Table of Contents

[INTRODUCTION 2](#_Toc39688984)

[1. What is Internet Privacy & Why it matter so much today? 3](#_Toc39688985)

[1.1. What is Internet Privacy? 4](#_Toc39688986)

[2. Common Internet Privacy Issues to Watch Out For 5](#_Toc39688987)

[2.1. Tracking 5](#_Toc39688988)

[2.2. Surveillance 6](#_Toc39688989)

[2.3. Theft 7](#_Toc39688990)

[3. 4 Internet Behavior That Impact Your Privacy 7](#_Toc39688991)

[3.1. Using the Same Credentials for Multiple Accounts 8](#_Toc39688992)

[3.2. Staying Logged into Websites 8](#_Toc39688993)

[3.3. Using Services without Reading their Terms & Conditions 8](#_Toc39688994)

[3.4. Opening Suspicious Attachments or Downloading Malicious Files 8](#_Toc39688995)

[4. 10 Ways to Protect Your Privacy and Security on the Internet 8](#_Toc39688996)

[4.1. Secure Your Web Browser 9](#_Toc39688997)

[4.2. Use a Virtual Private Network (VPN) 9](#_Toc39688998)

[4.3. Keep Your Software Up-to-Date 10](#_Toc39688999)

[4.4. Install an Anti-virus Program & Activate Firewall 11](#_Toc39689000)

[4.5. Delete Cookies at Browser Exit 12](#_Toc39689001)

[4.6. Adjust Your Settings on Google, Facebook, ect. 12](#_Toc39689002)

[4.7. Use HTTPS to Secure Your Online Connection 13](#_Toc39689003)

[4.8. Defuse Threats When Backing up to the Cloud 14](#_Toc39689004)

[4.9. Secure Online Communications 15](#_Toc39689005)

[4.10. Share Online Files Securely 15](#_Toc39689006)

[5. Conclusion 16](#_Toc39689007)

[6. Reference list 16](#_Toc39689008)

**INTERNET PRIVACY & USING THE INTERNET SAFELY**

****

# 

# **INTRODUCTION**

So far, humans have never had to suffer the impact of what is considered to be "invisible" like online newspapers, social networks today. A piece of information on Facebook, twitter will be known by millions of people and is constantly updated in a few minutes. Every day billions of people use social networks to share information from individuals to the community. It is these actions that made this service more and more developed. Along with traditional newspapers, electronic newspapers and social networks are also a great source of information for everyone. They use the internet every day as an essential part of life.

Besides the benefits of providing information quickly to everyone, there are also some big issues such as network security or personal freedom. A lot of the information on the internet without control is passed out very quickly. This has a direct impact on society, disrupting information, and adversely affecting government or organizational policies. In the world, there have been many scandals about the exploitation of personal information, the freedom on the internet, and that is a lesson for any government, organization, or individual.

Data from the Vietnam Computer Emergency Response Team and Bkav show that, in 2017, VNCERT recorded 13,382 incidents of network attacks in Vietnam. In particular, malicious code attacks are 6,400 cases; hacked change interface 4,377 cases and phishing attacks are 2,605 cases causing damage of more than 12,300 billion VND. For large companies, the risk of a system attack is the same as the loss of trillions of dollars, the reputation of customers is reduced. With health and defense agencies, the damage can be many times larger. Especially in recent years, people are talking a lot about the fact that Facebook has collected user information and disclosed information to third parties. Apple, a mobile phone company that is said to have good security, can not avoid data security errors when hacked.

This shows that the Internet always has the potential to steal personal data, while more and more tricks, malware, dangerous viruses are always ready to invade and take over your online account. Equipping the knowledge necessary to use the Internet safely is essential and is an urgent need today. Therefore, I chose the topic: "Internet privacy & using the internet safely" for my report.

1. What is Internet Privacy & Why it matter so much today?

Internet privacy is becoming a growing concern these days for people of all ages. Companies track your behavior across websites to serve you with highly relevant advertisements.

Governments monitor every move you make to predict your behavior and control you better. And cybercriminals leave no stone unturned to steal your data for their nefarious purposes!

****

Instant connectivity has changed the way we live and work for the better, but this convenience comes at a very big price: your privacy! That’s why it has become more important than ever for you to take responsibility for protecting your Internet privacy and personal information.

1.1. What is Internet Privacy?

Internet privacy, also commonly referred to as online privacy, is a subset of data privacy and a fundamental human right. Basically, it refers to the personal privacy that you’re entitled to when you display, store, or provide information regarding yourself on the Internet.



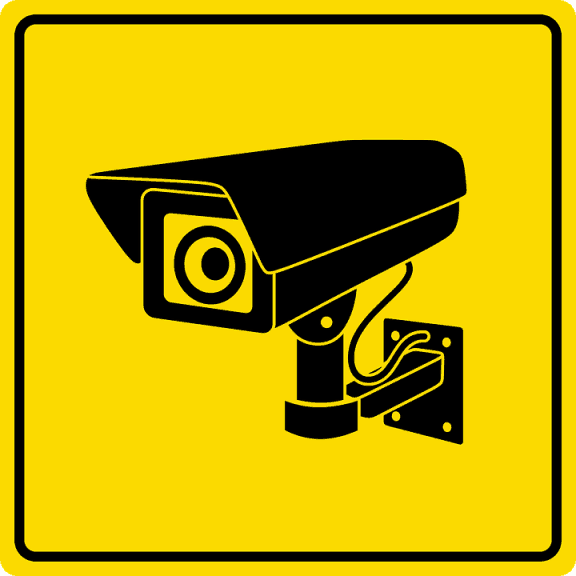
This can include both personally-identifying information (PII) as well as non-personally identifying information, such as your behavior on a website. Without Internet privacy, all your activities are subject to being collected and analyzed by interested parties!

2. Common Internet Privacy Issues to Watch Out For

Now that you understand what is an Internet privacy and its importance, let’s discuss the most common issues that surround your privacy online today:

2.1. Tracking

When you browse the Internet, you may have noticed those pesky ads following you where you go that are based on your earlier web searches or visits to websites. Well, that’s because your movements are tracked by websites, advertisers, etc.

****

Cookie profiling and other techniques are used to track your overall activities online and create a detailed profile of your browsing habits. Some people may not mind having relevant ads being served up to them, but for others, this is a serious invasion of privacy.

2.2. Surveillance

Some governments spy on their citizens online to supposedly assist law enforcement agencies. Take, for instance, the UK’s Investigatory Powers Act that authorizes mass surveillance and allows the government to legally monitor the Internet usage of its citizens.



Internet companies (ISPs), telcos, as well as other communication service providers are required to retain customers’ Internet connection records for a year, which can be obtained by government authorities and used in investigations – even if you’re not related to them in any way!

2.3. Theft

A staggering 17 million Americas have been affected by indentity in 2017, according to [Javelin Strategy](https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity). Cybercriminal use malware, spyware, and phishing techniques to break into your online accounts or device and steal your personal information to engage in activies like identity theft.



The victims, of course, end up losing most or all of their hard-earned money, just because they didn’t exercise caution when it comes to opening attachments, instant messages, or emails from unknown sources.

3. 4 Internet Behavior That Impact Your Privacy

You’ve heard time and time again that online privacy and security is important, but do you actually do something about it? Most of us practice bad Internet hygiene and don’t even realize it, so don’t forget to avoid doing the following:

3.1. Using the Same Credentials for Multiple Accounts

Sure, it’s easy to remember and get things done online when you use the same credentials across your accounts. But if a cybercriminal is able to gain access into your one accounts, they’ll most likely get into the other ones as well.

3.2. Staying Logged into Websites

Not logging out of websites and having them remember your credentials is indeed convenient. However, it also leaves your online accounts and personal information vulnerable to anyone who uses or hacks into your device.

3.3. Using Services without Reading their Terms & Conditions

Never click “agree” until you understand what you’re getting yourself into. You wouldn’t want to legally grant companies and service providers access to all kinds of data. Then sell this information to the highest bidder!

3.4. Opening Suspicious Attachments or Downloading Malicious Files

You should be careful when opening attachments in emails or on social media as they could contain malware and viruses. Similarly, it always downloads files from trusted sources because it may result in virus infection.

4. 10 Ways to Protect Your Privacy and Security on the Internet

If you’ve made it this far, you’ve probably got a better idea of what Internet privacy concerns affect users. Now, you may be wondering “how do I protect my privacy online?” Well, here are some measures that should be followed:

4.1. Secure Your Web Browser



Your browser is the main program you use to go online, so make sure that you take the necessary steps to secure it. After all, cybercriminals can take advantage of loopholes in browsers to access the personal data on your device. To protect your online privacy and security, we’d recommend that you follow the recommendations in our ultimate browser security guide.

4.2. Use a Virtual Private Network (VPN)

****

Using a VPN is the best way to protect your Internet privacy. Not only does it change your IP address and assign you a new one based on the VPN server you’re connected to, but it also protects your incoming and outgoing traffic with military-grade encryption.

As a result, your online activities and personal information stay secure and private from snoopers. PureVPN is regarded as the best VPN when it comes to online privacy and security, and for all the right reasons.

4.3. Keep Your Software Up-to-Date



If you leave vulnerabilities in your software, chances are that the bad guys will exploit them! Keep your operating system, browser, as well as other software (like Adobe Flash and Java) up to date to ensure that you don’t miss out on new features and security fixes. If you find it a hassle to manually apply updates, you can always use tools to automate your software updates.

4.4. Install an Anti-virus Program & Activate Firewall



You can keep your safe from harmful content on the Internet with a few simple precautions. A strong anti-virus program will keep your device free from all types of malware, such as spyware, viruses, Trojans, etc. You should also activate your firewall to keep unwanted network traffic at bay. The good news is that most operating systems come with it built-in.

4.5. Delete Cookies at Browser Exit



You should delete cookies regularly as they’re used by websites, advertisers, and other third parties to track you online. While you can clear your cookies manually, you’re better off configuring your browser to automatically delete them at the end of the browsing session. If you don’t know how to, follow our guide to deleting browsing cookies automatically at browser exit.

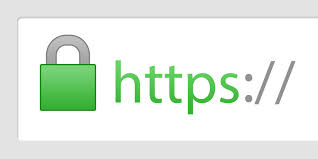
4.6. Adjust Your Settings on Google, Facebook, ect.



Take advantage of the options that are available to you. Big Internet companies such as Facebook and Google usually give you options to opt-out of some, if not all, of their personalization and tracking. For example, you can manage your ads preferences on Facebook from here, while Google allows you to turn off ads personalization from here.

4.7. Use HTTPS to Secure Your Online Connection

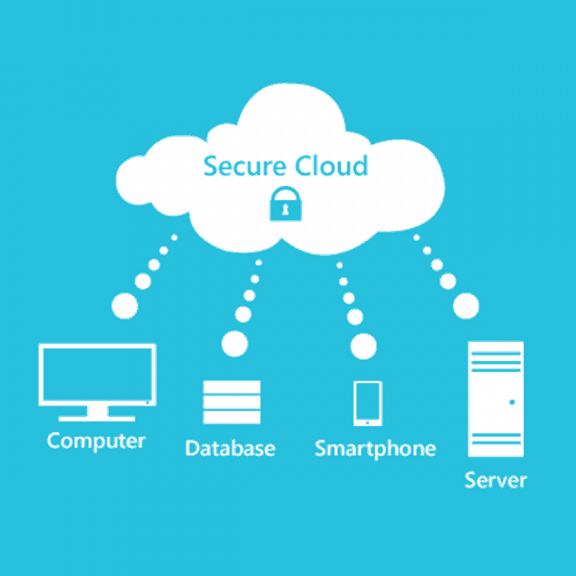
If you are on a website that uses HTTPS, it’s likely that any personal data flowing between you and the website is probably being monitored by trackers or potentially intercepted and stolen by malicious hackers. These entities are commonly referred to as man-in-the-middle.



An HTTPS or Secure Sockets Layer (SSL) encrypts your online communication with that website. If you are on any website especially a shopping website, you should ensure that you have an HTTPS connection. For the utmost online privacy and security, you should resort to a VPN service.

4.8. Defuse Threats When Backing up to the Cloud

In today’s era, we constantly back up our pictures and other files on the cloud. Backing up on the cloud comes packed with its own privacy issues. Anyone could intercept your internet connection and view the data you are backing up or downloading from the cloud.



To defuse this threat, it’s advised that you use [state-of-the-art AES 256-bit encryption](https://www.purevpn.com/features/256-bit-encryption) that will secure your internet connection, meaning you can download and upload sensitive information without worrying about anyone tapping in on your private data.

4.9. Secure Online Communications

Most of your online communications platforms are unsecure. While numerous messaging apps offer end-to-end encryption, security experts advise adding an additional layer of encryption to your online communication.



email encryptionAs far as emails and messaging on chat apps are concerned, you should opt for reputable services such as Signal, Telegram, etc. When it comes to emails, use secure mail services.

4.10. Share Online Files Securely

Securely share files with anyone on the web by password protecting them. With a password protecting your PDF or any other file, you can rest assured that it is only viewed by the intended recipient.



5. Conclusion

Privacy on the Internet is your basic right and you need to fight for it! By incorporating these Internet privacy tips into your daily lives, you’ll be able to protect your privacy online and browse with peace of mind, knowing that your personal information won’t fall into the wrong hands.

6. Reference list

[1] The Verge “How to increase your privacy online“, by Jacob Kastrenakes on Thursday, June 7, 2018.

[2] The Next Web “7 ways to protect your privacy on the internet“, by Morgan Slain on Tuesday, August 18, 2015.

[3] <https://www.purevpn.com/blog/what-is-internet-privacy-scty>

[4] <https://www.slideshare.net/trongthuy1/luan-van-thuc-trang-ve-an-ninh-mang-va-bien-phap-doi-pho-hot>

[5] https://www.sggp.org.vn/bao-ve-quyen-rieng-tu-tren-mang-9837.html