frontiers

Understanding Cyber Threats: A Safe Journey in Cyberspace

Agnė Brilingaitė [1,*], **Karen Parish** [2] **and Leanne Torgersen** [3]

[1] *Cybersecurity Laboratory, Institute of Computer Science, Faculty of Mathematics and Informatics, Vilnius University, Vilnius, Lithuania*
[2] *Department of Educational Studies in Teacher Education, Faculty of Education, University of Inland Norway, Hamar, Norway*
[3] *Department of Behavioural Medicine and Principles of Human Biology for the Health Sciences, Trier University, Trier, Germany*

Correspondence*:
Agnė Brilingaitė, Didlaukio str. 47, Vilnius LT-08303, Lithuania
agne.brilingaite@mif.vu.lt

ABSTRACT

People use digital devices every day. These devices help people with their work, help students engage in their studies, and provide people of all ages with entertainment. Through an internet connection, digital devices are connected to the global network that is called cyberspace. This article explains the concept of cyberspace and its threats. Most people enjoy cyberspace opportunities and use devices to communicate. However, others exploit cyberspace for unfriendly purposes. They work like thieves on the streets and steal digital data. Do you know how they can steal your data? This article explains how our daily behaviors in cyberspace can lead us into digital traps if we are not careful. We will also teach you about safety measures and how to use them, so you can safely enjoy your time online.

Keywords: cyberspace, cyber threat, hacker, physical threat, software

DIGITALIZATION IS RULING!

People in today's world spend a lot of time using digital devices. Computers, smartphones, and tablets are examples of digital devices that make up the digital environment around us. Digital devices help us with work and school, as well as with family and leisure activities. People work online with their peers on the same project, we can go online to pay bills or apartment rent, and we can watch TV shows and buy tickets to a sports event on our digital devices. People also use various application programs (commonly called apps) to study and communicate. We send messages and photos using messaging apps. People can play games on their devices alone or with friends who are far away. In short, most of us cannot imagine our lives without digital devices!

LIVING IN CYBERSPACE

The digital environment is often called Cyberspace. As we just described, most of us live very active lives in cyberspace. Therefore, we could be called cyber citizens [1]. Life in cyberspace can be compared to the physical world. In the physical world, we walk to sports events, meet new people, and cross the street. In cyberspace, we also make friends, belong to communities, and arrive at virtual "crossroads." Browsing

through web pages is like travelling from one destination to another. Registering for a gaming platform and accepting the game rules are examples of making a choice at a crossroads—after accepting the rules, you can continue playing. Very often, web systems require users to register so they can access important functions of the web pages.

Cyberspace represents the environment connected to the internet. Therefore, only devices that access the internet belong to cyberspace. Figure 1 provides examples of digital and non-digital devices. Typically, a

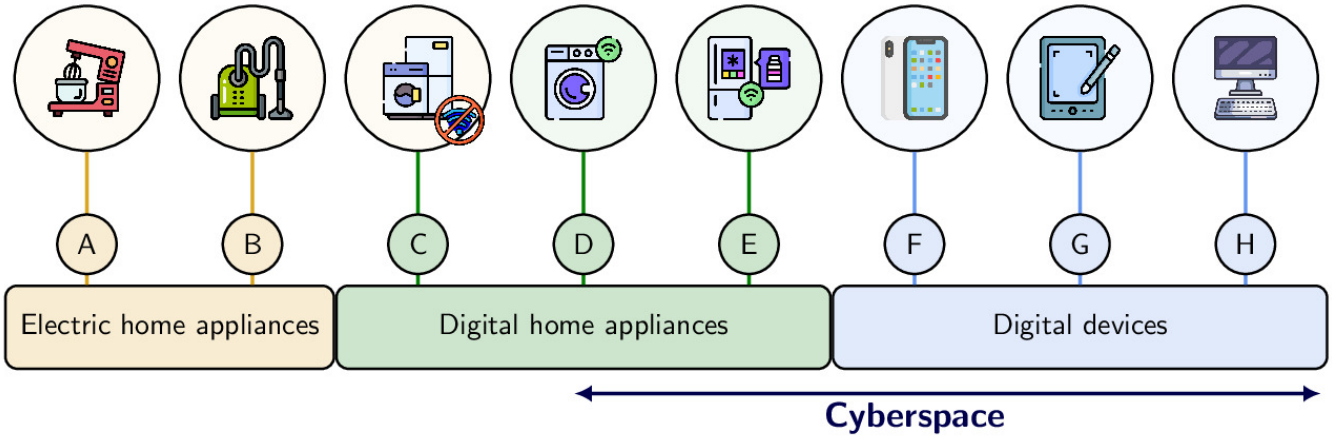

Figure 1. Digital and non-digital devices around us. **(A, B)** Many electric home appliances do not have internet. **(F–H)** Most digital devices have internet by default, but the internet connection can be switched off. Some digital home appliances have internet (marked with a green Wi-Fi symbol), while others do not. (Icons designed by Freepik)

food mixer and a vacuum cleaner are non-digital electric home appliances. Digital home appliances have mini-computers inside them, although some of those mini-computers are not connected to the internet, like a mini-computer to manage washing programs in a washing machine. Such devices can sometimes be updated using special tools that connect to the appliance using another connection type, for example, Bluetooth. However, a refrigerator or a washing machine with a wireless internet connection belong to cyberspace. For these devices, owners could use mobile or web applications to check humidity, temperature, or appliance status data. Digital devices also include computers and smartphones. All digital devices and cyberspace-connected appliances make up a person's Person network [2].

BUILDING BLOCKS OF DIGITAL SYSTEMS

Computer programs and applications are called Software. Software is a broad term that includes games, online educational systems, text editing tools, and booking systems to buy tickets or rent apartments. Software can be standalone or remote (Figure 2). Standalone software is installed on the user's personal device. For example, personal digital devices have operating system software, which enables all of the device's functions and controls the installation of applications such as games or a work-related program. The installed applications use the computing resources and settings of the personal device. You may have noticed that older devices have fewer computing resources. For example, maybe you have an old computer, phone, or gaming system that cannot run new games that require more computing resources.

In comparison, online systems run on remote computers—computers that are located somewhere else, often far away from the user. The remote computers are accessed via the internet. Access to online systems

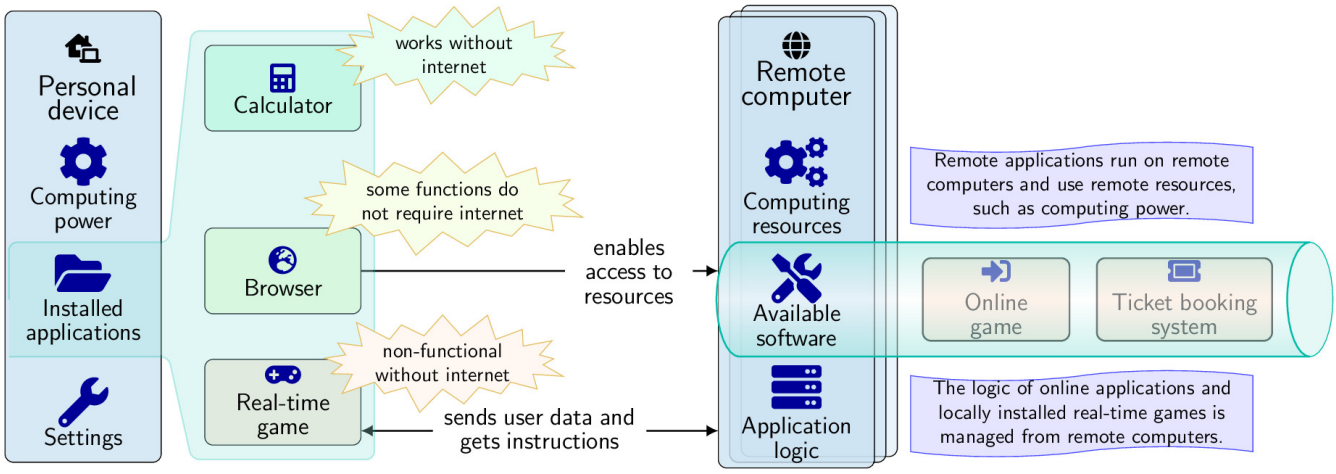

Figure 2. Online and standalone software. Standalone applications use the computing power and data of the local, personal device. For example, standalone applications such as a calculator work without internet. A computer's browser can function without internet to open local files, but it requires internet to access remote resources like online games or web systems. Online applications, such as real-time multiplayer games, are controlled from remote computers. Locally installed software works as a portal that allows users to access remote resources.

happens thanks to software installed locally, on the personal device. In most cases, people need Browsers to access online systems. We can think of local software programs as opening a "portal" to powerful online resources.

Standalone applications can work offline. However, they could send data to (or retrieve data from) remote databases upon request. For example, some games allow users to play without the internet. Then, the results are sent to a remote computer when internet is available. That way, the remote computer can make a leaderboard after getting the results, for example, or the current gaming scenario could be generated based on players' achievements. However, many games are only functional *with* the internet, such as multiplayer games that allow several users to play together in real time. Thus, a locally installed game application sends data about the user's actions to a remote computer without any delay.

CYBER THREATS—RISKS IN CYBERSPACE

Cyberspace has introduced new risks to our modern lives. Just like we take care of ourselves in the physical world, we must also protect ourselves in cyberspace. Most people do not go up to a random stranger on the street and shake hands with them—so why should we accept an invitation from an anonymous person in an online game? Similarly, most people do not go shopping for high-quality products in a building with no store name identified on a sign out front—so why should we download an application from an unknown web page? People generally cross the streets carefully, by looking left and right. Why, then, should we be willing to click any button that appears on our device's screen? Rules and safety measures, like those in the physical world, also exist in cyberspace. We must follow them to be safe when browsing web pages and making virtual friends. Even though the challenges of cyberspace relate to modern times, old fairy tales, told globally, indirectly reference cyber-related notions [3]. For example, most fairy tales include cases of fake identities.

In our daily lives, we may face physical threats to our assets. For example, unlocked bikes could easily be stolen. Digital devices are also sensitive to physical threats—they can be stolen or damaged.

Cyber threats relate to the Digital assets of the owner. Data, such as files and photos, are examples of digital assets. Apps that work properly on our personal devices are also considered digital assets.

Cyberspace is a playground for some cyber hooligans, also called Hackers, who perform unfriendly actions that could harm digital assets. Typically, hackers take over devices, which could change the behaviour of an application. Hackers have various motivations, ranging from curiosity to financial gain [4]. Thus, each cyber citizen should be aware of hackers the same way we try to be aware of pickpockets on busy city streets.

MOST COMMON CYBER THREATS

What are the most common threats in cyberspace? The first relates to the theft of personal and sensitive data. Data theft happens when people share their personal data, like their bank card information. This might happen after falling into a digital trap. For example, let us assume that a user shares details about personal interests online, such as on social media. The shared information could be used by hackers to lure the user into a trap. For example, a manga cartoon lover could receive a fake link, leading to a fake page that allegedly sells new series editions, and that looks just like the site of a well-known online retailer (Figure 3A). The user tries to buy a cartoon and provides real bank credentials to the fake system. The system records everything the user inputs. Now, the hacker can use the credentials to steal and spend the user's money.

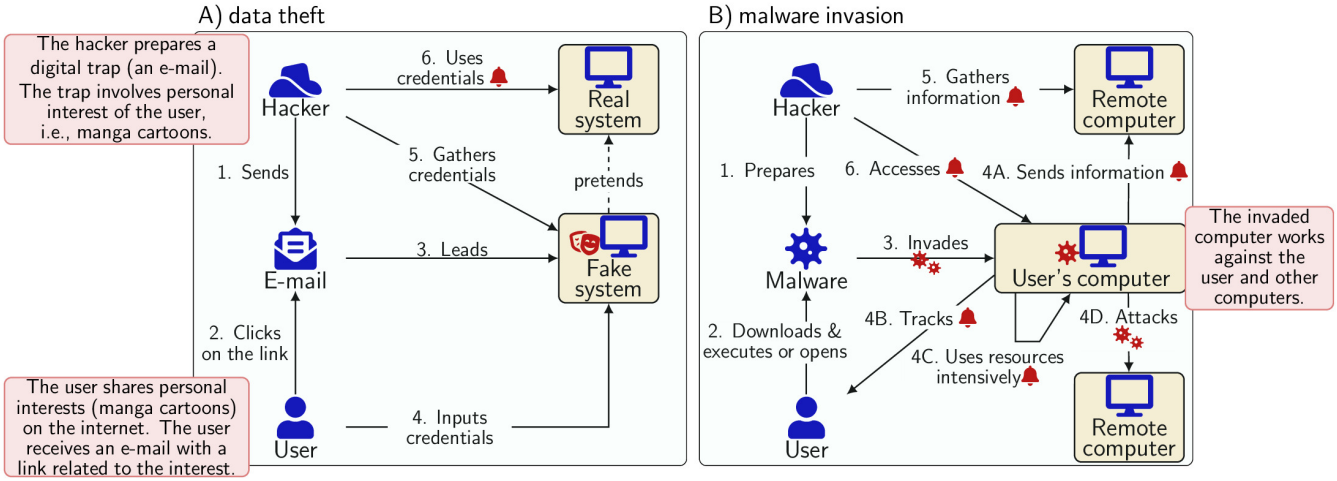

Figure 3. Data theft and malware are two common cyber threats. **(A)** In data theft, the hacker steals money after the user falls into the trap and provides their personal information, like banking data. **(B)** In malware, the hacker invades the user's computer when the user downloads and runs the malware-containing file. Malware can allow the hacker to use the device to attack other computers, track the user, and send the gathered information to remote computers. Each arrow starts at the active party, and the arrow end represents an impact; a bell identifies a risk.

Malicious software called Malware is another common cyber threat. How does a user get malware? Using a similar example, let us assume a manga cartoon lover receives a file via a messaging application (Figure 3B). The file contains a catalogue of a new manga series, yet it also contains malware. When the user opens the file, the malware can invade the user's device. Malware can harm the user's data and installed applications. For instance, data can be stolen or damaged—photos and saved passwords could be sent to remote computers or deleted. Malware can also track user behaviour. This means that all the

user's actions, including password inputs, are recorded. Sometimes malware replicates itself and uses the invaded computer's resources. Malware helps hackers take control of a device. Hackers can use malware on the user's device to carry out unfriendly actions against remote computers. In these cases, the invaded computer is used to hide the hacker's traces.

In short, the same way we would not share our personal matters with a stranger we meet on the street or take a box of sweets from that stranger, we should only share information carefully in cyberspace, and we should double-check any information that we receive.

LET US BUILD A CYBER SHIELD!

Should we be afraid of cyber threats? *No*. Should we take care of our digital assets in cyberspace? *Yes*. Who is the best warrior to defend you in cyberspace? *YOU!* Update your devices regularly—special software can protect devices against most malware types. When this software is installed on a digital device, it can prevent hackers from invading the device. However, most cyber threats happen due to an individual's intentional or unintentional actions [5], like clicking on the link to a fake web page, opening a file in an e-mail from a stranger, or giving personal details to a virtual friend. Every user should take time to assess each situation before taking any action—just like people do when crossing the street. By combining cyber threat-combatting software with online awareness and careful decision making, everyone can have safe adventures in cyberspace!

GLOSSARY

Browsers Software for accessing websites on the internet. 3

Cyber threats Activities that might harm digital assets. 4

Cyberspace An interconnected digital environment consisting of physical computers, networks, and software. Cyberspace includes social networks, email systems, online services, and humans . 1

Digital assets Anything created and stored digitally and having value . 4

Hackers People who break into computer systems without permission or legal reason. 4

Malware Malicious software used by hackers to steal data and disrupt computer systems. 4

Person network Interconnected electronic devices of an individual person. 2

Software A collection of instructions, data, and computer programs that runs on computers to perform specific tasks. 2

CONFLICT OF INTEREST STATEMENT

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

AUTHOR CONTRIBUTIONS

AB: Conceptualization, Visualization, Writing – original draft, Writing – review & editing. KP: Writing – original draft, Writing – review & editing. LT: Writing – original draft, Writing – review & editing.

ACKNOWLEDGMENTS

The authors thank their families for their friendly feedback and support in the journey of the paper preparation.

REFERENCES

[1] Limnéll J, Alasuutari M, Candelin N, Cullen K, Halonen O, Helenius M, et al. Cyber citizen skills and their development in the european union. Tech. rep., Aalto University Research Group, Finland (2023). https://cyber-citizen.eu/wp-content/uploads/sites/6/2023/03/Cyber-citizen-skills-and-their-development-in-the-European-Union_EN.pdf. Last access: June 30th, 2025.

[2] Sahoo BPS, Mohanty SP, Puthal D, Pillai P. Personal Internet of Things (PIoT): What Is It Exactly? *IEEE Consumer Electronics Magazine* **10** (2021) 58–60. doi:10.1109/MCE.2021.3077721.

[3] Viganò L. The cybersecurity of fairy tales. *Journal of Cybersecurity* **10** (2024) tyae005. doi:10.1093/cybsec/tyae005.

[4] Chng S, Lu HY, Kumar A, Yau D. Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports* **5** (2022) 100167. doi:10.1016/j.chbr.2022.100167.

[5] Moustafa AA, Bello A, Maurushat A. The Role of User Behaviour in Improving Cyber Security Management. *Frontiers in Psychology* **12** (2021). doi:10.3389/fpsyg.2021.561011.

BIOGRAPHIES

Agnė Agnė is an associate professor at Vilnius University in Lithuania. She is a computer scientist. Thus, her research involves the application of information technologies in various areas. She develops technological solutions and methods to improve work efficiency in daily routines and the applicability of information systems. Agnė also educates and trains students and professionals in computer science and cybersecurity—she searches for the best ways to explain technical concepts and to design learning materials that are adapted to the learners' needs so that learners stay actively engaged.

Karen is an associate professor at the University of Inland Norway. She is an educational scientist, focusing on student's learning. Karen´s research focuses on the safe and ethical use of digital technology in educational contexts, such as schools and universities, to promote digital competence. She is involved in several research projects related to the design of creative learning processes in technology-rich environments, which incorporate the use of digital games, virtual and augmented reality, and humanoid robots.

Leanne is a Ph.D. student in nursing sciences at the Trier University in Germany. She is also a registered nurse from the United States. Her research focuses on human factors in cybersecurity, psychology, communication, and stress and emotional regulation. Her Ph.D. research project is looking at patients with cardiac implantable electronic devices, the cyber risks these patients have by possessing such devices, the need for patients to be educated about the cyber risks of their devices, and the patient's ethical right to choose regarding issues affecting their health. A key factor of nursing is to engage, encourage, and empower patients. Leanne believes in educating not only at the bedside with a patient but also in the classroom. Knowledge empowers a person to make the best informed decisions.