Hacks don't only happen to others!

Actively protect your online life

A practical guide for everybody

Nowadays, almost everyone spends a significant portion of their life in the virtual world, using various online platforms such as email, social media, and online banking, among others. This guide is designed to assist you in safeguarding your online presence and preparing for a possible major hack that could potentially wipe out all your cyber life, make your life miserable, not to say get your lifetime savings disappear.

Don't think it affects you? Listen to the testimonial video from the Wall Street Journal. Too many people believe it only happens to other people. It could happen to you!

This guide is intentionally brief for quick reading and implementation of recommendations. It has been written for non-technical people.

You can never be 100% protected, but by following the advice in this guide, you can minimize the risk and have ways to recover in case of a hack.

A must watch video for everybody: Wall Street Journal, your passcode unlocks far more than just your phone.

https://www.wsj.com/tech/personal-tech/apple-iphone-security-theft-passcode-data-privacya-basic-iphone-feature-helps-criminals-steal-your-digital-life-cbf14b1a

Have an inventory of all your accounts

It is highly recommended to maintain a record of all your important online accounts such as emails, social media, online storage (e.g., Dropbox), productivity tools (e.g., Microsoft Office 365), and online banking. Creating a list is a good way to do this. You can use Excel for this purpose, protect it with a password, and avoid storing it on online storage to ensure added security.

Put a note in your calendar to review this list and update it at least once per year. Ideally 2-3 times per year.

Store that inventory in a physical safe if you have one, to which a very limited number of trusted people have access.

To effectively manage each account or service, it is important to keep track of the following information:

- Name of the provider (e.g., gmail.com)
- Description of the service (e.g., online email service provided by Google)
- Location of the service (e.g., in the United States)
- Confidentiality of the data stored on that service (e.g., confidential)
- Criticality of the service for you (e.g., your eBanking is high criticality, Spotify is low criticality)
- Strongness and uniqueness of password
- Type of security in place (e.g., login only, 2FA)

- Backup offered by provider (i.e., is the provider doing backups for you, or not)
- Backup internally (i.e., do you backup this data yourself. If you do, make sure it's protected correctly)
- Encryption at rest (i.e., is the data encrypted when it's stored)
- Encryption in transit (i.e., is the data encrypted while being communicated, e.g., while in communication on the Internet)

Do not store your passwords on that list!

Review your list a few times yearly to keep it updated and determine if additional security measures are necessary.

Prepare for the worst!

It is common to hear stories of individuals passing away and their loved ones being unable to access their online accounts, including social media platforms like Facebook and even e-banking services. To prevent this from happening, it is essential to keep a separate list of your account information and passwords in a secure location. This will ensure that your loved ones can access your accounts should you pass away. Keep this in a very secure place, accessible only from people you trust. And don't forget to keep that list up to date.

Write this list by hand, do not store it electronically. And keep it in the most secure place (e.g., a physical safe). Do not forget to keep it up to date if you change some of your passwords.

Protect your phone and tablet at all costs

You should always have a strong passcode for your phone, with at least eight characters. This will make it much harder for someone to shoulder surf and gain access to your device. Do not use a 4-digit passcode!

On an Apple device, go to >Settings >Face ID & Passcode >Change passcode >Passcode Options at the bottom of the screen >Custom Numeric Code (or Alphanumeric Code)

Set the auto-lock to maximum 3 minutes. The shorter the better. Whenever you stop using your phone, instinctively lock it!

>Settings >Display & Brightness >Auto-Lock

You must understand that if someone has access to your phone, they will have access to most of your digital life. Including using the authenticator for 2FA that is probably on your ... phone!

Your phone is probably the one thing you must protect at all costs!

When you unlock your phone using Face ID or a fingerprint, there is no risk involved. However, if you use a passcode, it is important to ensure that no one is watching you entering it, and that there are no cameras recording you as you type.

You think "don't be paranoid? Actually, you must be!

Protect your computer

You need to do the same with your computer: put in a strong password, set the auto-lock to maximum 5 minutes,

Whenever you leave your computer, even for a minute, lock it! Even at home.

Never leave your computer in any public transport or a plane. NEVER!

Use a privacy screen when working in an open space.

and encrypt the hard drive. Whenever you stop using your computer, instinctively lock it!

Use strong passwords

A secure password should contain at least 12 characters, including a combination of uppercase and lowercase letters, numbers, and special characters. You can make it a passphrase. The longer, the better.

Do not use guessable information like your birthdate or the name of your children. Avoid words from the dictionary.

Check how strong your password is here:

Do not write down your passwords.

Do not use the same password across accounts so that if one is compromised, you do not compromise multiple accounts.

Consider using a password manager tool or use an "algorithm" that only you know to build and remember your passwords. Example of an algorithm: take the last letter of the name of the service in upper case, add 75, add "Zurich" because you live in Zürich, add "ilis" for "I Live In Switzerland", add $$. For your Apple account, the password would be *E75Zurichilis$$*. Cracking this password would take 15 billion years! Want to make it even stronger, add another two-three digits at the end.

Use 2-factor authentication (2FA)

Set up 2FA for all your accounts, especially your email accounts and eBanking accounts. If someone gets access to your email and there is no 2FA in place, she can probably take control of your cyber life in a few minutes.

As much as you can, avoid 2FA via SMS. Use an authenticator whenever possible.

Most authenticator solutions (e.g., Google, Microsoft) do not offer an alternative password. This is a major security gap we hope they will close soon.

Someone who is overly cautious may choose to use a separate device solely for their authenticator, despite the inconvenience, in order to maximize security. FYI, I am not going that far!

Protect your Gmail account with 2FA:

Protect your online banking

Setting up two-factor authentication (2FA) for your online banking is essential.

If your online banking does not support 2FA or a mechanism similar to 2FA, you should not use it!

Do not store your online banking ID on your computer, phone, or tablet. Make sure you type it each time you want to log in!

Make sure your phone and online banking pin codes are different.

For an added layer of security, avoid having your online banking app and authenticator on the same device.

Do the same for your Credit Card application if you use one.

Backup your important data

As you increasingly store your data in the cloud with some history management, it is still important to ensure you have your own backups.

Back up frequently your important data. At minimum twice per year. Ideally continuously or every monthly.

It's highly recommended to regularly backup your files, photos, and videos on an external hardware device. Avoid online backups, as they may be compromised if your online identity is hacked or if someone takes control of your data. For added security, encrypt the backup drive and secure it with a password. For even more security, store the drive in a physical safe.

Install an anti-virus/malware on your computer

Protect your computer with a security solution (anti-virus and anti-malware). Even if you have an Apple Macintosh! Make sure that all users in your house do the same as the weakest link is the problem!

Do not trust anyone

Never divulge your credentials (username and password) to anyone. Nobody else but you needs them! NEVER DIVULGE YOUR CREDENTIALS.

Do not click on links or open documents you do not trust.

Always make sure that the email is coming from a legitimate email address. Check for typos in the email name.

Use a virtual private network (VPN) when required

Use a virtual private network (VPN) to hide your internet address. However, it is important to note that private networks may not always guarantee anonymity during court investigations.

Public Wi-Fi.

By default, do not trust public Wi-Fis and make sure they are legitimate. Use a virtual private network to protect yourself over a public Wi-Fi.

Recover your stolen email account

This might not be possible. Once it is stolen, it might be gone. To avoid that, make sure you have 2FA in place! So that, they cannot change your email password.

If you believe your email account has been compromised, immediately connect, change its password (and enable 2FA it's not yet done.)

Have recovery codes

Most online solutions and tools that offer 2FA propose to save some recovery codes. Make sure you store them in a very secure place, and that they are available on paper in case of a total meltdown of your online life.

Install the latest software releases

Always install the latest releases of the operating systems and software you use. Especially security updates, they should be deployed ASAP. Today, it's very simple on any Mac, PC, iPhone, and Android device. Enable automatic updates.

Have your passwords been hacked?

To check if some of your passwords have been released online, you can use the website https://haveibeenpwned.com. For the accounts appearing on that list, make sure you immediately change their passwords.

Recovering from a hack – Ransomware

If any of your devices have been infected with ransomware despite following these guidelines, the best course of action is to completely reinstall the affected devices and restore from your backups. Should you require assistance, consider seeking help from a professional firm.

Recovering from a hack – Stolen accounts

It might be complicated or impossible. The best solution is to protect your accounts with strong passwords, 2FA, and by keeping your phone secure. Should you require assistance, consider seeking help from a professional firm.

Privacy

This document is not about protecting your privacy. But two things you must understand:

Make sure to check the privacy settings for every online platform (e.g., Facebook, Snapchat) and understand what they do with your data.

Put a camera cover on all your devices. It is almost impossible on an iPhone and iPad. So, just keep in mind that your cameras could be hijacked.

Continue to educate yourself.

The Social Dilemma documentary

The Great Hack documentary

Online Life Security Checklist

- □ I have an inventory of all my online accounts
- □ My loved ones know where to find the information about my online accounts, including their passwords
- □ My phone has at least an 8-digit passcode
- □ My phone auto-locks after a maximum of three minutes
- □ My computer is protected with a strong password
- □ My computer auto-locks within a maximum of five minutes
- □ My computer's hard drive is encrypted
- □ I use strong passwords across all my online accounts
- □ I do not reuse the same password across my online accounts
- □ All my important online accounts have 2FA (or equivalent) in place
- □ My email accounts have 2FA in place
- □ My online banking has 2FA in place
- □ My online banking ID is NOT stored on any of my devices. I always have to type it in
- □ My phone and online banking have different PIN codes
- □ My online banking authenticator is on a device that does not have access to my online bank/no online banking app (optional)
- □ I back up my important data frequently
- □ The hard drive used for my backups is encrypted and password-protected
- □ The hard drive used for my backups is kept in a safe location
- □ I have recovery codes when available, and they are stored in a very safe location
- □ All my computers have an up-to-date security solution installed
- □ When possible, my cameras have a cover