HOME ROUTERS

- Many manufacurers ship devices with a single default password for all their devices. Be sure to change the default password to protect access on your internet router.
- Install all available firmware updates and patches for your router and make sure “auto-updates” to firmware is enabled.

WIFI NETWORKS

- Create a Guest WiFi network and connect any IoT devices (cameras, doorbells, Sonos, etc.) to your Guest WiFi network.
- Anyone outside your household should only have access to your Guest Wifi.

HOME AUTOMATION

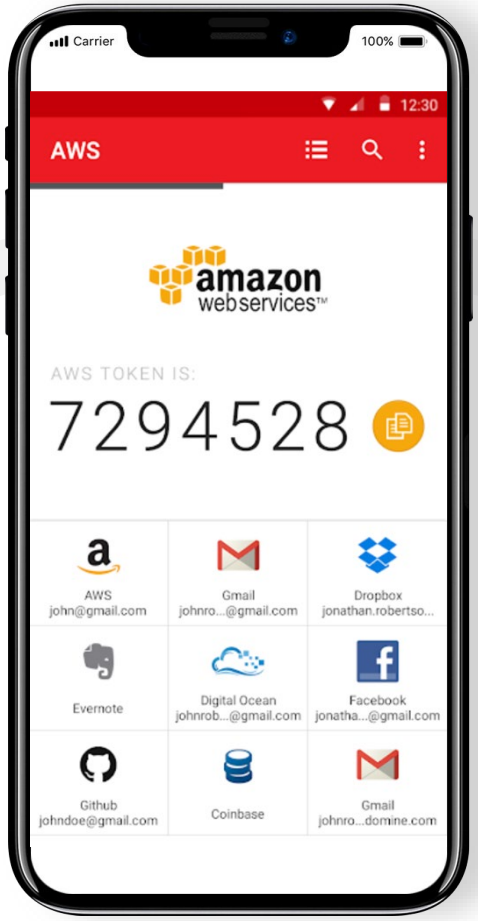
- Ensure all of your smart devices are running the most updated version of software.
- Only use larger companies (e.g., Nest, Amazon) that have a proven track record in securing, monitoring, and maintaining their IoT equipment. Don’t buy any home automation from “tier 2” vendors.

Mobile device best practices

Replace your phone as soon as your vendors stop providing security updates (generally 3 years after the release date)

"**It pays to pay**" – Paid apps are less likely to be malicious or monetize themselves by selling your data

Don't install apps from outside of the vendor-managed app stores or apps from unknown vendors / providers



Be keenly aware of the permissions that apps require. Think critically… "Why does this game need to track my location?"

Turn on auto-update on your device's operating system. Reboot your phone when prompted.

Mobile device security products are mostly a waste of money

The mobile device security hierarchy:
IOS > Android

Desktop and laptop best practices

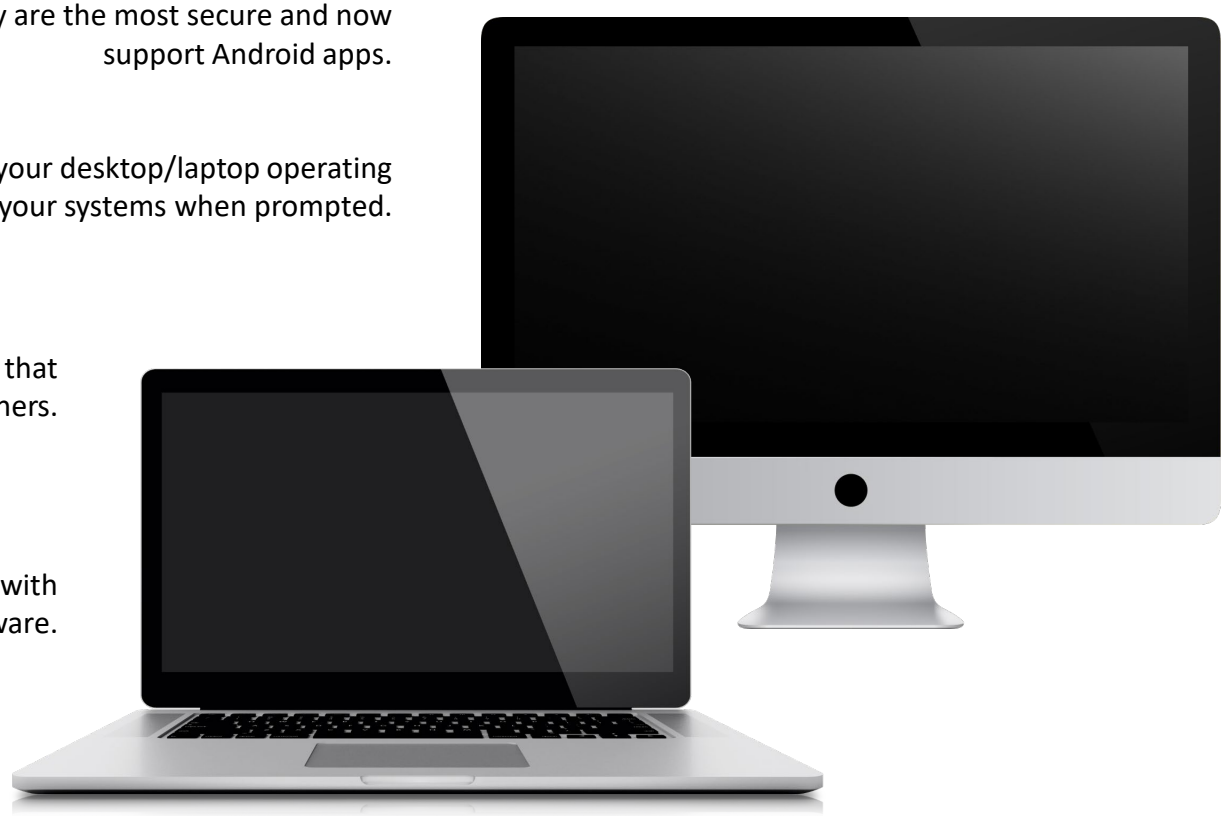
If you can live inside a web browser, buy and use a **Chromebook**. They are the most secure and now support Android apps.

Turn on **auto-update** on your desktop/laptop operating systems. Reboot your systems when prompted.

Don’t install apps you don’t need or that don’t come from reputable publishers.

Don’t pirate software! It’s loaded with malware.

Minimize your public “footprint” on social media and the like - less info makes you and your service providers harder to phish.



Use Chrome as a browser and don’t visit “bad neighborhoods.”

An anti-malware product on Windows is a must. The built-in Windows Defender isn’t bad. But you may also consider **Cylance.**

What about tablets?
If your goal is to optimize your security and privacy, we generally don’t recommend using tablets. If you do use a tablet, we encourage you to exercise caution and follow the best practices for mobile devices (previous page).

If you have a small business, consider a Managed Security Services provider like **SKOUT Cybersecurity.**

Who can help with implementation?

You can simply enlist the help of local support services like Geek Squad.

Service providers such as Geek Squad can help you configure your devices and implement advanced security measures:

- Updating firmware and software on all of yout Internet-connected devices
- Creating and properly configuring Guest WiFi networks
- Updating passwords and implementing 2FA across mutliple services
- Enabling hard drive encryption and storing the encryption keys
- Configuring Yubikeys
- Configuring password managers
- Installing and configuring 3rd party anti-phishing software