УДК 004.62

I. I. Storozhuk

HOW SECURE IS YOUR PRIVATE INFORMATION ONLINE?

Вінницький національний технічний університет

Анотація
Запропоновано методи для захисту вашої особистої інформації в інтернеті.
Ключові слова: конфіденційність, безпека в Інтернеті, приватна інформація в Інтернеті.

Abstract
Methods for protecting your personal information on the Internet are offered.
Keywords: privacy, internet security, private information on the Internet.

Have you ever wondered why you see ads on Google about the same topic you just sent a Facebook message to your friend about? Have you ever wondered why some advertisers know more about you than you think they should? As technology becomes ever encompassing, you should understand how your actions affect what people and companies know about you, as well as know how to protect your privacy. Remember, any information that you post online, stays online forever. Also, be careful where you enter your information and who you provide it to, as advertisers like to share information, and the thing that you are getting for free, isn't actually free, it's costing you your privacy [1].

The purpose of the work is to research methods for protecting your personal information on the Internet. Internet privacy and internet security are different but closely related. Privacy usually deals with legal data collection (like what you post on Instagram, Snapchat, and other social media), while cybersecurity focuses on illegal data collection (like protecting your accounts from hackers). But there's a lot of overlap. Good security enhances privacy, and enhanced privacy helps maintain good security. By taking some simple steps, you can improve both.

How to Protect Your Online Privacy:

1. Commit to sharing less online:
    - Share less on forms. Skip any "optional" information, like a middle name or phone number
    - Create a throwaway email address. Email lists are often sold or rented on the Dark Web and can fall into unsafe hands. Consider making a throwaway email just for subscriptions.
    - Limit collaborative folders, albums, or playlists. The more people who have access to your data, the more likely it could be leaked or hacked.
    - Protect your Wi-Fi password. Your router handles plenty of sensitive information, from passwords to financial information. Anyone with your Wi-Fi password and nefarious intent could try to steal your information.
2. Use strong, unique passwords and two-factor authentication:
    - Strong passwords are the most important — and sometimes the only — protection we have against identity theft and hackers.
    - If you don't already have passwords or passcodes for all your devices (including guest accounts), add them now.
    - Unique password on your online accounts.
    - And finally, set up two-factor authentication for every account that allows you to.
3. Tighten privacy settings for your online accounts. The next step you can take—and perhaps the easiest—is to simply review the privacy settings on the online accounts you use regularly:
    - The best settings for you depend on what you want to share and what you want to protect. But there are a few areas where you should pay careful attention.
    - Location tracking. Consider turning off automatic geolocation data on your social media posts, photos, and comments.
    - Public information. Think carefully about what information should be public, hidden, or somewhere in-between. There are typically three levels of data: profile data, your content,

and your interactions with other content.
    - Likes, shares, and comments. We usually think about limiting what we share, but your "likes" and comments on other posts are usually public as well. Profile pictures, names, and comments on other posts often show up in search results, even for "private" accounts.
4. Purge unused mobile apps and browser extensions:
    - Once you stop using an app, delete it. Purge any program you don't use regularly, from mobile apps to browser extensions.
    - If you use Chrome, you can see all extensions by typing chrome://extensions/ in your search bar. It's good to delete — not just disable — any extensions that you're not using.
    - Even if you still visit a site every once in a while, it's safer to access it through your browser than download the app on your device.
5. Block search engines from tracking you:
    - Your search engine collects a huge amount of personal data about you. And for 92% of us, that search engine is Google.
    - The first step to improving search engine privacy is deleting your data.
    - For Google: Go to the My Activity dashboard and delete everything.
    - For Microsoft: You'll need to clear data separately from Microsoft Edge and Bing.
    - For Yahoo: You can delete data from search history management.
    - Unfortunately, there's no way to eliminate all tracking on Google. An alternative is to switch to an online privacy-focused search engine like DuckDuckGo.
6. Browse online with a secure VPN:
    Leveraging a secure VPN can encode your browsing information and make it unreadable to hackers. A VPN is essential if you're forced to use public Wi-Fi, like at a coffee shop or airport. (Remember: there are numerous dangers of using public or unsecured Wi-Fi networks.)
7. Don't ignore software updates:
    - The first and most crucial step is to set your operating system to install updates automatically. Follow instructions to set up auto-update for Microsoft Windows, Apple macOS, and Google Chrome OS.
    - You can also download antivirus software to protect against malware like spyware, which collects data like credit card information in the background.
8. Disable ad and data tracking:
    - Most of your personal data collected online isn't for scams or data breaches — it's for marketing. With a few simple steps, you can disable many of these trackers.
    - First, when pop-ups ask if you want to share data, say no.
    - Whenever possible, decline cookies on websites. If you use an iPhone or other Apple mobile device, iOS versions 14.5+ let you disable cross-app tracking.
    - Finally, you can disable ad customization across the apps you use, including Google search, other Google services, Apple, Facebook ad settings, third parties that use Facebook data, Twitter, Microsoft, and Amazon.
9. Use encryption to keep data from prying eyes:
    - The solution is to set up encryption on Windows and Mac so the data will be meaningless to anyone without your password.
    - And of course, remember the obvious: before selling or giving away a device, wipe its data and reset it to factory settings.
    - It's also a good idea to store less in the cloud.
    - You can add extra privacy protection against email hackers by disabling "smart features and personalization" in Gmail and other Google Apps.
    - And again, take a simple but often-overlooked step: disable message previews on your lock screen.
10. Revoke unnecessary third-party app connections:
    - Finally, you can improve the security of all your apps by fencing them in that is, limiting the number of connections they have to other apps.
    - For example, your Spotify account is only as safe as your Facebook account if that's what

you use to sign in. The first step, then, is to replace any single sign on (SSO) with unique logins [2].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Privacy and Internet Security [Електронний ресурс] URL: https://ociso.ucla.edu/security-best-practices/privacy-and-internet-security (дата звернення: 20.04.2023)

2. How To Protect Your Privacy Online [Електронний ресурс] URL: https://www.aura.com/learn/how-to-protect-your-privacy-online (дата звернення: 20.04.2023)

Сторожук Іоанна Ігорівна — студентка групи 3КН-21б, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, м. Вінниця, e-mail: loxipty@gmail.com

Кухарчук Галина Вікторівна — викладач кафедри іноземних мов, Вінницький національний технічний університет, м. Вінниця.

Storozhuk Ioanna Igorivna — student of Intelligent Information Technologies and Automation Department, Vinnytsia National Technical University, Vinnytsia, email : loxipty@gmail.com

Kukharchuk Galyna Viktorivna — an Assistant Professor of Foreign Languages Department, Vinnytsia National Technical University, Vinnytsia.