How Privacy and Security works

Van Londen
International Data Privacy

Privacy, in many countries is considered a human right. Special accords are made for data privacy. The Electronic Frontier Foundation (EFF) advocates for the free expression and digital privacy of all citizens of the world through their activism, legal work, and software development. Their site provides a list of international data privacy agreements and articles/discussions, such as the EU’s General Data Protection Regulation (GDPR) of 2018. A group of 30 countries (OECD), a group of 47 countries (Council of Europe), and the 27 members of the EU oversee and/or protect the flow of personal data between countries. The APEC group of 21 Asia-Pacific members undertake privacy commitments on a voluntary basis. Under some regulations, countries can fine tech companies for mishandling private data.
Due to a lack of trust and different rules for each country, the EU created the General Data Protection Regulation (GDPR) to give citizens control over their personal data, such as names, addresses, ID names, health profile, income, ethnic groups, etc. Companies as well as their employees who process data are responsible for safeguarding that data to improve speed and reduce costs (by about 2.3 billion Euros). Employees in businesses must communicate their intentions to consumers, allow them to opt in or out of future marketing campaigns, get their consent to use their data, make their data accessible and portable, inform them of breaches, and allow them to erase their data from accounts. If profiling is used, then a human must review the data. Collecting data from children requires parental consent. I
EU GDPR (continued)
If the data will be transferred to non-EU countries then **safeguards must be in place** as part of the design. **Contracts and Data Protection Officers** are also required in some cases, such as for third-party use, search engine advertising, and genetics processing. Small as well as large businesses **must keep records** about the reasons for collecting specific categories of personal data as well as the timeline for removal. They must **have security measures in place** in case of a breach. In cases where risks are high, then an **Impact Assessment** is required, such as with new technology, automated processing, public monitoring, and biometric processing. The cost of failing to safeguard data results in **suspension and fines**.
Online Security

Crash Course: Cybersecurity #31 talks about online security techniques, often called a threat model. They help protect our secret and confidentiality information and property from threats by malicious actors. The integrity of data ensures only authorized people have access to it. A denial-of-service attack, for example, reduces the availability of online websites. Knowing who you are securing your hardware and software from must be part of the model. Beyond never sharing your passwords, it is important to authenticate only to the right person (userID and password) using very strong strings of characters (longer than 8). A hacker might use brute-force attack to guess your easy and typical passwords. Sometimes, a lockout is set if a hacker misguesses a few times.
Online Security (continued)

**Botnets** attack many computers simultaneously which increases the chances of a correct guess. To circumvent these attacks, passwords must use a mix of numbers, letters, and other characters. Sometimes, using three or more words in combination is easier to remember but harder to crack. Using a *secret token* is also useful and not guessable. **Biometric scanners** for fingerprints or eyes can be helpful, but are still quite expensive. Sometimes they are not reliable due to use of photography or similar physical traits. **Multi-factor authentication** gives access control to the right people to read, write, and/or execute in a “no read up, no write down” model called the **Bell-LaPadula model**. **Software patches** are important to reduce data leakage and hacking. Verification and Validation of code improves security.
Cybercrime and Cybercriminals

White hat hackers are motivated to find Zero Day Vulnerability bugs that prevent black hat hackers (cybercriminals) from performing Social Engineering, according to Hackers and Cyber Attacks. Cybercriminals exploit software vulnerabilities that allow them to leave malware like viruses and worms on our computers. They also inject malicious scripts into web sites using a buffer overflow with SQL queries or using brute force to hack into them and hijack the site. NAND mirroring allows hackers to keep trying new passwords even though their three chances are up. They also use email systems to enact Dedicated Denial of Service (DDoS) attacks, phish for private credentials by tricking us, send ransomware that locks your data until you pay them, or attach documents with Trojan Horses.
Cybercrime and Cybercriminals (continued)

**Pretext** is where hackers call an office pretending to be from IT. They will get transferred so their number looks internal, then instruct an employee to complete an insecure task, which allows them access to company servers. Sometimes governments buy exploits to spy on other governments or organizations. **Security patches** should be done frequently so that worms are not added to computers. Many worms working together form a **botnet** which computes in the background to mine cryptocurrency and use up electricity and processing power. **Cyberwarfare**, in addition to physical warfare is being played out daily. A country’s major infrastructures are repeatedly bombarded with hacks in an effort to bring electricity, transportation, and information systems down, which could cost more lives than traditional warfare.
Malware Symptoms, Prevention, and Removal

11 Tell-Tale Signs... provides a list of symptoms to watch out for when using computers. **Check financial account** balances daily for unusual transactions and notify the sellers to get help removing them. If a device slows down, it might be **hijacked** and need more **security checks** and fixes. Software that has been **disabled**, isn’t working properly, has **pop-ups**, or seems to **operate on its own** should be removed or updated. Browser **add-ons/extensions** or **search histories** that you don’t recall installing/viewing should also be removed, as they could have been placed there without your knowledge. If your device **randomly shuts down** on its own then it may have a bug. If a device is bombarded with email or text messages then it has likely been compromised. Don’t click on any internal links. Contact your account companies if you are unable to login due to being hacked.
When multiple problems occur, it is best to **change passwords** for all accounts and ensure each account has a **unique password**. Use **security software to scan** for viruses and fix and/or remove problem files and settings. In some cases you’ll need to **disconnect from the internet**. You may need to **reset to factory settings** and **reinstall** clean versions of software updates. Be sure to save a backup of all of your files first. **Report breaches** to the site or application company. Consult with them as needed to ensure a smooth recovery.
Private Browsing

According to [Want to browse the web privately?](#) different options provide different amounts of privacy in different ways. For example, when browsing in private or **incognito mode**, the history of that tab of the browser does not track your IP address or cookies but the website you visited does see your IP address. Using a **VPN** would obscure the IP address when browsing but not from sites you’re logged into. Some VPN software keeps log files of your activity and others do not. **TOR** can also obscure IP addresses when it routes and **encrypts searches** through other randomly selected computers. When asking sites **not to track** you, they don’t have to comply but adding browser extensions like Ghostery and Privacy Badger can allow you to block trackers. Using a **combination** of all of these options provides the best anonymity online.
How to Opt Out of Targeted Ads Around the Web includes a list of options to try when you don’t want advertisers to bombard you with ads based on your demographics and search history. The first recommendation is to use the WebChoices app from the Digital Advertising Alliance. The app scans your devices to locate 134 targeting details and allows you to choose the ones you want to opt out of. You’ll still see ads, but they won’t be targeted to you personally. The tool works for a single browser so run it on all of your computer’s browsers. A similar tool is AdChoices for mobile devices. To have more control over social media ads, use the Opt Out settings for those companies. For example, Facebook’s Account Settings-->Ads screen allows you to categorize what you want to see and hide what you don’t. Similar settings are available from Google, Instagram, and Twitter.
Password Management Software

Techradar’s Best Free Password Manager 2019 list of important password tools reminds users to make unique passwords for each account we have, to avoid having multiple accounts hacked if a single account gets hacked. Because remembering those passwords is difficult, they recommend installing an Password Management app on a web server or hard drive to manage the credentials for each account. These apps will generate unique strings of text, numbers, and special characters and store them behind a master password...so users only have to memorize one. These apps will usually auto-fill form fields, too. LastPass is free but has a premium option. Dashline is $60 per year! RoboForm works well on mobile devices but starts at $24 per year. Keepass isn’t free either, but will work from a USB stick drive. Sticky Password uses two-factor authentication.
How phone companies sell your location data

Motherboard reporter, Joseph Cox, described his experience with third-party geotracking in *I Gave a Bounty Hunter $300. Then he located our phone*. The results show that major cell phone companies sell our real-time location data to third-party companies. Policing agencies require a warrant to track a citizen’s location, but with software readily available for anyone to purchase, everyone’s location is easily found and exploited. Purchases often happen via the black market without licenses, so developing companies have little control over the users. Legitimate businesses like location aggregators as well as criminals and stalkers, are not regulated, however, CTIA, an industry trade group recommends users get notice and consent, however, it doesn’t protect them. One aggregator, LocationSmart, leaked data for nearly every American phone through their website.
Bibliography


