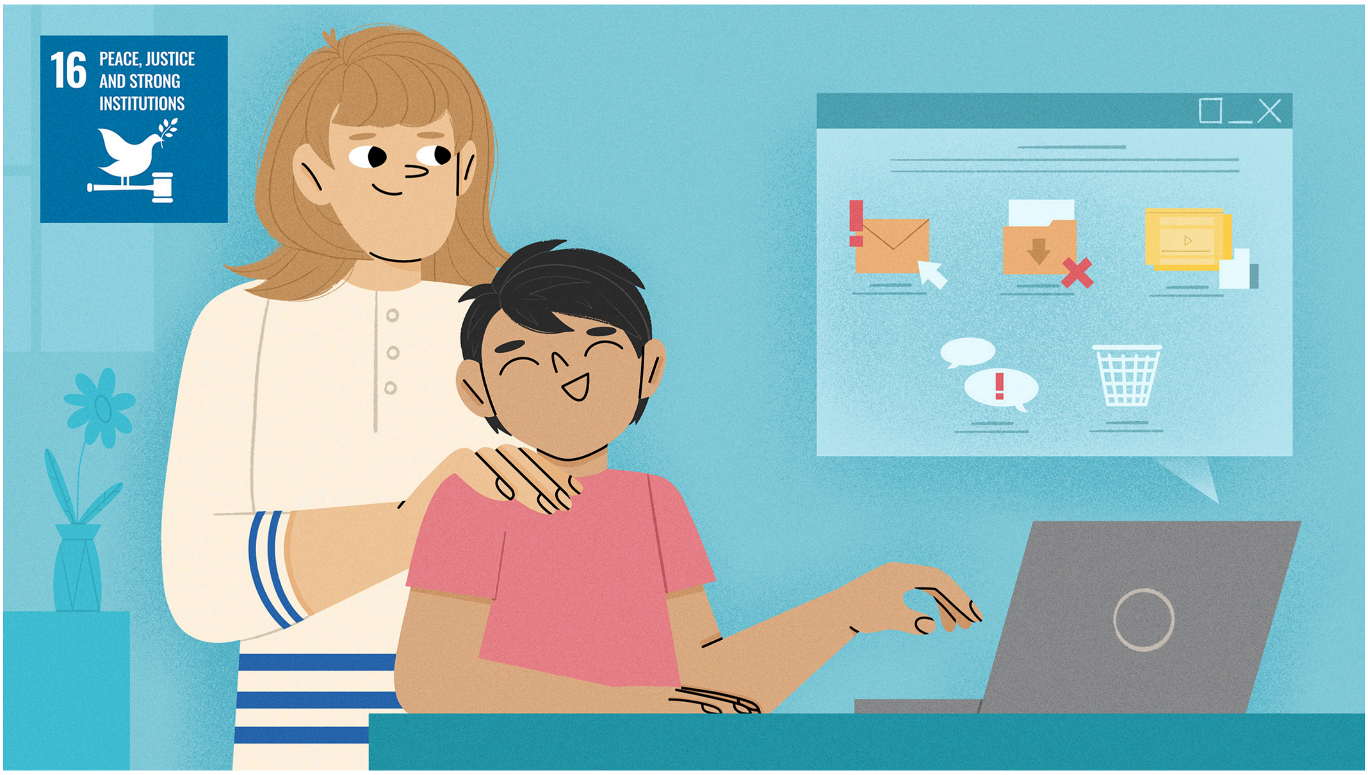
ENGINEERING AND TECHNOLOGY
Published: 11 September 2024
doi: 10.3389/frym.2024.1396135



TOWARDS SDG 16: SAFE AND SECURE USE OF DIGITAL TECHNOLOGIES

Taous Madi, Charalambos Konstantinou* and Paulo Esteves-Verissimo

Computer, Electrical and Mathematical Sciences and Engineering (CEMSE) Division, King Abdullah University of Science and Technology (KAUST), Thuwal, Saudi Arabia

YOUNG REVIEWERS:

AISYAH
AGE: 14

KATERINA
AGE: 9

SHIRHAN
AGE: 16

ZAHRAA
AGE: 16

VIDEO 1

Watch an interview with the authors of this article to learn even more!

The United Nations' Sustainable Development Goal (SDG) 16—Peace, Justice and Strong Institutions—aims to ensure that we all live in societies that are safe, fair, and shield us from danger. Information and communication technology (ICT) refers to the digital devices that we use. ICT involves using digital services to achieve tasks. For example, we use computers and tablets to work, shop, or learn. However, multiple threats might affect our safety in ICT. Stolen private information is one type of threat. To be safe in the digital world, it is important to be aware of those dangers and be a responsible user of ICT. In this article, we aim to raise awareness about the security risks of ICT. You will learn how scientists are keeping our digital world secure and how everyone can be protected from those risks.

Watch an interview with the authors of this article to learn even more! (Video 1).

DIGITAL TECHNOLOGIES HAVE RISKS

Sustainable Development Goal 16 (SDG 16), introduced by the United Nations in 2015, aims to provide people with safe, fair, and fear-free societies. The UN is an international organization founded in 1945, committed to maintaining peace and security, developing friendly relations among nations, and promoting social progress, better living standards, and human rights worldwide. SDGs are a set of 17 global objectives adopted by UN member states in 2015 as part of the 2030 Agenda for Sustainable Development. They cover a broad range of interconnected issues such as poverty, inequality, climate change, and peace. The main target of SDG 16 is to promote peaceful environments, where conflicts and disputes are kindly resolved. It emphasizes the importance of eliminating all forms of violence, especially against children. SDG 16 also aims to ensure that groups of people and countries have equal rights, an identity, and that they are protected by law. By enforcing those important values among individuals, organizations, and countries, SDG 16 will ensure a healthy society [1].

Information and communications technologies (ICT), like social media platforms, messaging apps, and online shopping websites, play an important role in our lives. We now live in a so-called **digital environment**—but this environment can sometimes be unsafe. Users of ICT might face multiple threats, like **cyber-bullying**, which is a form of violence, or theft of their private information, which threatens their safety. Therefore, cautious ICT usage is crucial to achieving SDG 16.

RISKS RELATED TO ICT USAGE

More and more people of all ages are using technology for many kinds of activities. In many schools, students use websites and emails for education and communication. Mobile applications are used for purposes including entertainment, training, and tracking physical activity. Friends connect on social media to share their experiences. Some meet on gaming platforms. Although these tools are beneficial, they come with many **cybersecurity** and safety concerns that you should be aware of as a young ICT user.

From the cybersecurity perspective, there are three main concerns to look out for. The first is when information that should be kept secret, like passwords, is disclosed to other people. This is much like a stranger who somehow has a copy of your house key or who is trying to use your identity cheat on an exam. This is called a **confidentiality** issue. Second, when files and documents, such as study reports, are changed without the consent and awareness of the owner. Think of a situation in which a classmate messes up your project without you knowing it.

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT)

All the electronic devices that we use. It involves using internet-based services to achieve various tasks.

DIGITAL ENVIRONMENT

The environment created by the use of ICT, to facilitate everyday activities like communication, collaboration, making appointments, etc.

CYBER-BULLYING

The use of digital communication platforms to intimidate, harass, or harm individuals or groups, often through repeated aggressive behavior or spreading of harmful content.

CYBERSECURITY

The practice of keeping ICT safe and defending against misbehavior and misuse, such as information theft or file deletion.

CONFIDENTIALITY

The assurance that sensitive information is protected from unauthorized access or disclosure. In the context of ICT and cybersecurity, confidentiality ensures that data is only accessible to those authorized to view or use it.

This is an **integrity** issue. Third, when your devices cannot be used properly anymore because they are being used by people who are not allowed to use them. This is known as an availability issue.

How do these cybersecurity issues show up in our everyday lives?

Websites and Email Boxes

We use websites and email boxes every day to accomplish tasks, interact with one another, or learn things. Although engaging, some websites can damage our devices or show us inappropriate content. For instance, if you click on a suspicious object, you might be redirected to another website—perhaps one that shows unsuitable content. In other situations, after clicking, **malware** can be downloaded to your device. Depending on its nature, malware can cause various kinds of damage [2].

Malware may damage your data, for example by erasing the content of your files. Or it may impact confidentiality by allowing access to sensitive information, such as your identity information, home address, or bank details. Some types of malware target availability by consuming all the resources (like processing power and storage space) we have on our devices. For example, a trojan horse is a well-known kind of malware that can give hackers access our devices (Figure 1). You can imagine those hackers as cyber thieves, trying to take things that do not belong to them in the digital environment. Those things can be photos, passwords, or even a country's important security documents, if they invade a government device.

INTEGRITY

The quality of data being accurate, complete, and unaltered. In the realm of cybersecurity, integrity refers to maintaining the consistency and trustworthiness of data, ensuring that it has not been tampered with or modified in an unauthorized manner.

MALWARE

A malicious software installed on devices without the user's approval. Malware instructs the device to misbehave in a way that compromises confidentiality, integrity, and availability.

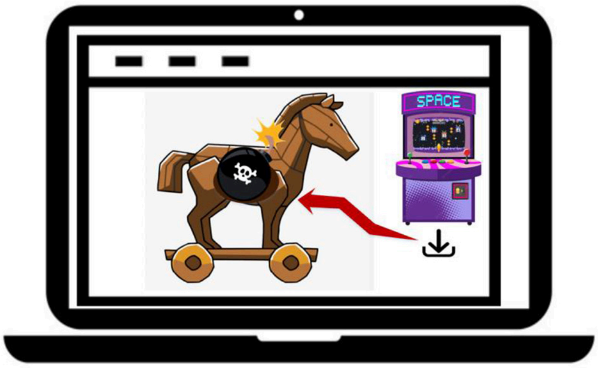


Figure 1

Figure 1

When you click on certain download icons, a Trojan horse might be downloaded to your device without your awareness. Once downloaded, the Trojan horse performs negative operations, such as giving hackers access to your device. The term Trojan horse is inspired by the ancient Greek story of the giant wooden horse that led to the fall of the city of Troy. The people of Troy thought the giant horse was a present, so they brought it inside the gates. However, the giant wooden horse opened at night and soldiers sneaked out of it and invaded the city.

Mobile Applications

Many ICT users download applications onto mobile phones. Games and activity-tracking apps are popular ones. Although those applications may seem to be safe, some of them may contain malware, often in the form of auto-clickers. An auto-clicker is a simple malware that imitates the user's actions and clicks on many places at once (Figure 2). This causes our devices to use a lot of resources, making them slow at performing tasks. Auto-clickers can also click on download buttons and download more malware to our devices, which hackers can then use to access our information. Sadly, applications with malware are common. For instance, out of 56 mobile applications found to have malware, 24 were children's applications [3].

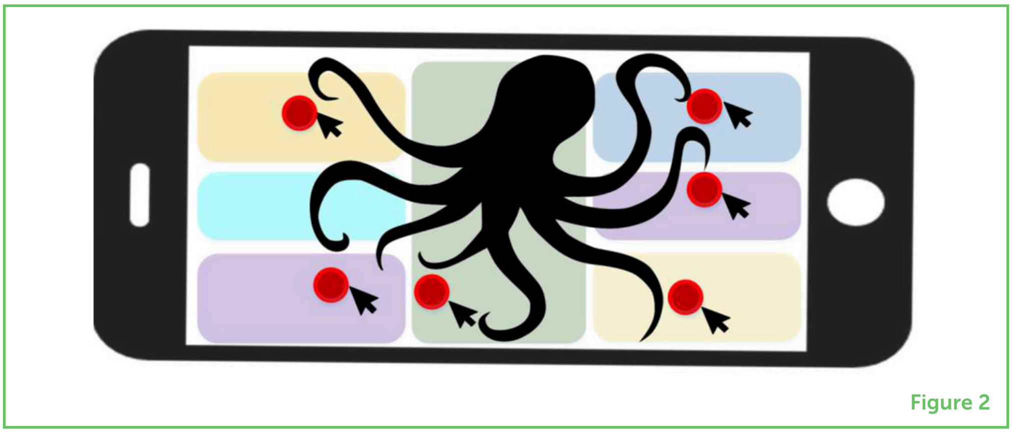


Figure 2

Figure 2

An auto-clicker clicks many times in an automated way. You can think of it as an octopus with multiple legs. All of them perform automated clicks in parallel, for example on advertisements and banners that appear in the applications.

All these security threats may affect our safety in the digital environment, put our money in danger, and damage our ability to access vital services. When you think about this at the country level, and how it can impact the overall safety, integrity, and privacy of citizens' data, it is easy to understand that cybersecurity directly impacts how safe, fair, and strong a society can be.

HOW CAN SCIENCE HELP?

Fortunately, many people are working together to make the digital environment safer. Cybersecurity researchers work on protecting the digital world against threats. They develop ways to detect and stop malware before it causes any damage. They also try to figure out who is responsible for the bad actions, such as identity theft. To strengthen the security level of ICT, researchers also work on things like **authentication**, which means verifying the identity of users to ensure they are who they claim to be, or access control, such as limiting who can access certain resources or data.

AUTHENTICATION

The process of verifying the identity of a person or device, similar to showing an ID card to prove who you are.

As an example of one of our research projects, we set out to create software that could prevent damage to ICT systems even in the face of harmful events. In other words, we wondered if we could build a software that could protect devices from any malicious activities [3, 4]. The software has two main components, a detection component and a recovery component. You can think of the detection component as a policeman and the recovery component as an ambulance rescuer. Much like a policeman, the detection component continuously keeps an eye on what is happening in the device and checks for any unusual activities. This is called monitoring. When the detection component suspects something is wrong, it raises an alarm for immediate attention and action. The alarm instantly triggers the recovery component, which repairs any possible damage, to bring the device back to a healthy state (Figure 3).

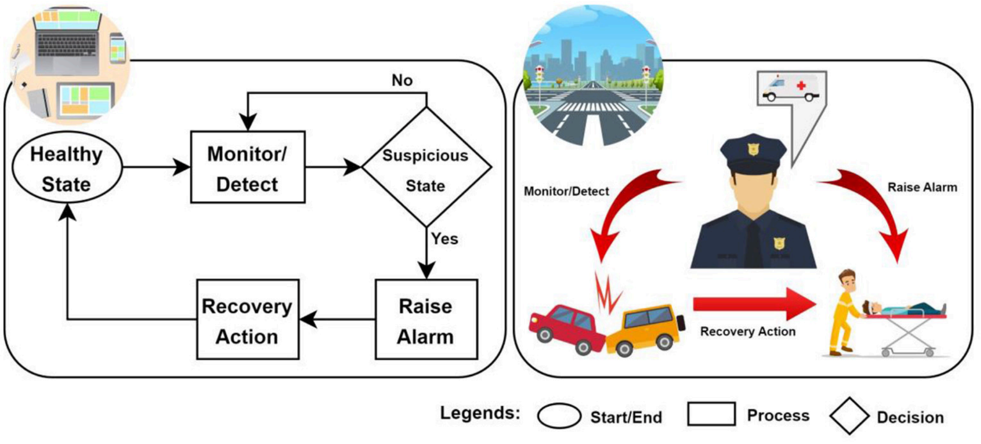


Figure 3

Figure 3

Our digital hero, a software with two key parts: a detection component, which serves as a watchful monitor similar to a police officer watching the roads, and a recovery component, like an ambulance responder providing crucial assistance in emergencies.

This is similar to a real-life situation in which a policeman calls an ambulance after an accident occurs. The ambulance rescuer collects important information from the police and works to understand the damage and rescue injured people. By testing our software with simulated threats, we found that it successfully detected the threats and could repair the damage caused by our mock-attack! In a nutshell, we built a digital hero to safeguard our digital environment.

ENJOYING A SAFE AND SECURE EXPERIENCE WHILE USING OUR DEVICES

Several institutions are putting plans in place to help people use ICT safely. For instance, the International Telecommunication Union (ITU) - the specialized agency from the United Nations for digital technology - provides a series of guidelines on how to minimize the risk and protect children while using ICT's [5]. In the USA, the Children's Online Privacy Protection Act (COPPA) was created to protect children using ICT. It prohibits websites from getting children's personal information without the agreement of their parents [6].

To keep yourself safe while enjoying the ICT universe, you should be aware of the risks and acquire good behaviors. Be cautious when accessing and using websites and email boxes; only access websites that are suggested and approved by teachers/parents; not download files from unknown senders; limit the number of downloaded applications on your devices; and, finally, tell your teachers/parents about any abnormal or offensive behaviors, such as cyber-bullying or hate messages.

CONCLUSION

ICT can be a wonderful resource for learning, working, and having fun. However, these technologies can also carry threats that endanger everyone's safety. In this article, we told you about some of those threats and summarized some ways that the research community and institutions are working on making ICT safer and more secure. We also provided some basic precaution tips you can use for fear-free ICT usage. By ensuring everyone uses ICT safely, we can keep everyone protected and able to enjoy a safer and happier life, in strong and trusted countries—just like SDG 16 envisions. We hope you become more aware of cybersecurity and share its importance in keeping our societies safe.

ACKNOWLEDGMENTS

We would like to thank Nicki Talbot at KAUST for her invaluable support during the review process, without which this collection would not have been possible. We would also like to extend our gratitude to the Office of Sustainability and UNDP-Saudi Arabia Country Office for their dedication to raising awareness of the importance of the UN SDGs in our journey toward fight for a more sustainable world.

REFERENCES

1. United Nations 2015. *Transforming Our World: The 2030 Agenda for Sustainable Development*. Available at: https://www.un.org/sustainabledevelopment/development-agenda/
2. Blancaflor, E., Beltran, S. S., Jayag, J. E., Obog, A., Salem, F. E., and Sungahid, M. D. 2022. "A security assessment on malwares disguised as children's applications", *2022 7th International Conference on Multimedia communication Technologies (ICMCT)* (Xiamen, China). p. 15–19. doi: 10.1109/ICMCT57031.2022.00012
3. Madi, T., and Esteves-Verissimo, P. 2022. "A fault and intrusion tolerance framework for containerized environments: a specification-based error detection approach", *2022 International Workshop on Secure and Reliable Microservices and Containers (SRMC)* (IEEE).
4. Konstantinou, C., Wang, X., Krishnamurthy, P., Khorrami, F., Maniatakos, M., and Karri, R. 2022. HPC-based malware detectors actually work: transition to practice after a decade of research. *IEEE Des. Test.* 39:23–32. doi: 10.1109/MDAT.2022.3143438
5. International Telecommunication Union n.d. *Child Online Protection Guidelines*. Available at: https://www.itu-cop-guidelines.com/

6. Children's Online Privacy Protection Act 1998. 15 U.S.C. §§ 6501–6506. Available at: https://www.ftc.gov/legal-library/browse/statutes/childrens-online-privacy-protection-act

SUBMITTED: 05 March 2024; **ACCEPTED:** 22 August 2024;
PUBLISHED ONLINE: 11 September 2024.

EDITOR: Rúben Martins Costa, King Abdullah University of Science and Technology, Saudi Arabia

SCIENCE MENTORS: Emma Louise Nason

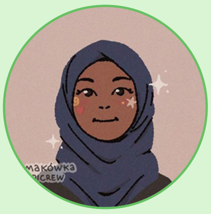
CITATION: Madi T, Konstantinou C and Esteves-Verissimo P (2024) Towards SDG 16: Safe and Secure Use of Digital Technologies. Front. Young Minds 12:1396135. doi: 10.3389/frym.2024.1396135

CONFLICT OF INTEREST: 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.

YOUNG REVIEWERS

AISYAH, AGE: 14
I am a little science enthusiast with Social Studies somehow being my favorite subject. When I am not working on school, I am cooking up dishes, jumping up in badminton or slumped down in front of a coding course.

KATERINA, AGE: 9
I love animals and plants. I am very curious to explore the world I live in and learning more about science. My hobbies are doing gymnastics, swimming, and school. Also, music, art, and math.



SHIRHAN, AGE: 16
My favorite subject in school is science and a specific science I am really interested in is earth and plant science. However astronomy has always fascinated me. When I am not learning about different sciences, I enjoy reading and creative writing. It has been a privilege to work with many people on the Frontiers for Young Minds project!

ZAHRAA, AGE: 16

I am a dedicated student interested in science and mathematics and their application in our daily lives. I have enjoyed joining the Frontiers for Young Minds program and growing my knowledge about matters such as cybersecurity and the world around us.

AUTHORS

TAOUS MADI

Taous Madi is currently an Experienced Researcher at Ericsson Canada. Previously, she served as a Research Scientist at the Resilient Computing and Cybersecurity Center (RC3) in King Abdullah University of Science and Technology (KAUST). She holds a Ph.D. in Information Systems Engineering from Concordia University, Montreal. Her research interests include security in 5G and beyond telecommunication networks, machine learning, and formal verification. She has co-authored a book and several conference and journal articles at reputable cybersecurity venues.

CHARALAMBOS KONSTANTINOU

Charalambos (Harrys) Konstantinou is currently an Associate Professor with the Computer, Electrical and Mathematical Science and Engineering Division, King Abdullah University of Science and Technology (KAUST), Saudi Arabia. He is the Principal Investigator (PI) of the Secure Next Generation Resilient Systems Laboratory (SENTRY Lab). He received the M.Eng. degree in ECE from the National Technical University of Athens, Greece, and the Ph.D. degree in Electrical Engineering from New York University, NY, USA. Before joining KAUST, he was an Assistant Professor with the Center for Advanced Power Systems, Florida State University. His research interests include critical infrastructures security and resilience with special focus on smart grid technologies, renewable energy integration, and real-time simulation. *charalambos.konstantinou@kaust.edu.sa

PAULO ESTEVES-VERISSIMO

Paulo Esteves-Veríssimo is a professor at KAUST and Director of its Resilient Computing and Cybersecurity Center. He is also Research Fellow of SnT at the University of Luxembourg (LU) and Adjunct Professor of ECE at Carnegie Mellon University (US). He is Fellow of IEEE and of ACM, and author of over 200 peer-refereed publications and co-author of 5 books. He is currently interested in resilient computing, in areas like: SDN-based infrastructures; autonomous vehicles; distributed control systems; digital health and genomics; or blockchain and cryptocurrencies.