Basic introduction to digital security

Opportunity Network for At-Risk Writers, Artists, Rights Defenders, and Scholars (ONWARDS)

PROBLEM => SOLUTION

PROBLEM #1 => SOLUTION 1.1, 1.2, 1.3, …
PROBLEM #2 => SOLUTION 2.1, 2.2, 2.3, …
PROBLEM #3 => SOLUTION 3.1, 3.2, 3.3, …
…

USUALLY we see the opposite (((((

https://cpj.org/2025/04/cpj-safety-advisory-traveling-to-the-us/

https://freedom.press/digisec/blog/border-security/

https://www.eff.org/

https://ssd.eff.org/ - old classics, instructions by Electronic Frontier Foundation

https://digitalfirstaid.org/ - Digital First Aid Kit

https://www.shira.app/ - Interactive phishing training

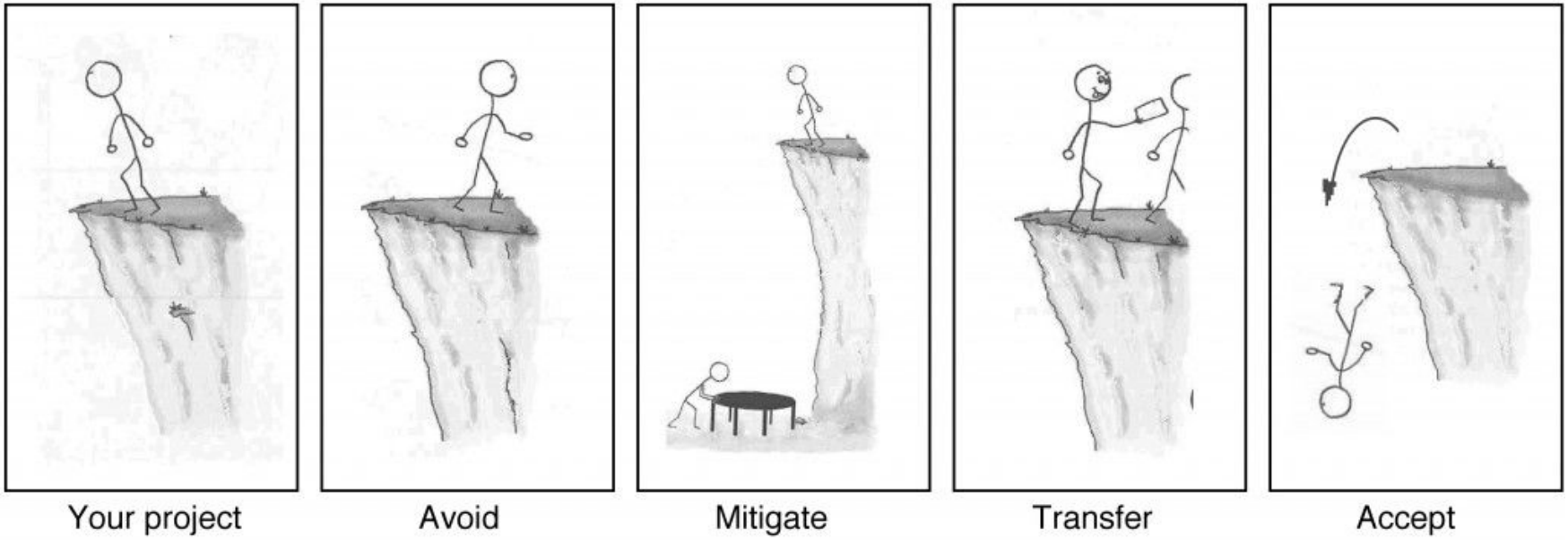
https://freedomlab.io/courses/managing-risks-safety-and-security-in-human-rights-work/ - online course by OSCE ODIHR

Risk assessment

1. List of important information assets = **what to protect** (specific sensitive data, devices, processes, accounts, messengers etc)
2. What bad could happen to each of the assets? What do we want to prevent? What is the probability (1-low, 2-medium, 3-high) and impact (1-low, 2-medium, 3-high)?
3. Rank the list from the highest to the lowest [probability X impact] = our list of the risks

Risk treatment

What could be done about each of the risk: Avoid, Mitigate, Transfer, Accept



Selecting/developing security measures

Risk 1 (the highest one) - security measure 1, measure 2, measure 3

Risk 2 - security measure 4, 5, 6, etc

Risk 3 - accept (for example), do nothing

Risk 4 - avoid, don’t use the platform / don’t do the project / don’t travel to a country X, etc

Risk 5 - buy insurance for example (transfer/share)

…

No time for all this, need a simple solution?

1. Find support/assistance
2. Implement the recommended security measures; ask for support if needed
3. Repeat every 12 months

The **expenditure** on relevant controls is expected to be proportionate to the perceived business impact of the risk materializing.

Risks can be accepted if, for example, it is assessed that the risk is low or that the **cost of treatmen**t is not **cost-effective** for the organization. Such decisions should be recorded.

Device security: how to secure data from physical confiscation/theft

- Windows/MacOS/iOS/Android updated to the latest versions = new devices if not supported
- Full Disk Encryption - BitLocker / Filevault
- Strong password to unlock device
- Biometric unlock - depending on the context
- Lock screen notifications - content off
- Autolock (after how long inactivity?), manual lock (Win+L, close the lid)
- Flashdrives, harddrives, etc - don’t forget

Professional IT support usually needed

Device security: how to secure data from malware, spyware

- Windows/MacOS/iOS/Android updated to the latest versions = new devices if not supported
- All the applications updated to the latest versions
- NO pirated software
[- Corporate antivirus + professional monitoring]
- Lockdown mode for Apple users - IF there is a risk of targeted spyware
- Google Advanced Protection for Androids

Professional IT support usually needed

The main accounts’ configurations

1. Jurisdiction - trusted
2. End-to-End encryption
3. 2FA (ideally - phishing-resistant MFA) / registration lock / Two-Step Verification
4. Strong password (long, unique, no personal data)
5. Active sessions / logins / devices
6. Third-party applications (login with Google, etc)
7. Google Advanced Protection Program
8. Auto-delete messages (Signal, other messengers)
9. Phone number’s jurisdiction

We used to be told to look out for scammers and identity thieves. Who else is looking for our information? What are they looking for?

How do governments gather their data about us? Do they target specific individuals and then dig into their digital lives, or do they do broad sweeps and follow leads from what they find?

Are we being monitored in real time, or only when we are trying to cross a border, apply for a visa, apply for a job, etc.?

What sort of online content can cause legal problems for me, especially if I am living on a visa in the United States?

Is it possible to delete my history on X, Facebook, Instagram, TikTok, LinkedIn, WhatsApp, or other platforms? What are the risks of doing this?

Can I download and securely save my social media history?

Should I have alternate social media identities?

How do I recognize phishing attempts on social media or email?
https://www.shira.app/

What should I do if my social media accounts are being hacked? How about my email?

Should I use a secure browser? Does private mode work?

What makes a communication platform secure or not secure?

Are there secure platforms for email communication? Messaging? Voice communication?

Should I use secure platforms for certain types of communications and use less-secure platforms for others?

Should I have a burner phone?

Should I have a travel laptop?

Is there anything I can do to limit third-party access to content I have already shared with others (e.g., emails, SMS messages, Messenger messages, Instagram messages)? - sometimes “delete for all users”

How secure are money transfers? What are the best ways to move money internationally?

What should I know about Google Drive, Dropbox, and other widely available file storage systems?

What sort of locally stored content can cause legal problems?

What is the best way to wipe a hard drive? - full disc encryption + format after

How can I securely preserve my digital writings, music, or images?

How can I safely store sensitive digital information (e.g., passwords, bank account numbers)? - https://1password.com/

How can I safely store physical items (identity cards, birth certificates, marriage certificates, passports, work certificates, property titles, wills)?

Thank you!