This booklet is made to help identify what you might have to protect in your digital world. Read in its entirety, you will find each persona has characteristics you may share, or fears you have heard before. These cartoon animals are not made to be the focus; it is the threats they face and solutions they suggest that are important.

We present here only the beginning of the conversation: a place to start. If you are interested in implementing the solutions, or want to ask questions about your personal context and challenges, contact the **Access Now Digital Security Helpline** at [help@accessnow.org](mailto:help@accessnow.org), or visit the resources listed on the back of the book.

---

Access Now is an international organization that defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.

For more information or assistance, please contact [info@accessnow.org](mailto:info@accessnow.org). For digital security assistance, contact [help@accessnow.org](mailto:help@accessnow.org) or visit [https://www.accessnow.org/help](https://www.accessnow.org/help).

---

This work is provided under the Creative Commons Attribution-NoDerivatives 4.0 International licence. To access the full legal text of this licence, please visit [https://creativecommons.org/licenses/by-nd/4.0/legalcode](https://creativecommons.org/licenses/by-nd/4.0/legalcode).
Savant is a journalist communicating with survivors of puppy mills. Savant's sources have secret information about the mill that has the chance to shut it down. Shady characters have already attempted to find out what information that is, so now Savant takes care that all of their communications are encrypted, and when they collaborate on an article, they use encrypted document sharing options as well.

Savant relies heavily on their phone for on-the-go communication. They constantly collaborate with others on their future articles and documents. Savant is known for taking on stories that question the status quo, and they have no shortage of powerful people interested in that work. To mitigate these vulnerabilities:

1. Sources: names, communications, and contact
   Savant encrypts emails to sources from their laptop ensuring the confidentiality of the messages.

2. Correspondence with the editors
   They use encrypted texting and voice apps on their phone to connect with sources.

3. Time-sensitive research
   For chatting on a laptop or desktop, Savant uses an encrypted instant messenger and voice client.

4. Draft documents and articles, sometimes involving collaborators
   Their collaboration work is done through encrypted document sharing.

   When on shared or untrusted wifi (like a cafe), Savant uses a Virtual Private Network (VPN) to securely access the internet.

   When moving through security checkpoints, they turn off their computer to ensure full-disk encryption is active.

   Savant is a journalist communicating with survivors of puppy mills. Savant's sources have secret information about the mill that has the chance to shut it down. Shady characters have already attempted to find out what information that is, so now Savant takes care that all of their communications are encrypted, and when they collaborate on an article, they use encrypted document sharing options as well.
Maya is an activist and blogger who calls attention to the effect of rising ocean temperatures on coast-dwelling penguins. Not everyone agrees with Maya’s work, and her online accounts are often at risk of hacking and defacement. Recently, tensions have increased and Maya is concerned about someone stealing her devices. She has decided to encrypt all hard drives to better ensure the safety of her information.

**What needs protecting?**

1. Research and data, contained on hard drives
2. Online accounts
3. Communications with other activists

Carefully cultivated over years of work, Maya’s online social media accounts and blog are her life. Their integrity is of the utmost importance to her, her readers, and her contacts. Important research, data, and plans are kept on her hard drives, and she fears their falling into unfriendly hands.

To mitigate these vulnerabilities:

- All of her online accounts are guarded by **two-factor authentication**.
- Maya ensures all of her devices have **full-disk encryption** enabled.
- Maya keeps track of what computers have accessed her accounts, and from where, with the **security checkups** offered by Google and Facebook.
- She encrypts all sensitive files, including external media, like flash drives and hard drives.
- Strong passwords are employed on all accounts: over 30 characters, all unique, with numbers and special characters managed with a **Password Manager**.
- Maya expands short urls she finds on social media in order to know in advance where links are going to take her.
- She employs **anonymous chat** to organize events and gatherings.
Julio is vulnerable during his frequent travels due to the unprotected wifi, border checks, and multiple hotels he stays in. He has an open and helpful nature which may make him trust too quickly. His organization is widely known for its work, and he is their public face, often being contacted by strangers for assistance or advice.

To mitigate these vulnerabilities:

1. Julio keeps software up-to-date.
2. He has a password manager where he generates unique, strong passwords with over 30 characters, never using words that can be found in dictionaries, but including numbers and special characters.
3. When on shared or unknown wifi (like a cafe), Julio uses a Virtual Private Network (VPN) to create a secure line to the internet.
4. When reading email, Julio uses caution in opening unexpected links or attachments, unless he has verified the senders’ identity by calling or messaging them.
5. When crossing country borders, Julio turns off his computer to ensure his full-disk encryption is active to prevent unauthorized access to his information.
6. He remembers what is posted outside of work can hurt the NGO as well. He employs mindful posting to ensure what he publishes on his personal accounts cannot be used against him (wary of posting locations, specific dates, home addresses, etc.).

Julio works at a civil rights NGO. Though he does not work directly with clients, he knows his personal habits protect his co-workers and thus, the clients as well. Julio works very hard to ensure his security hygiene is quite good to responsibly care for his organization.

What needs protecting?

1. Financial information, both donors and employees
2. Contact lists of partners and clients
3. Integrity and trust the organization has built
4. Private documents, like client statements and advocacy strategies

Financial information, both donors and employees

Contact lists of partners and clients

Integrity and trust the organization has built

Private documents, like client statements and advocacy strategies

When crossing country borders, Julio turns off his computer to ensure his full-disk encryption is active to prevent unauthorized access to his information.
Jaha does not want her family, or many of her social circle, to know her interests yet. She wants the freedom to explore this possible new side of herself without feeling watched and judged by others. Maya has created a separate self online and does not want to risk public exposure until she is ready, but she still wants to access some material the university has censored.

To mitigate these vulnerabilities:

- **Jaha employs circumvention and anonymity tools** to confuse her identity and avoid censorship.
- **Anonymous chat** lets Jaha connect with others like her.
- **She maintains separate online personas** to divide her personal life from her academic life, taking special care to avoid being identifiable.
- **Jaha regularly clears out her chat histories** to avoid malicious access to previous conversation logs.
- **She uses privacy enhancing browser extensions** to avoid ad-tracking which may reveal some of her interests.
- **Jaha employs mindful posting** to ensure what she publishes online cannot be traced back to her (wary of posting locations, specific dates, home addresses, etc.).

**What needs protecting?**

1. Personal privacy
2. Personal control over identity
3. Access to free flow of information
4. Separation of online personas
RESOURCES TO HELP YOU IMPLEMENT PRACTICES LISTED IN THIS BOOK:

https://ssd.eff.org
https://securityinabox.org

WANT MORE PERSONALIZED ASSISTANCE?

The Digital Security Helpline is a free of charge resource for civil society around the world. It is run by the international human rights organization Access Now (accessnow.org).

The Helpline offers real-time, direct technical assistance and advice to activists, independent media, and civil society organizations.

OUR SERVICES

- Rapid response on digital security incidents
- Personalized recommendations, instructions, and follow-up on digital security issues
- Guidance on the usage of digital security tools
- Support for securing technical infrastructure, websites, and social media against attacks
- Supported languages include English, Spanish, Arabic, French, Filipino, and Portuguese.

HOW TO REACH US

help@accessnow.org

Great news! Your email message has been sent successfully.

Digital Security Helpline
accessnow