Steps to understanding Cybersecurity by Jamie Ruppert

1. Decide if you want to be online. The internet only works well for you if you surrender a certain amount of privacy. The future of online privacy depends on new technology and agreements between users and providers.

2. What does Data Security Mean? Simply put, data security tends to refer to protections involving personal data. Data Security refers to data in general.

3. Cybersecurity involves system interconnections and overall online operations. Data security tends to be regulated and subject to enforcement. Cybersecurity is the ever-arching term.

4. The European Union’s new General Data Protection Regulation (GDPR) expanding and updating the existing EU privacy directive—creates new privacy and data security obligations for virtually every company operating around the world. Watch this future trend.

5. A proxy is a type of computing system that functions as a go-between for your connected device and your web connection. These servers also have their own IP addresses, so transfers can’t be traced directly to your computer.

6. Off-the-Record (OTR) Messaging encrypts the communication channel and offers proper authentication. If you’re on a Mac, Adium provides built-in OTR support. For Windows and Linux, you can use the OTR plug-in for Pidgin.

7. New technology called Blockchain exists as a shared and continually updated database. The blockchain database isn’t stored in any single location. Data is accessible to anyone on the internet because it is hosted by millions of computers on the internet. It would be impossible for hackers to corrupt every copy in every location.

8. A virtual private network (VPN) is a secure and private solution within the wider internet itself that allows users to send and receive data while maintaining the secrecy of a private network. Add a VPN app to your device.
TECHNOLOGY ALONE CANNOT ADDRESS ALL THE CONCERNS SURROUNDING A COMPLEX ISSUE LIKE ONLINE SECURITY. THE TOTAL FUTURE SOLUTION MUST COMBINE POLICY, LAW, AND TECHNOLOGY.

IF YOU ADD COMMON SENSE APPROACHES TO CURRENT TECHNOLOGIES AND FUTURE TRENDS THERE ARE STEPS YOU CAN TAKE NOW TO KEEP YOUR DATA SECURE.

1. Don’t give passwords to anyone. Don’t click on anything until you investigate the identity of the company or individual. A little research goes a long way. If your employer demands passwords to personal accounts, contact the ACLU.

2. Read the Terms of Service (TOS)! You can also use an app that rates the companies TOS. Anything that requires you to agree to the TOS may intend for you to give them access to things you don’t want to share.

3. Use encryption software for all financial transactions. Look for the lock icon on the status bar of your internet browser. If you see a lock the data is encrypted.

4. Use Strong Passwords. Substitute numbers for some words or letters. For example, “I like to eat apples and bananas.” could become 1L2EaAaB.

5. Unplug and turn off any device that has the potential of listening when you aren’t using it. Alexa may only listen for the keyword, but how does she hear the keyword if she isn’t always listening?

6. When you work online, be sure not to send financial or sensitive information over public wifi. Thieves pretend to be public wifi to get your information.

7. Don’t use the “save your password” feature for anything important like bank accounts. If your phone or laptop are stolen, your information would be easy to steal if your device remembers passwords.

8. Keep regular backups, and use wipe utilities to permanently delete all information before disposing of old phones and computers.

The path to cybersecurity is awareness.
References


