**CYBER SECURITY INTERNSHIP**

**PROJECT ON PRIVACY**

NAME: I PRASANTI

SIC: 20BCEA56

BRANCH: CEN

# **INDEX**

|  |  |  |
| --- | --- | --- |
| **Sl no** | **Topic** | **Page No** |
| **1.** | **Introduction** | **2** |
| **2.** | **Privacy concerns in internet and online services** | **2-3** |
| **3.** | **Privacy concerns in social media** | **3-5** |
| **4.** | **How to safeguard privacy online** | **5-8** |
| **5.** | **Various tools to protect privacy** | **8-14** |

# **Topic: Privacy**

Date:28-07-2022

1. **Introduction**

* **What is Internet Privacy?**
* Online privacy, also known as internet privacy or digital privacy, refers to how much of our personal, financial, and browsing data remains private when we’re online.
* It has become a growing worry, with browsing history and personal data at increased risk.
* The fact is that internet privacy has always mattered, whether it’s 2010 or 2022. The only difference between the decade is that online threats and data breaches have escalated 10 times. That’s not a good number nor a great time to be heading online without security measures.
* Internet privacy is becoming a growing concern these days for people of all ages. Companies track our behaviour across websites to serve us with highly relevant advertisements, making it essential for us to have an encrypted online connection.
* Governments monitor every move that we make to predict our behaviour and control us better.
* And cybercriminals leave no stone unturned to steal our data for their nefarious purposes.

1. **Privacy concerns in Internet/Online services.**

* **Tracking:**
* When we browse the Internet, we have noticed those pesky ads following us where we go based on our earlier web searches or visits to websites. Well, that’s because websites, advertisers, etc. track our movements.
* Cookie profiling and other techniques are used to track our overall activities online and create a detailed profile of our browsing habits. This is a serious invasion of privacy.
* **Surveillance:**
* Some governments spy on their citizens online to supposedly assist law enforcement agencies. For example, the UK’s Investigatory Powers Act authorizes mass surveillance and allows the government to monitor the Internet usage of its citizens legally.
* According to Data Privacy Statistics, Facts & Trends of 2022, a report by Cloudware, more than 70% of internet users have resorted to an online tool or software, which can keep them safe from online surveillance.
* **Theft:**
* Cybercriminals use malware, spyware, and phishing techniques to break into your online accounts or devices and steal our personal information to engage in identity theft activities.

1. **Privacy concerns in social media.**

* Social media plays a greater role in our lives with each passing day. As such, privacy on these networks has never been more important.
* **Account hacking and impression:**
* Spammers, hackers, and other online criminals are targeting social networks like Facebook, Twitter, and Instagram and using them to carry out a variety of cyberattacks. Once threat actors have access to our account, they can impersonate us and use the trust we’ve built up with our followers to get them to download malware or give up confidential information.
* Cybercriminals also use the wealth of personal information in our social profile to commit identity theft.
* For example, bad actors might open lines of credit in our name and use this new credit card or loan to make major purchases and not pay the bills, thus destroying our credit history.
* Often, thieves and scammers steal our identity without our knowledge. In fact, many us don’t realize there is a problem until we are turned down for a loan or start receiving calls from creditors demanding payment for things we never bought.
* **Stalking and harassment:**
* Social media is a gift to stalkers and harassers in that it often provides them with a detailed description of what we do and where we go. As such, the more we share on social media, the more vulnerable we are for physical and cyberattacks.
* **Being compelled to turn over passwords:**
* As people increase the amount of information they share on social media websites, the need for heightened security and privacy controls also increases. The potential for abuses and privacy violations is just too high.
* **Walking a fine line between effective marketing and privacy intrusion:**
* Advertisers pumped billions of dollars into social media ads last year, and with all that investment comes the desire to target users more accurately. Unfortunately, there is a dark side to all of this targeting. Already, Facebook has faced criticism over its ad targeting engine, which in some cases was [illegally discriminating](https://www.washingtonpost.com/news/the-switch/wp/2017/02/08/facebook-cracks-down-on-ads-that-discriminate/?utm_term=.611219cfe543) against certain types of people.
* **The privacy downside of location-based services:**
* Most of today’s social media users don’t access the services on a traditional computer, they do it on their smartphones. As social media continues to take advantage of mobile devices and location-based services, the potential for privacy and security threats increases. In fact, most people’s smartphones automatically [collect location data](https://www.reputationdefender.com/blog/privacy/why-geotracking-is-a-growing-threat-to-online-privacy) continuously, and social media apps are some of the heaviest users of this data.
* **Data mining and IP tracking:**
* Social networks are notorious for their attempts to mine data and sell it to third-party companies. Every time we create an account on a social network, we willingly relinquish some of our personal data, such as our name, address, occupation, and more. However, companies also tend to mine for more specific data, such as behavioral trends, social contacts and interactions, and various personal interests.

1. **How to safeguard privacy Online.**

* **Read and Understand the Privacy Terms:**
* Every website on the internet has privacy terms, including social media sites.
* Before signing into any social media and registering an account, it is important that you read and understand their privacy terms.
* Pay particular attention to the privacy terms of the information you are registering and agreeing to share when you sign up for an account with a social media platform. For instance, what content can be shared with the third party, can you delete your content on the website permanently.
* **Site Features:**
* Ensure you familiarize yourself with the social media site’s functionality before you broadcast or share any messages. Understand who will see your messages and whether they’ll be only specified recipients or all users on the platform. Above all, understand the privacy settings and privacy vulnerabilities on the social media site.
* **Account Information:**
* Consider carefully the kind of personal detail you provide on your social media profile. Never provide sensitive information such as nearest schools, political affiliation, bank account information, former or current workplace, Social Security numbers, or general interests, among others.
* Providing this information may appear harmless, but it can be used to scam you or serve you unnecessary ads.
* **Biographical Information:**
* To register an account with many social media platforms, you’ll be required to provide your biographical information such as full name, year of birth, age, or address.
* Keep these pieces of information to yourself to limit what other social media users know about you. Such information can provide cybercriminals with enough data to cause you harm.
* You may consider customizing the privacy settings on your media to minimize personal information on the same platform.
* **Turn on private browsing:**
* Many internet websites use technologies such as **cookies to capture the Internet Protocol (IP) address** of a specific computer before collect information about online activities.
* We can **prevent the storing of cookies** (as well as other details like browsing history and temporary internet files) in our computers by websites and thus make it less likely for unauthorized gathering of info on how we surf the net to occur.
* Turning on private mode in our browser (even on our smartphone) should be our **first line of defense** when browsing online.
* **Hiding IP address:**
* As it is still possible for websites to **link one’s IP address with the sites he or she visits,** we can still be tracked (by our Internet Service Provider, for instance) based on our IP address. If we want even more secure browsing, we should use web proxies such as open networks.
* **Remember to log out:**
* Our online activity can also be consistently **monitored across different platforms** since our Facebook account can be logged on via any device with an Internet connection. So, it is best to remember to log out every time we are done with our social networking sites or any other major accounts like Google.
* **Stay updated on privacy policies:**
* Most websites you encounter have privacy policies available for visitors, indicating what information they collect from your computer and who they will share this to. Because these policies are usually **lengthy and full of jargon,** people do not actually read them at all. But in order to safeguard our privacy we should read the important points.
* **Checking in:**
* Frequent check-ins put our online and offline privacy in jeopardy and make us an easy target for actual stalkers. Location-based services provided by Facebook, Instagram and more let us **reveal where we are and what we are doing at a particular time of the day.**
* Social media and networks are designed for people to share things about themselves to their peers, but there should be a **clear line drawn between your privacy and safety**versus our need to feel a sense of belonging and connection with our peers.
* **Beware of open Wi-Fi Hotspots:**
* Open Wi-Fi sources in public areas have **no encryption**, which means that someone near our location can **capture data we transmit online** such as our passwords, bank accounts and emails.
* The best prevention you can take is to avoid connecting to unsecured public Wi-Fi connections in public places, such as cafes, hotels, libraries, etc.
* **Avoid Clickbait:**
* No social media will take responsibility for third-party apps. When prompted to ‘comment below to see magic’ or ‘check which celebrity you share a birthday with,’ avoid clicking these random baits. They are third-party apps that try to capture and misuse your private information.
* **Be careful about posting photos online:**
* Before you post any photos, think twice. Posting photos on social media has been identified as one of the risky social networking activities. For instance, a simple, harmless picture of your child without a name may already be revealing too much information.
* Advertising your whereabouts through pictures could make you, your loved ones, or your home a tempting target for cybercriminals.

1. **Various privacy tools.**

* **Secure and Privacy friendly browsers:**
* **Brave:** This project is based on Chromium. But then, there is a significant emphasis on privacy from the browser’s inception. It blocks trackers and ads, is customizable, and is among the fastest in the industry. Most importantly**,** it is designed to prevent browser fingerprinting from external observers.
* **Mozilla Firefox:** The Firefox web browser has a high degree of versatility. Hence, it can be your worst privacy nightmare or one of your best privacy friends, depending on how you use it.

Indeed, Mozilla Firefox is an excellent option for privacy protection if we take time to tweak it a little. So, it’s not a superb out-of-the-box option like Brave, but it will still do the trick if you take the time.

* **Tor Browser:** It is a Mozilla Firefox browser altered by the TOR project to browse through the Tor network only. It means that all your traffic goes through a couple of nodes in the network, and it is encrypted. But it also means that you should be ready to bear the slow speeds.
* **Chromium:** The standard Chromium web browser offers some great features, except that it doesn’t connect automatically to a Google account (which is good for privacy).
* **Virtual Private Networks (VPN):**
* **Nord VPN:**

Nord VPN is the most potent, advanced, and versatile VPN out there. It performs every task an excellent VPN should perform at the highest level in the business. Also, it offers many additional features on the side.

* **Express VPN:**

Express VPN has been around for a very long time in the VPN world. So, it has had time to accrue one of the best reputations in the industry. It is among the most versatile and advanced VPNs offering many features besides encryption and IP masking. It also sticks to a zero-log policy, the critical issue in privacy-friendly jurisdiction.

* **ISP Spying:**

A VPN will encrypt and anonymize your internet connection. This makes your traffic completely unreadable to your ISP and other third parties.

* **Blocked content:**

A VPN will let you easily get around blocked content and censorship. Simply connect to a VPN server in the region you need and access the website or stream as normal.

* **IP and location tracking:**

Many websites and advertisers track users through their IP address. With a VPN, your IP address and location will be replaced by the VPN server’s IP address and location.

* **Copyright issues:**

Torrenting and streaming media from third-party sources can come with some risk in the form of copyright issues. A VPN will anonymize your IP address and help keep you safe.

* **Blockers: Advertisements, Trackers, and Malware:**
* **Browser adblocker extensions:**

Many browser extensions will block ads for you, like uBlock Origin. But they have their tradeoffs. In some cases, the ads and their tracking activity can still use your system’s resources even if you can’t see them. Whereas, some others collect your data for profit (Ghostery, AdblockPlus), some others still show you “approved” (non-malicious) ads.

* **Adblocker apps:**

Dedicated apps will generally do a better job than browser extensions. AdGuard is both popular and reputed.

* **VPN adblocker:**

While using a VPN is ideal, it’s better to pick one with an adblocker. Such VPNs offer reliable security and privacy.

* **Router adblocking:**

You can block those nasty ads from your router! You can achieve this goal in several ways, like using an adblocking DNS to loading custom filters to your router.

* **Pi-hole:**

It is a network that works as a DNS server that you can deploy in several ways. It’s popular on Raspberry Pi implementations, connected to a home router.

* **Password Managers:**
* **NordPass:**

From the developers that brought us the NordVPN service and NordLocker, we have NordPass, a secure and friendly password manager that has passed external audits.

* **Keeper:**

A robust password solution that also offers dark web monitoring. While its prices are slightly higher, Keeper ‘s biggest strength is its 30-day free trial offer.

* **Dashlane:**

A big name in this market, Dashlane offers many features and strong security standards like end-to-end encryption.

* **Secure Messaging Apps:**
* **Signal:**

It is an open-source messenger with a rapidly growing fan base. It’s probably the most technologically advanced app, designed to protect users’ privacy at all costs.

The app’s performance is excellent in most regards. But it lacks many additional features that most WhatsApp users are already familiar with. Nonetheless, following the surge in its customer base, Signal has introduced numerous helpful changes improving the app’s performance.

* **Wickr Me:**

It’s also free, like Signal, and it offers some unique privacy and security features.

* **Wire:**

Hailing from Switzerland, this is an excellent messenger that is very secure, friendly, and fully featured. It’s free for personal use but you may struggle to find and activate that option.

* **Threema:**

It costs 3 USD for a lifetime license, a rare feature in open-source projects. But it remains a good option.

* **Telegram:**

It started in Russia, then moved to the UK. It now works from the Middle East. As WhatsApp replacements go, Telegram is probably the most popular. But beware: encryption is not the default, so you have to activate it manually for each user in your contact list.

* **Private Search Engines:**
* **DuckDuckGo:**

It is probably the most popular private-friendly search engine on the internet**.**

* **MetaGer:**

A German open-source metasearch engine with exciting features.

* **Searx:**

It’s privacy-friendly, versatile, based on metadata search, and it’s also open-source.

* **SwissCows:**

Zero-tracking search engine from a secure Swiss complex.

* **Qwant:**

A French private search engine.

* **Mojeek:**

This one is a real search engine (not a meta searcher) from the UK with its own index and crawler.

* **YaCy:**

A Peer-to-peer search engine.

* **Private Email:**
* ProtonMail
* Tutanota
* CTemplar
* Runbox
* Fastmail
* Posteo
* Hushmail
* Mailbox.org
* Mailfence
* **Privacy and Security Hardware:**
* **Apricorn:**

This company makes computer storage products. It has external storage hardware with 256-bit encryption specifically for organizations requiring secured data storage.

* **Bitdefender:**

Bitdefender is known for its antivirus suite. But it also sells a network security hardware piece for devices in the Internet of Things.

* **Purism:**

This company produces a variety of hardware solutions like smartphones, laptops, and USB security tokens. They are all designed with privacy as the priority.

* **Helm:**

A secure personal server that helps you protect your emails and other online data.

* **Kingston Technology:**

You probably already own several USB flash memories from Kingston Technology. The company brings encryption along to improve the security in its devices so that they comply with AES-256, FIPS 197, and FIPS 140-2 security standards.