IETI Transactions on Engineering Research and Practice
http://ieti.net/TERP/

2023, Volume 7, Issue 2, 13-20, DOI 10.6723/TERP.202312_7(2).0003

INCREASING THE SECURITY AND PRIVACY OF DIGITAL INFORMATION BY PROTECTING AND ENCRYPTING FILES FOR PERSONAL AND SHARED USE

Rusko Filchev[1,a]
[1]Technical University of Varna, №1 Studentska str., 9010, Varna, Bulgaria
[a]rusko.filchev@tu-varna.bg

Abstract The research presents applied technical means for increasing the security and privacy of digital information by using resources available to users. In a systematized form, the specific needs and requirements for securing files, which must be ensured with good quality and increased protection, are summarized. This includes both personal information and financial, health, and other confidential data concerning an individual or society as a whole. In the research, various methods of ensuring security and protection are applied, and the means and way of working is presented in an open form, so that the obtained results will be useful for a wide range of users.

Keywords: Human factors; cybersecurity; data protection; digital data transfer; encryption.

1. INTRODUCTION

In recent years, digitization has been present in a large part of our daily lives. Apart from carrying out certain activities, every person has contact with digital data characterizing his personal data and personal facts. Information can be qualified with varying degrees of importance. From one that is temporary in nature (for example, entertainment, information received daily from the mass media), customized for educational or applied needs, and one of high importance that concerns personal security (personal ID card, driver's license, other professional or personal identification, financial and banking data and others). The availability of information concerning personal security predisposes the individual person or group of people (organizations, business companies, public and financial organizations and others) to take actions to ensure and increase the security and protection of digital data (stored on certain computer files) [1-9].

The protection of personal data, which are already in a number of digital databases (of state organizations related to passport, health, driving, etc., as well as financial data provided to banking and other organizations and companies) are a sufficient condition, every citizen, as well as the related organization to take a serious approach to ensuring maximum protection of information. It is personal, moral, legislative, etc. responsibility, but it is important to take into account the human factors, which on the one hand affect the personal actions of citizens, on the other of public and other organizations, as well as the prevention against ill-wishers who seek to stole and/or gain personal information with malicious intent [10-16]. Apart from the personal actions of each of the parties, there is another danger with the so-called automated malicious software, used by hackers

2023, Volume 7, Issue 2, 13-20, DOI 10.6723/TERP.202312_7(2).0003

personally or automatically acting through artificial intelligence. All these aspects are covered by the area of cyber security, which is wide-ranging and one of the most significant in modern society, where practically every citizen is in relative insecurity and needs increased digital protection of personal and other important information data [17-20]. The purpose of the report is to summarize, after experimenting with various available technical means to provide digital protection to users.

2. SECURITY AND PROVISION OF DIGITAL PROTECTION OF PERSONAL FILES FOR PERSONAL USE

There are many options and different ways to encrypt files, folders and system drives. Despite the often presented positive qualities of encryption, it should be known that it is imperative to provide additional protection in parallel, such as secure storage of access and protection passwords, otherwise in case of password loss or a bad approach to choosing a technical means - a certain type of software or poor operation may cause irreparable damage to the computer software and/or operating system as a whole.

2.1. Encryption With Free and Open Source Software 7-zip

By far the most available (free and open source) software is 7-Zip [21]. Apart from the fact that every user can use it, working with it is relatively much easier. To ensure the protection of the file archive, it is necessary to directly enter and repeat the password [22] in the field specified for this when creating the archive (Figure 1). When the procedure is completed, the archive is successfully created, and in order to be able to use it in the future, it is necessary to enter the correctly created password when starting the file archive (Figure 2).

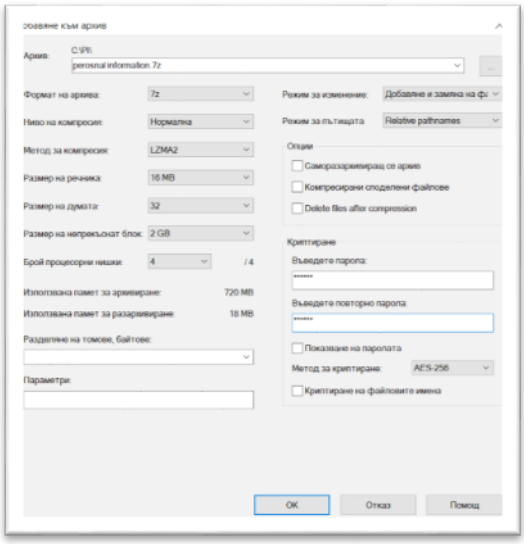


Figure 1. Create an encrypted (adding password) archive in 7-Zip.

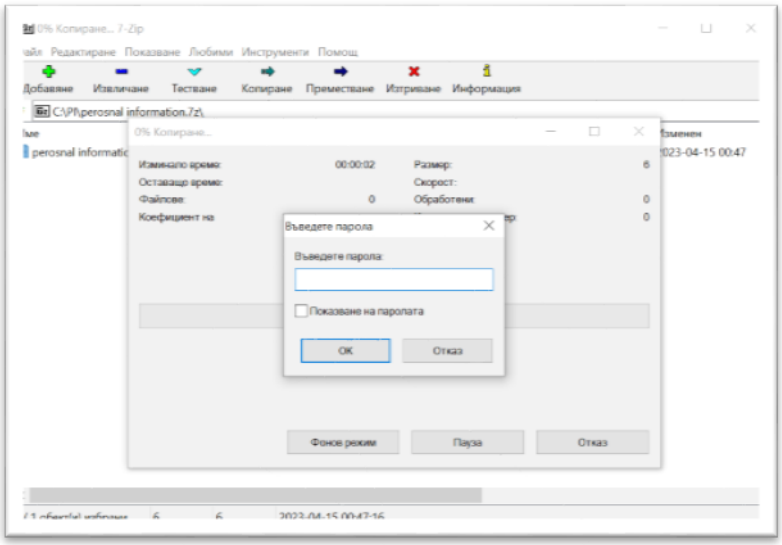


Figure 2. Open contents of encrypted archive in 7-Zip (password required).

Main features of the 7-Zip software are [23]:

- Open architecture

2023, Volume 7, Issue 2, 13-20, DOI 10.6723/TERP.202312_7(2).0003

- High compression ratio
- Strong AES-256 encryption
- Ability of using any compression, conversion or encryption method
- Supporting files with sizes up to 16000000000 GB
- Unicode file names
- Solid compressing
- Archive headers compressing

7-Zip supports encryption using the AES-256 algorithm. This algorithm uses an encryption key with a length of 256 bits. To generate this key, 7-Zip uses a derivation function based on the SHA-256 hash algorithm. A key derivation function generates a derived key from a text password defined by the user. To increase the cost of exhaustive search for passwords, 7-Zip uses large number of iterations to generate cipher key from text password [24]. In general, 7-zip is considered a robust file encryption and protection software, but the fact that the newly created archive file (with password included) is visible in the folder already makes it a target for hackers who, with programs like Hashcat software and others make attempts to break through the defense [25-33]. For this reason, it is desirable for users to use longer and more complex passwords, as well as to look for opportunities for additional protection, through combined methods with different technical means and not to trust only one. For example, additional security can be created by hiding the file(s) in the folder as presented in point 2.2.

2.2. Encryption Without Specialized Software

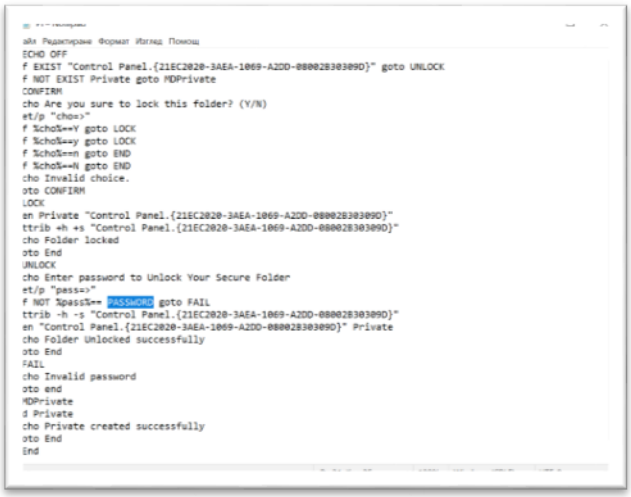
Encryption without specialized software is of great importance if the user is not sure of the technical reliability of the available encryption software. Given this, it is a good idea to use the scripting resources directly in Windows Notepad, with the final option being converted to a suitable executable for direct protection [34-35]. Containing script refers to the string "Control Panel" (Windows shell command that can be used to open a folder that has been encrypted using the built-in Windows EFS (Encrypting File System) feature). When a folder is encrypted using EFS, its name and contents are encrypted with a symmetric key, which is in turn encrypted with a public key associated with the user's EFS certificate. The user can access the encrypted folder by using their EFS certificate and private key to decrypt the symmetric key and access the folder. To open an encrypted folder in Windows, can use the command in the Run dialog box or from the command prompt. This will open the encrypted folder in Windows Explorer, allowing the user to access its contents. This command only works if the user has the necessary EFS certificate and private key to decrypt the folder. The batch script is written in the Windows Command Prompt (CMD) language. The script appears to be a simple file/folder locking mechanism that asks the user to input a password to lock or unlock a folder named "Private". When the folder is locked, its attributes are set to hidden and system. When the correct password is inputted, the folder is open to use [34, 35].

The most important point in a fully working script is to replace "PASSWORD" with the author's newly created password, which he must keep (and/or remember), Figure 3. When the script is ready and the new password is created, save the file with the extension *.bat, and it is very important to select all files and the setting in notepad: Encoding ANSI (Figure 4). By running the created bat file (*.bat) in Windows, a folder named "private" is automatically created, in which the files that need

IETI Transactions on Engineering Research and Practice
http://ieti.net/TERP/

2023, Volume 7, Issue 2, 13-20, DOI 10.6723/TERP.202312_7(2).0003

to be protected can be placed. By running the created bat file (*.bat) in Windows, a folder named "private" is automatically created, in which the files that need to be protected can be placed. Using in future newly created *.bat file the "private" folder can be repeatedly locked (Figure 5) with "y" and key enter and unlocked with the password and key enter (Figure 6).



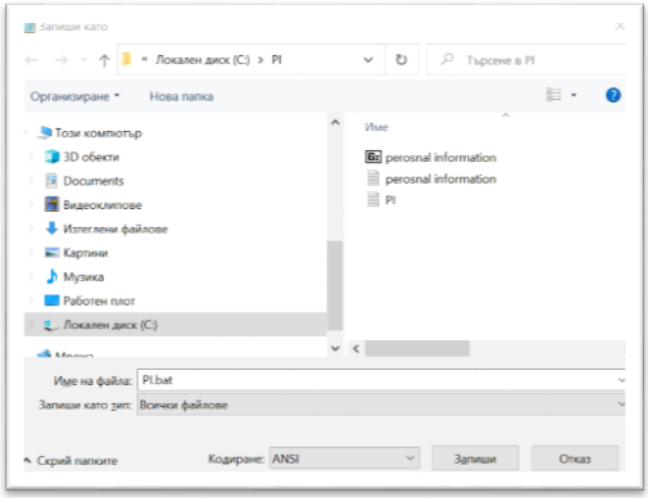
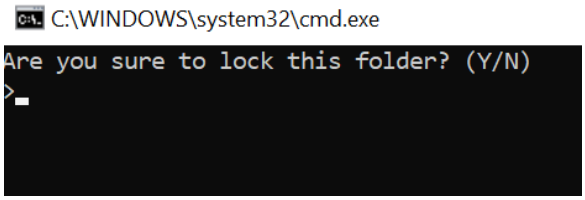


Figure 3. Enter a script directly into Windows Notepad, providing digital protection (need to enter a personal user password in place of „PASSWORD“), [34, 35].

Figure 4. Saving the file: enter a file name with the extension .bat - all files are specified in the parameters and for encoding: ANSI.



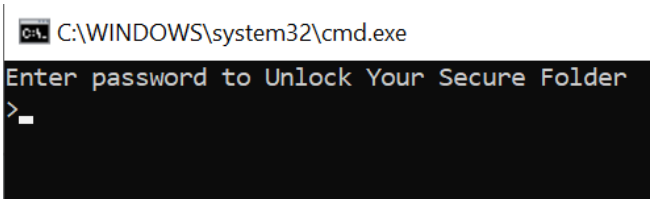


Figure 5. Locking the folder.

Figure 6. Unlocking the secure folder.

This type of file protection also has a purely visual advantage over other methods, making files invisible, which for ill-prepared attackers will be quite enough to protect the user's digital data.

3. SECURITY AND DIGITAL PROTECTION OF FILES FOR ONLINE TRANSFER BETWEEN DIFFERENT USERS

In the online transfer of digital data between users, the protection of information is also of great importance. This gives rise to the need to search for new ways and means to ensure protection, by encryption on the one hand, so that digital information is not intercepted by foreign intervention (external or by the email provider) [36-38]. The Tutanota Online System application for the transfer of encrypted digital data is particularly popular [39]. The Tutanota's encryption and security measures make it a highly secure email service provider that is trusted by individuals and

IETI Transactions on Engineering Research and Practice
http://ieti.net/TERP/

2023, Volume 7, Issue 2, 13-20, DOI 10.6723/TERP.202312_7(2).0003

businesses alike who value privacy and security. Tutanota online system uses end-to-end encryption to secure its users' emails, contacts, and calendar entries. This means that the contents of a message are encrypted on the sender's device before being sent to Tutanota's servers, and remain encrypted until they are decrypted on the recipient's device. This process ensures that no one except the sender and the recipient can access the contents of the email, including Tutanota's own staff. Also to end-to-end encryption, Tutanota online system uses other security measures to protect its users, such as SSL/TLS encryption for secure connections, and automatic encryption of metadata, such as the subject line and the sender and recipient email addresses. This ensures that even if a hacker intercepts the metadata, they won't be able to read it. The online data transfer process of a secure encrypted file is shown in Figures 7 (Tutanota workspace - sender), Figure 8 (Receiving a secure email with direct link to the file) and Figure 9 (entering the required password - recipient).

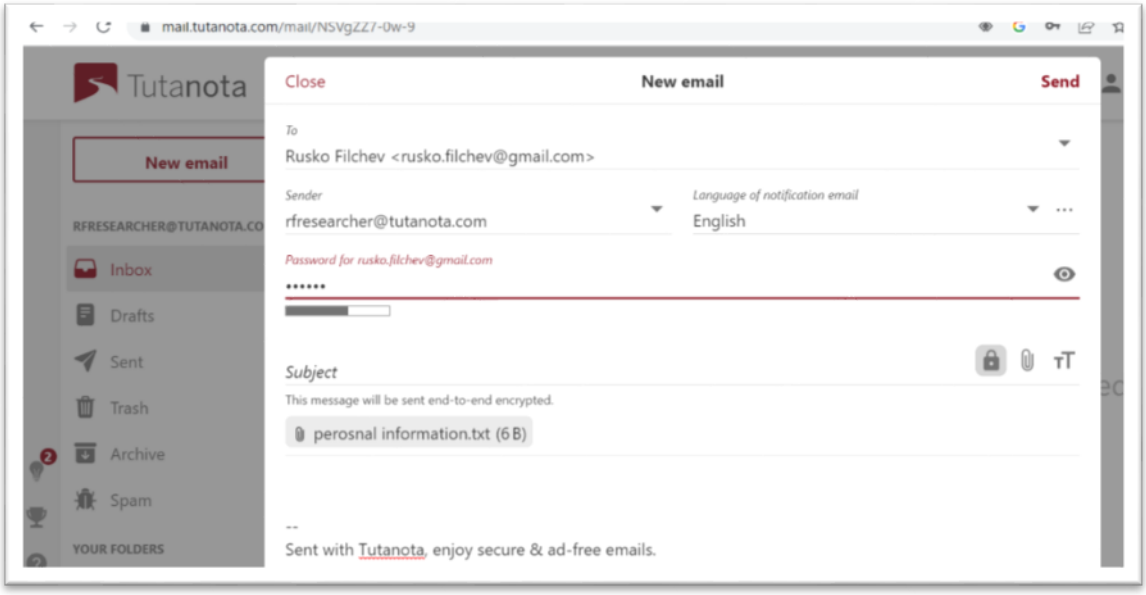


Figure 7. Tutanota workspace – sender: specify the recipient's email by entering the password directly in the required field / attach file/s.

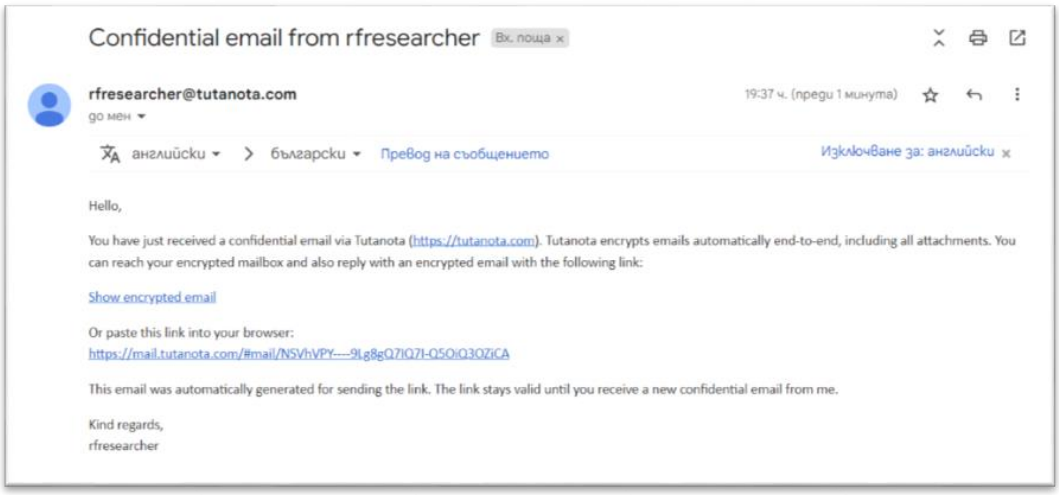


Figure 8. Received secure email (recipient email interface): to open the content, the indicated direct link is activated.

IETI Transactions on Engineering Research and Practice
http://ieti.net/TERP/

2023, Volume 7, Issue 2, 13-20, DOI 10.6723/TERP.202312_7(2).0003

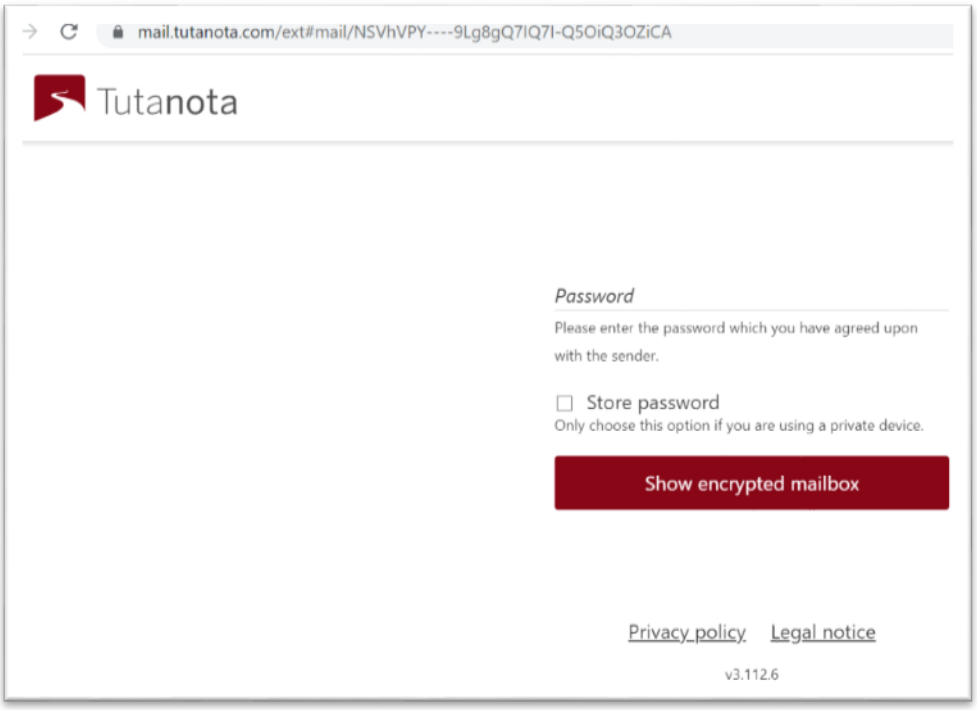


Figure 9. Require recipient to enter password to access content.

4. CONCLUSION

This article explores the extremely serious and important issue of providing affordable technical means and methods for personal computer-based digital data protection, transmission and encryption using scripts and open source software. The article makes a strong scientific and applied contribution, highlighting the importance of the problem and offering real solutions for the benefit of users. The research results contribute to:

- Raise citizens' awareness of the use of accessible technical tools, software and resources for digital protection;
- increase the computer literacy of a large number of citizens - users of digital services where protection is needed;
- the overall digital protection of users in an online communication environment;
- the development of a digital society in the field of cybersecurity.

Acknowledgements

- The study was conducted with the support of CIII-HU-1506-01-2021 Ergonomics and Human Factors Regional Educational CEEPUS Network.
- Bulgarian Association of Ergonomics and Human Factors (BAEHF).

2023, Volume 7, Issue 2, 13-20, DOI 10.6723/TERP.202312_7(2).0003

References

[1] Maglaras L., Kantzavelou I. and Ferrag M.A., 2021, Digital Transformation and cybersecurity of critical infrastructures, *Applied Sciences*, 11(18), 8357. doi:10.3390/app11188357.

[2] Burov O., Butnik-Siversky O., Orliuk O. and Horska K., 2020, Cybersecurity and Innovative Digital Educational Environment, *Information Technologies and Learning Tools*, 80(6), pp. 414–430.

[3] Slavković M, Pavlović K, Mamula Nikolić T, Vučenović T, Bugarčić M., 2023, Impact of Digital Capabilities on Digital Transformation: The Mediating Role of Digital Citizenship, *MDPI Systems*, 11(4),172. https://doi.org/10.3390/systems11040172

[4] Rupeika-Apoga R, Petrovska K, Bule L., 2022, The Effect of Digital Orientation and Digital Capability on Digital Transformation of SMEs during the COVID-19 Pandemic, *Journal of Theoretical and Applied Electronic Commerce Research*, 17(2), 669-685.

[5] Rawindaran N, Jayal A, Prakash E., 2022, Exploration of the Impact of Cybersecurity Awareness on Small and Medium Enterprises (SMEs) in Wales Using Intelligent Software to Combat Cybercrime, *MDPI Computers*, 11(12), 174. https://doi.org/10.3390/computers11120174

[6] Bahaddad AA, Almarhabi KA, Alghamdi AM., 2022, Factors Affecting Information Security and the Implementation of Bring Your Own Device (BYOD) Programmes in the Kingdom of Saudi Arabia (KSA), *MDPI Applied Sciences*, 12(24), 12707. https://doi.org/10.3390/app122412707

[7] Han Q., 2017, Personal Data Protection Strategy Research Based on the Theory of Information Ecology, *Proceedings*, 1(3),147. https://doi.org/10.3390/IS4SI-2017-04073

[8] Drosatos G, Rantos K, Demertzis K., 2022, Advanced Technologies in Data and Information Security, *Applied Sciences*, 12(12), 5925. https://doi.org/10.3390/app12125925

[9] Taylor MJ, Whitton T., 2020, Public Interest, Health Research and Data Protection Law: Establishing a Legitimate Trade-Off between Individual Control and Research Access to Health Data, *Laws*, 9(1), 6. https://doi.org/10.3390/laws9010006

[10] Li S-C, Chen Y-W, Huang Y. 2021, Examining Compliance with Personal Data Protection Regulations in Interorganizational Data Analysis, *Sustainability*, 13(20), 11459. https://doi.org/10.3390/su132011459

[11] Calzada I., 2022, Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL), *Smart Cities*, 5(3), 1129-1150.

[12] Holbl M, Kežmah B, Kompara M., 2021, Data Protection Heterogeneity in the European Union, *Applied Sciences*, 11(22), 10912. https://doi.org/10.3390/app112210912

[13] Yuan B, Li J., 2019, The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation, *International Journal of Environmental Research and Public Health*, 16(6), 1070. https://doi.org/10.3390/ijerph16061070

[14] Maniadaki M, Papathanasopoulos A, Mitrou L, Maria E-A., 2021, Reconciling Remote Sensing Technologies with Personal Data and Privacy Protection in the European Union: Recent Developments in Greek Legislation and Application Perspectives in Environmental Law, *Laws*, 10(2), 33. https://doi.org/10.3390/laws10020033

[15] Nifakos S, Chandramouli K, Nikolaou CK, Papachristou P, Koch S, Panaousis E, Bonacina S., 2021, Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review, *Sensors*, 21(15), 5119. https://doi.org/10.3390/s21155119

[16] Szabó G., Balogh Z., Dovramadjiev T., Draghici A., Gajšek B., lulić T. Jurčević, Reiner M., Mrugalska B., Zunjic A., 2021, Introducing the Ergonomics and Human Factors Regional Educational CEEPUS Network, *Acta Technica Napocensis, Series: Applied Mathematics, Mechanics, and Engineering*, 64 (1), pp. 201-212.

[17] Diamantopoulou V, Androutsopoulou A, Gritzalis S, Charalabidis Y., 2020, Preserving Digital Privacy in e-Participation Environments: Towards GDPR Compliance, *Information*, 11(2), 117. https://doi.org/10.3390/info11020117

2023, Volume 7, Issue 2, 13-20, DOI 10.6723/TERP.202312_7(2).0003

[18] Friedhoff T, Au C-D, Ladnar N, Stein D, Zureck A., 2023, Analysis of Social Acceptance for the Use of Digital Identities, *Computers*, 12(3), 51. https://doi.org/10.3390/computers12030051
[19] Appenzeller A, Hornung M, Kadow T, Krempel E, Beyerer J., 2022, Sovereign Digital Consent through Privacy Impact Quantification and Dynamic Consent, *Technologies*, 10(), 35. https://doi.org/10.3390/technologies10010035
[20] Lax G, Russo A., 2022, Advances in Information Security and Privacy, *Applied Sciences*, 12(16), 7995. https://doi.org/10.3390/app12167995
[21] 7-Zip open source software, Website https://www.7-zip.org/ (Accessed March 2023).
[22] Shelton Y., 2023, How to Encrypt & Password Protect your Files with 7-Zip, https://7ziphelp.com/password-protect-on-7zip (Accessed March 2023).
[23] 7-Zip open source software. Main features of the 7-Zip software, https://www.7-zip.org/7z.html (Accessed March 2023).
[24] Josef Huˇsek J., 2029, The use of cryptography in 7-zip. Bachelor's thesis, https://dspace.cvut.cz/bitstream/handle/10467/83024/F8-BP-2019-Husek-Josef-thesis.pdf (Accessed March 2023).
[25] Hashcat, Advanced password recovery software, https://hashcat.net/hashcat/ (Accessed March 2023).
[26] Infinite Logins. How to Crack Encrypted 7z Archives, 2020, https://infinitelogins.com/2020/04/29/how-to-crack-encrypted-7z-archives/ (Access March 2023).
[27] Nam S, Jeon S, Kim H, Moon J., 2020, Recurrent GANs Password Cracker For IoT Password Security Enhancement, *Sensors*, 20(11), 3106. https://doi.org/10.3390/s20113106
[28] Nam S, Jeon S, Moon J., 2020, Generating Optimized Guessing Candidates toward Better Password Cracking from Multi-Dictionaries Using Relativistic GAN, *Applied Sciences*, 10(20), 7306. https://doi.org/10.3390/app10207306
[29] Taneski V, Kompara M, Heričko M, Brumen B., 2021, Strength Analysis of Real-Life Passwords Using Markov Models, *Applied Sciences*, 11(20), 9406. https://doi.org/10.3390/app11209406
[30] Mokhtar BI, Jurcut AD, ElSayed MS, Azer MA., 2022, Active Directory Attacks—Steps, Types, and Signatures, *Electronics*, 11(16), 2629. https://doi.org/10.3390/electronics11162629
[31] Wu T, Yang Y, Wang C, Wang R., 2019, Study on Massive-Scale Slow-Hash Recovery Using Unified Probabilistic Context-Free Grammar and Symmetrical Collaborative Prioritization with Parallel Machines, *Symmetry*, 11(4), 450. https://doi.org/10.3390/sym11040450
[32] Bojato J, Donado D, Jimeno M, Moreno G, Villanueva-Polanco R., 2022, Password Guessability as a Service (PGaaS), *Applied Sciences*, 12(3), 1562. https://doi.org/10.3390/app12031562
[33] Kim P, Lee Y, Hong Y-S, Kwon T. A., 2021, Password Meter without Password Exposure, *Sensors*, 21(2), 345. https://doi.org/10.3390/s21020345
[34] Pastebin, 2019, Lock Folder - Windows Chimp, https://pastebin.com/K5Y9s3e5 (Accessed March 2023).
[35] Seribu Blog, Inilah Cara Mengunci Folder Di Laptop, https://medium.com/@pemainblogger/inilah-cara-mengunci-folder-di-laptop-3d5347edd074 (Access March 2023).
[36] Winarno A, Sari RF., 2022, A Novel Secure End-to-End IoT Communication Scheme Using Lightweight Cryptography Based on Block Cipher, *Applied Sciences*, 12(17), 8817. https://doi.org/10.3390/app12178817
[37] Kim S-Y, Yun S-W, Lee E-Y, Bae S-H, Lee I-G, 2020, Fast Packet Inspection for End-To-End Encryption, *Electronics*, 9(11), 1937. https://doi.org/10.3390/electronics9111937
[38] Le T-V., 2023, Cross-Server End-to-End Patient Key Agreement Protocol for DNA-Based U-Healthcare in the Internet of Living Things, *Mathematics*, 11(7), 1638. https://doi.org/10.3390/math11071638
[39] Tutanota secure email service, The end-to-end encryption online system, https://tutanota.com/ (Accessed March 2023).