https://doi.org/10.53656/str2023-2-3-cha

*Education in the Information Society*
*Образованието в информационното общество*

# CHARACTERISTICS AND COMPONENTS OF THE CYBER HYGIENE AS A SUBCLASS OF CYBER SECURITY IN MILITARY ENVIRONMENT AND EDUCATIONAL ISSUES

**Prof. Boyan Mednikarov, DSc. Prof. Yuliyan Tsonev**
**Dr. Borislav Nikolov, Prof. Andon Lazarov, DSc.**
*Nikola Vaptsarov Naval Academy*

**Abstract.** In the present study based on the main characteristics and components of the cyber hygiene as a subclass of the cyber security, educational challenges on the cyber hygiene in military area are considered. Based on institutional experience in the scope of the cyber security in the digital environment, a sequence of activities to keep resilient and reliable cyber hygiene in army organizations are analyzed and recommended. Definitions of basic cyber hygiene characteristics are suggested. Cyber hygiene software issues and institutional information security controls are discussed. A malware infection as main cyber hygiene concern is analyzed. Fundamental cyber hygiene instructions to ensure military Internet users and institutions stay protected are defined. Exemplary curriculum for education of military staff with basic themes is presented.

*Keywords*: Cyber hygiene; Cyber security; Cyber hygiene's instructions

## 1. Introduction

Cybercrime is on the rise on the global network. Criminal hackers through phishing emails, supply chain, password and malware attack millions of users' workstations. In the last two years, the number of global ransomware attacks have reached above 600 million. This requires special measures that need to be taken by organizations, network administrators and users to counter this global threat (Singh 2020, Such 2022, Trevors 2017).

Cyber hygiene provides protection and security in maintenance and exploitation of the computer networks. Multiple points of view regarding issues that arise with different cyber attackers, cyber threats and cyber-risks from that can be referred to cyber-hygiene of individuals and institutions are considered in (Singh 2020). Effectiveness of the Cyber Essentials scheme and its security activities that mitigate the threats they were designed for, i.e., those threats exploiting vulnerabilities remotely is discussed in (Such 2022).

Malicious network users scan network devices for vulnerable devices, investigate network security mechanisms, and detect vulnerabilities in the network to retrieve security layer (SSL) certificates or invalid URLs. During the Cyber Kill Chain recognition phase, security software is evaluated and vulnerabilities are identified (FS-ISAC 2021).

Methodology for realization of cyber hygiene practices in Smart Grid Systems, focused on smart metering systems is proposed and tested in (Trevors 2017). It is proven that implementing cyber hygiene instruments can improve smart meter cybersecurity and be suitable for implementing other sensitive Smart Grid components

Effective cyber hygiene is challenging tasks for the entire institution, and the responsibility of individual employees. If the role of cyber hygiene is to be summarized, it is responsible for the integrity and availability of data. Cyber hygiene includes many rules and activities to ensure cyber security.

A list of main activities in the scope of the cybersecurity and cyber hygiene including a set of practices for managing the most common and pervasive cybersecurity risks faced by employee and institutions is discussed in (Ead 2022).

It is compulsory, that users must follow strictly a high level of cyber hygiene in financial analytical area, security and military sphere, marine and air traffic control, etc., having in mind that many employee keep not good cyber hygiene. They openly exchange passwords and share private information on social networks.

Analysis of end-user's behavior to promote the creation of more successful approaches in the financial analytical climate is provided in (Olivares-Rojas 2022). It includes recommendations that allow improving the institution's cyber hygiene in access to financial solutions in the area. A cyber hygiene checklist to prevent attacks on computer networks and rules of cyber hygiene that has to follow by institutions and internet user are discussed in (Bedrich, RSI Security 2021).

There are different definitions of the term "cyber hygiene". There is no consensus on what constitutes cyber hygiene. Different national institutions have their own specific recommendations and rules, i.e. there is no single standard or commonly accepted mechanism for an institution to assess, evaluate or demonstrate cyber hygiene. The main characteristic of the cyber hygiene, cybersecurity ratings and measures, common cyber hygiene problems and practices are discussed in (Tyas 2022).

The rest of the article is organized as follow. Section II suggests cyber hygiene definitions, cyber hygiene – basic software issues, cyber hygiene – institutional information security controls. Section III discloses malware infections – cyber hygiene main concerns. Section IV presents a subject of the curriculum in cyber hygiene. Section V gives conclusion remarks.

## 2. Cyber hygiene as a subclass of cyber security

### *2.1 Cyber hygiene definitions*

Cyber hygiene as a part of cyber security refers to the network users and institutions as a whole. It is a system of instructions and recommendations aimed at improving users' activity to help them gain knowledge and skills that guarantee network security, and thus ensure system cyber health. The cyber hygiene is a multilayer system of rules and activities users have to follow working in Internet. It is a distinctive feature. From other hand, cyber hygiene means abilities and habits that help users and organizations mitigate the networks potential vulnerability to cyber-attacks and enhance resilience against threats of cyber-attacks.

Cyber hygiene includes an aggregate of user's habitual skills and activities to ensure secure data exchange and resilience of networks and network devices to cyber impacts. It's similar to the classical medical hygiene each person has to follow. It consists of routine activities to prevent or mitigate health problems. Cyber hygiene practice includes the surveillance of all end devices connected to local networks, control of vulnerabilities, regular update and patching of the computers' software components. Cyber hygiene is not only responsibilities of detached employee and/or personnel but institution's and command stuff obligations, and network administrators. Cyber hygiene means training to form professional habits ensuring cybersecurity so that to prevent network cyber threats and internet security issues. Cyber hygiene aims to maintain hardware and software's basic health and security, ensuring they are protected from threats such as malware. Applied in everyday life, cyber hygiene helps to keep data, hardware and software safe and secure. As with any habit to be gained, cyber hygiene skills require learning and practical education to apply specific routine and repetition activities.

The routine in respect of cyber hygiene helps prevent cybercriminals from causing network intrusions, security breaches or stealing personal information. It helps keeping software and operating systems up to date.

### *2.2 Cyber hygiene – basic software issues*

Basic software issues that are in the focus of the cyber hygiene are as follows.

– Security breaches caused by threats from hacker's attacks as phishing, malware, and viruses.

– Data loss caused by not reserved hard drives and virtual cloud storage vulnerable to unauthorized penetration and corruption.

– Vulnerability to cyber-attacks caused by out of date software;

– Cyber threats caused by obsolescent, i.e. not up to date antivirus security software that is less effective at protecting to newest software attacks.

Therefore, to ensure adequate and effective cyber hygiene, the network user must follow cyber hygiene periodicity of activities and apply the appropriate software instruments to ensure cyber hygiene.

The cyber hygiene periodicity means regular control and test routines, drawing up a schedule of different activities to be fulfilled to keep cyber hygiene on a certain level. For instance, scanning the computer for viruses using up to day antivirus programs, removing the old password and establishing new one, keeping user's applications, system software, and operating systems of all devices up to date, and cleaning computer's hard drive. Once the user assimilates the cyber hygiene rules, it becomes part of regular personal cybersecurity routine (Kaspersky lab 2023).

Appropriate software instruments to ensure cyber hygiene are as follow.

– Firewall – prevents an unauthorized access from the internet.

– Software for data-deleting prevents a risk of losing personal data while introducing new software, add on hardware, or modify system files and clears out not necessary data from the hard drive.

– A password manager maintains track of multiple passwords while using strong, complex passwords which are changed regularly to keep internet hygiene.

– Antivirus software of high quality that schedules and performs periodic scanning to detect and remove malware, and protect from multiple network threats.

– Freeing users from unusable electronic communication devices, such as laptops, smartphones, desktops, raises serious questions about cyber hygiene. The user must not only delete their files, but also reformat the hard drive of the devices. This also ensures the deletion of personal information stored on the disk.

The main rule of the cyber hygiene is maintaining the application and system software and hardware up to date. Web browsers, user and mobile applications, and network devices' operating systems have to be updated regularly. It eliminates software security issues. By regular updates new software patches are delivered to correct software failures. For instance, the vulnerability Joomla – Core – XSS (Cross-Site Scripting) Attack Vector via SVG (Scalable Vector Graphics) (2021) (CVE (Common Vulnerabilities and Exposures)-2022-23801) is discovered in versions Joomla 4.0.0 to 4.1.0 embedding in commedia. In updated version Joomla 4.1.1 the problem is fixed. Hardware updates guarantee preventing CPU performance issues.

*2.3 Cyber hygiene – institutional information security controls*

The basic controls provided by the institution are as follow (Tyas 2022):

1. Control usage of the hardware devices: It means to control only authorized devices to have access to restricted area and sensitive data.

2. Control usage of the system and application software: It means to control and mitigate risk by manage network software so that only certified and licensed software is installed on devices and can exploited.

3. Control continuous network vulnerability and risk management: It means to control acquiring regularly information in respect of new network vulnerabilities, to remove them and reduce the range of their risk impacts.

4. Control usage of administrative rights: It means to control administrative rights by access control and access restriction, such as two-stage authentication or multi-stage authentication, as well as to be created approaches and instruments to track, control, prevent and correct the use, assignment, and configuration of administrative rights.

5. Secure configuration of hardware and software on network devises: mobile sets as tablets, i-phones and laptops, and stationary workstations and servers: It means that institutions must establish, implement and actively manage the security

configuration of mobile devices as tablets, i-phones and laptops, and stationary routers, switches, servers and workstations to prevent attackers from exploiting vulnerable services and settings. This should include the use of complex passwords.

6. Analyze of audit documents: It means that institutions must collect, control and analyze audit logs of intrusion events to help the detection, identification and to recover from cyber-attacks.

In addition, there are the following foundational information security controls:

1. Email and web browser protections: It is performed by minimizing the attack fronts and opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

2. Malware defenses: It is performed by controlling the installation, spread, and execution of malicious code and to enable rapid updating of defense, data gathering, and corrective action.

3. Limitation and control of network ports, protocols, and services: It means to control and manage the ongoing functionality of ports, protocols, and services on networked devices in order to minimize vulnerabilities  available to attackers and opportunities cyber impacts.

4. Data backup and recovery capabilities: It means applying servers instruments and protocols to reliable back up critical information with an effective methodology for timely recovery of it.

5. Reliable and secure configuration of network devices, such as routers, switches and firewalls: It means the institution and network administrators to establish, implement and manage the security configuration of network infrastructure devices by configuration and processes of management, change and control to prevent cyber-attacks and exploiting vulnerabilities of services and settings.

6. Boundary defense: It means boundary defense controls detection, prevention and correction of the information flow transferring across networks of different trust levels focused on security-damaging data.

7. Data protection: Sensitive data are different types and reside in different places. It means data protection through combination of encryption, integrity protection, and data loss' prevention techniques.

8. Controlled access based on the need to know: It means institutions to use instruments and processes to track, control, prevent and correct secure access to critical data according to access control rights of operators to computers, and applications based on a need or right previously classified.

9. Wireless access control: It means to manage wireless access, processes and tools to track, control, prevent and correct the secure use of wireless local area networks (WLANs), access points and wireless client systems.

10. Account monitoring and control: It requires to control management across the life cycle of system and application accounts – their creation, use, dormancy, and deletion - to reduce opportunities for cyberattacks.

There are four institution information security controls, namely:

1. Establish a security awareness and training program: It means the institutions must build the specific knowledge, cyber security skills and abilities to ensure the cyber defense trough developing and executing a plan for identification and evaluation of problems and remediate through, planning, training and awareness programs.

2. Application software security: It means the institution must control the security of all acquired and used software over its life cycle.

3. Incident response and control: It means institution must protect their information and reputation by developing and implementing an incident emergency response infrastructure (e.g. plans, defined roles, training, communications, and management oversight) to quickly discover attacks and then contain the damage, eradicate the attacker's access and restore the integrity of the network and systems

4. Penetration tests and red team exercises: It means institution must test their overall defense (technology, processes, and employee) by simulating the objectives and actions of an attacker. This may include on-site and off-site penetration testing, network security assessments and testing the implementation of information security policies

## 3. Malware infection – cyber hygiene main concerns

### *3.1. Main Definitions*

The term “malware” means malicious software that contains a malicious and destructive code. It is intentionally designed to damage, disrupt, and steal information, slow down and disrupt the functions of network devices – computers and servers. The malware is installed on network devices by system and internet users through downloading files or opening e-mails' attached files. Malware can damage the data and software while residing on the storages and memory but it cannot harm the hardware parts of systems or network equipment. The term “virus” is usually used to define entire malicious/damaging software. However, the virus is just a type of malware.

Malware infection vectors are a multidirectional transmission of malicious codes to network platforms and devices with the aim to infiltrate, infect and spread through the system by exploiting vulnerabilities. Malware vectors capture victims who

– Trust social networking forums like Facebook, Skype, Viber, etc.

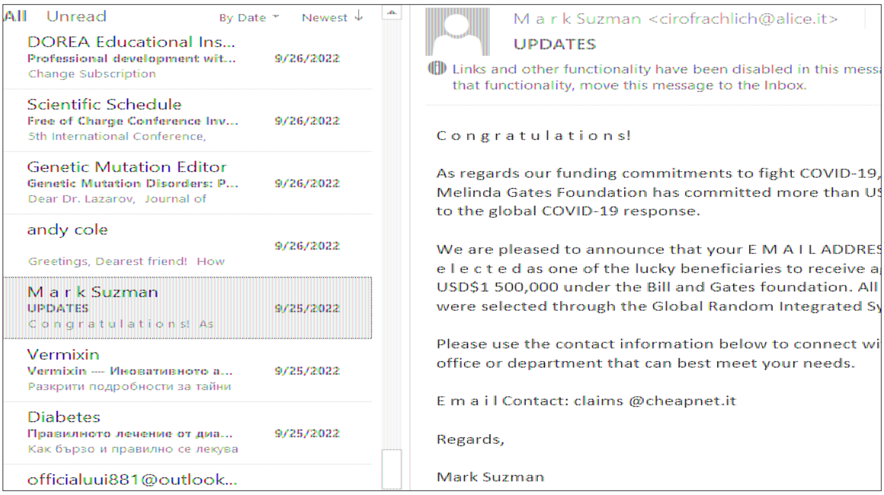
– Show inquisitiveness and curiosity about any interesting event.

– Lack expert awareness and experience.

It is important to know that accessing an account by cracking a user's email password gives the malicious user access to the attacked user's contact list, thereby gaining access to their business contacts on social networks and allowing them to attack others users. The downloaded and embedded malware contains documents as photo, movie, music, and more, providing criminal access to the entire communication system and network of the attacked user.

Local server or network computers can be infected with one or some malicious software as virus, worm, adware, crypto locker, spywares, toolkits, Trojan, botnet, etc. It performs destructive activity according to their nature like stealing of personal or confidential information of users or institutions, tracking and monitor activities of the computer, installs backdoors and keystrokes loggers, makes target server crash, harm performance of online systems, usage of system resources like CPU cycles, memory and network, encrypt sensitive data. The spyware or adware can cause sudden change in functionality. It must be aware that the infection level depends on the system defense and residence of malware on it.

Malware criminals (Kaspersky lab 2014) use social engineering techniques to distribute and infiltrate malware, and inforce users to download, embed, and run a malicious code on their systems without realizing it (Fig. 1).



DOREA Educational Ins...
Professional development wit... 9/26/2022
Change Subscription

Scientific Schedule
Free of Charge Conference Inv... 9/26/2022
5th International Conference,

Genetic Mutation Editor
Genetic Mutation Disorders: P... 9/26/2022
Dear Dr. Lazarov, Journal of

andy cole
9/26/2022
Greetings, Dearest friend! How

Mark Suzman
UPDATES 9/25/2022
Congratulations! As

Vermixin
Vermixin ---- Иновативното а... 9/25/2022
Разкрити подробности за тайни

Diabetes
Правилното лечение от диа... 9/25/2022
Как бързо и правилно се лекува

officialuui881@outlook...

Mark Suzman <cirofrachlich@alice.it>
UPDATES

Links and other functionality have been disabled in this mess
that functionality, move this message to the Inbox.

Congratulations!

As regards our funding commitments to fight COVID-19,
Melinda Gates Foundation has committed more than US
to the global COVID-19 response.

We are pleased to announce that your EMAIL ADDRES
elected as one of the lucky beneficiaries to receive a
USD$1 500,000 under the Bill and Gates foundation. All
were selected through the Global Random Integrated Sy

Please use the contact information below to connect wi
office or department that can best meet your needs.

Email Contact: claims @cheapnet.it

Regards,

Mark Suzman

**Figure 1.** A worm (virus) attack inside the attached file

Once an attacker infects a system, they can have complete control and access to that system's information and devices. Malware products exploit weak places in in the cyber defense of the computer system. Malware infections find out vulnerabilities in security in previous versions of standard software applications such as picture viewers, Media Players, Adobe and the Windows operating systems (Kaspersky lab, 2014).

Malicious internet users apply social engineering tactics to find out weak security places and to transfer monovalent code in a computer in order to install their malicious code which are able to steal confidential information. They rely on the responsiveness of people as well as their mistakes and poor cyber hygiene. Cybercriminals find vulnerabilities in a computer network to infiltrate it and gain access to personal and confidential information. This damages the security not only of an individual user, but also of the institution as a whole. All malware tools applied by cyber criminals use social engineering technique to perform their monovalent work. Several ways are applied to spread viruses using social engineering (Internet organized crime threat assessment 2015):

– Straight questioning.

– Step-by-step search for information.

– After gaining physical access.

– Reverse social engineering (reverse social engineering is a type of social engineering that aims to steal sensitive information and/or money through psychological manipulation and back contact of the victim).

– Online social engineering (social engineering is performed online).

*Market to device*: This attack is initiated by the electronic market. The malware author uploads his malicious application to the e-marketplace site using a stolen/ unauthorized identity. In the presence of malicious applications on the e-marketplace site, many users can be attacked (Internet organized crime threat assessment 2015).

*Web browser to device*: This is a virus's distribution technique typically using downloading tactics, applied recently by network cyber-attacks.

*SMS to device*: The malicious software is propagated via SMS or MMS.

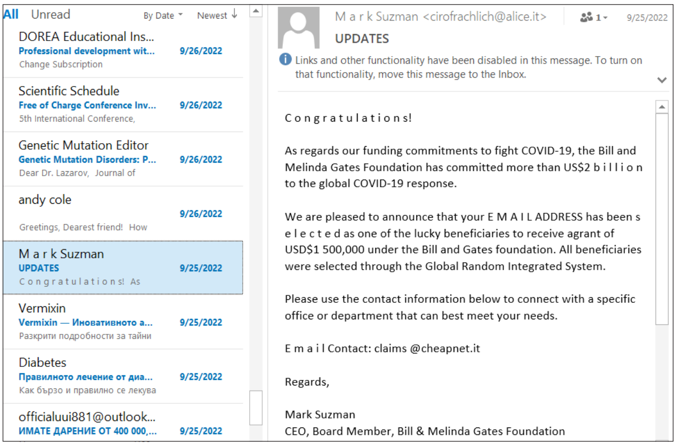
*Network to device*: It is performed by exploiting software vulnerabilities and hardware misconfigurations.

*Device to device*: The infection is disseminated from device to device in point-to-point manner.

*USB to Device*: The infection is disseminated by USB devices by connecting to an infected computer with new variants of a virus.

*Botnet*: The term “botnet” means a robotized network. Botnets are networks of computer devices infected with a malicious backdoor program used by a malicious user to automatic carrying out different cyberattacks, such as data theft, server crashing, sending spam from zombie computers to attack government and military networks, DDoS (Distributed Denial of Service) attacks, anonymous Internet access; cyber criminals’ access to web server using zombie machines to commit cybercrimes such as hacking websites or transferring stolen money, selling and leasing, allows distributing malware in computer networks.

*Phishing by a botnet*: Botnet allows changing the addresses of phishing pages frequently using infected computers as proxy servers (Fig. 2).



DOREA Educational Ins...
Professional development wit... 9/26/2022
Change Subscription

Scientific Schedule
Free of Charge Conference Inv... 9/26/2022
5th International Conference,

Genetic Mutation Editor
Genetic Mutation Disorders: P... 9/26/2022
Dear Dr. Lazarov, Journal of

andy cole
9/26/2022
Greetings, Dearest friend! How

Mark Suzman
UPDATES 9/25/2022
Congratulations! As

Vermixin
Vermixin — Иновативното а... 9/25/2022
Разкрити подробности за тайни

Diabetes
Правилното лечение от диа... 9/25/2022
Как бързо и правилно се лекува

officialuui881@outlook...
ИМАТЕ ДАРЕНИЕ ОТ 400 000,... 9/25/2022

Mark Suzman <cirofrachlich@alice.it> 9/25/2022
UPDATES

Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox.

Congratulations!

As regards our funding commitments to fight COVID-19, the Bill and Melinda Gates Foundation has committed more than US$2 billion to the global COVID-19 response.

We are pleased to announce that your EMAIL ADDRESS has been selected as one of the lucky beneficiaries to receive agrant of USD$1 500,000 under the Bill and Gates foundation. All beneficiaries were selected through the Global Random Integrated System.

Please use the contact information below to connect with a specific office or department that can best meet your needs.

Email Contact: claims @cheapnet.it

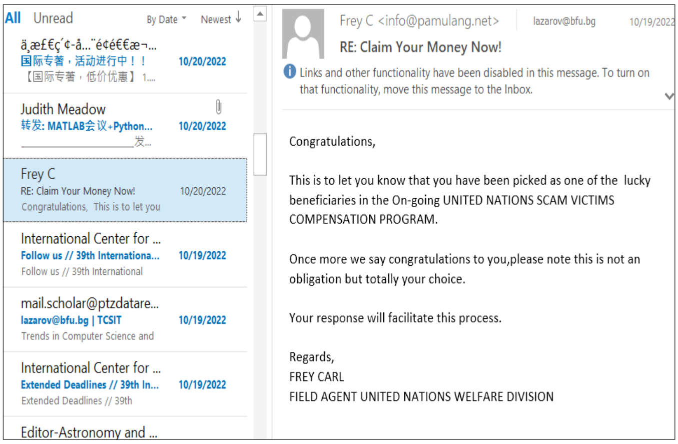
Regards,

Mark Suzman
CEO, Board Member, Bill & Melinda Gates Foundation

**Figure 2.** Phishing e-mail attack

*Virus*: a type of malware attached to another software document or a legitimate program. It makes multiple replicates, infects and corrupts other files without user's awareness.

*Trojan horse*: a type of malicious malware hidden or embedded in an email attachment or in a program such as a computer game, attractive to encourage a user to install it. The most insidious (and ironic) types of Trojan Horses are programs that offer to clear user's computer of viruses, but instead deliver viruses to victim's computer illustrated in Fig. 3.



ä¸æ£€ç´¢-å…¨é¢é€€æ¬...
国际专著，活动进行中！！ 10/20/2022
【国际专著，低价优惠】 1....

Judith Meadow
转发: MATLAB会议+Python... 10/20/2022
________________发...

Frey C
RE: Claim Your Money Now! 10/20/2022
Congratulations, This is to let you

International Center for ...
Follow us // 39th Internationa... 10/19/2022
Follow us // 39th International

mail.scholar@ptzdatare...
lazarov@bfu.bg | TCSIT 10/19/2022
Trends in Computer Science and

International Center for ...
Extended Deadlines // 39th In... 10/19/2022
Extended Deadlines // 39th

Editor-Astronomy and ...

Frey C <info@pamulang.net> lazarov@bfu.bg 10/19/2022
RE: Claim Your Money Now!

Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox.

Congratulations,

This is to let you know that you have been picked as one of the lucky beneficiaries in the On-going UNITED NATIONS SCAM VICTIMS COMPENSATION PROGRAM.

Once more we say congratulations to you,please note this is not an obligation but totally your choice.

Your response will facilitate this process.

Regards,
FREY CARL
FIELD AGENT UNITED NATIONS WELFARE DIVISION

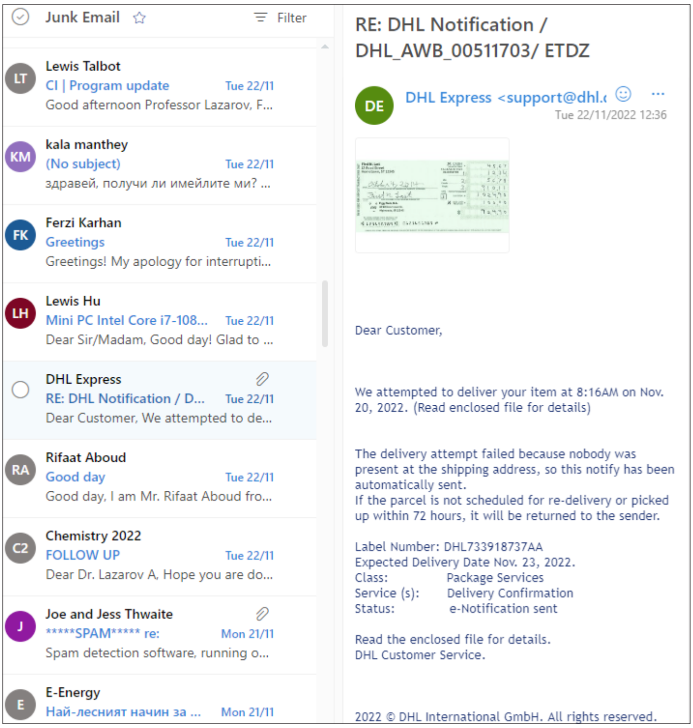
**Figure 3.** Trojan horse: Answer to this e-mail letter instead protection and viruses cleaning delivers viruses to a victim computer

*Spyware*: a type of malware installed on computers or network devices without knowledge of the user. The spyware activated on computers collects and transmits personal and institutional information as passwords, and numbers of credit card.

*Ransomware*: is a type of malware applying an encryption code to lock and/or block user's access to a computer system or user's files until a specific amount of money is paid – usually by cryptocurrency (e.g. Bitcoin), since the transaction cannot be traced or refunded. In case the ransom is not paid, then the system's and victim's files are destroyed.

*Computer Worm*: a type of malware, a self-replicating program that copies itself from computer to computer. Rather than infect files, its main purpose is to use resources such as computer memory and network bandwidth to inflict damage.

Computer worm infection is illustrated in Fig. 4. The malware (worm) is inside the attached file.



LT Lewis Talbot
CI | Program update Tue 22/11
Good afternoon Professor Lazarov, F...

KM kala manthey
(No subject) Tue 22/11
здравей, получи ли имейлите ми? ...

FK Ferzi Karhan
Greetings Tue 22/11
Greetings! My apology for interrupti...

LH Lewis Hu
Mini PC Intel Core i7-108... Tue 22/11
Dear Sir/Madam, Good day! Glad to ...

DHL Express
RE: DHL Notification / D... Tue 22/11
Dear Customer, We attempted to de...

RA Rifaat Aboud
Good day Tue 22/11
Good day, I am Mr. Rifaat Aboud fro...

C2 Chemistry 2022
FOLLOW UP Tue 22/11
Dear Dr. Lazarov A, Hope you are do...

J Joe and Jess Thwaite
*****SPAM***** re: Mon 21/11
Spam detection software, running o...

E E-Energy
Най-лесният начин за ... Mon 21/11

RE: DHL Notification / DHL_AWB_00511703/ ETDZ

DE DHL Express <support@dhl.
Tue 22/11/2022 12:36

Dear Customer,

We attempted to deliver your item at 8:16AM on Nov. 20, 2022. (Read enclosed file for details)

The delivery attempt failed because nobody was present at the shipping address, so this notify has been automatically sent.
If the parcel is not scheduled for re-delivery or picked up within 72 hours, it will be returned to the sender.

Label Number: DHL733918737AA
Expected Delivery Date Nov. 23, 2022.
Class: Package Services
Service (s): Delivery Confirmation
Status: e-Notification sent

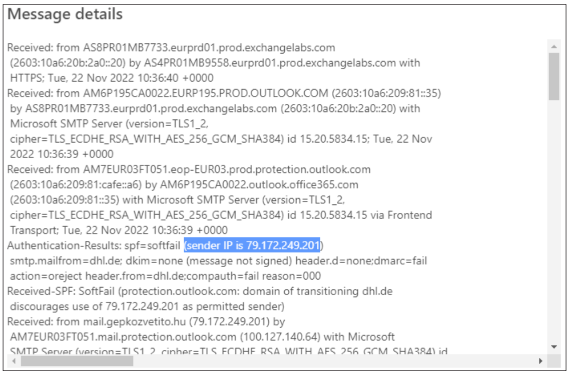
Read the enclosed file for details.
DHL Customer Service.

2022 © DHL International GmbH. All rights reserved.

**Figure 4.** Malware (worm) is inside the attached file.
The computer will be infected while opening the attached file

The sender as a rule is under fake e-mail address. To disclose the real e-mail address of the sender and the server location of this e-letter, it is recommended to open the e-letter.

Go to three dots on upper right corner. Click on three dots. Scroll down and follow More option > View > View message details > Message details are presented in Fig. 5.



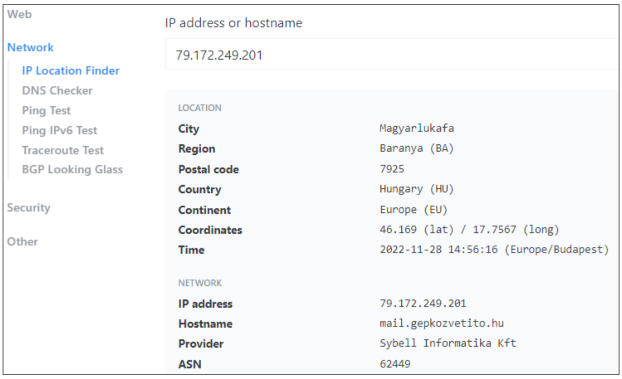
Message details

```
Received: from AS8PR01MB7733.eurprd01.prod.exchangelabs.com
 (2603:10a6:20b:2a0::20) by AS4PR01MB9558.eurprd01.prod.exchangelabs.com with
 HTTPS; Tue, 22 Nov 2022 10:36:40 +0000
Received: from AM6P195CA0022.EURP195.PROD.OUTLOOK.COM (2603:10a6:209:81::35)
 by AS8PR01MB7733.eurprd01.prod.exchangelabs.com (2603:10a6:20b:2a0::20) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5834.15; Tue, 22 Nov
 2022 10:36:39 +0000
Received: from AM7EUR03FT051.eop-EUR03.prod.protection.outlook.com
 (2603:10a6:209:81:cafe::a6) by AM6P195CA0022.outlook.office365.com
 (2603:10a6:209:81::35) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5834.15 via Frontend
 Transport; Tue, 22 Nov 2022 10:36:39 +0000
Authentication-Results: spf=softfail (sender IP is 79.172.249.201)
 smtp.mailfrom=dhl.de; dkim=none (message not signed) header.d=none;dmarc=fail
 action=oreject header.from=dhl.de;compauth=fail reason=000
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning dhl.de
 discourages use of 79.172.249.201 as permitted sender)
Received: from mail.gepkozvetito.hu (79.172.249.201) by
 AM7EUR03FT051.mail.protection.outlook.com (100.127.140.64) with Microsoft
 SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
```

**Figure 5.** Message details including a real IP address of the sender 79.172.249.201

Read the message on the row Authentication-Results: spf=softfail (sender IP is 79.172.249.201) > Go to Google Search > Write IP location > Paste 79.172.249.201

The real location of this letter is in city of Magyarlukafa, Hungary as can be seen in Fig. 6.



IP address or hostname

79.172.249.201

LOCATION

| | |
|---|---|
| City | Magyarlukafa |
| Region | Baranya (BA) |
| Postal code | 7925 |
| Country | Hungary (HU) |
| Continent | Europe (EU) |
| Coordinates | 46.169 (lat) / 17.7567 (long) |
| Time | 2022-11-28 14:56:16 (Europe/Budapest) |

NETWORK

| | |
|---|---|
| IP address | 79.172.249.201 |
| Hostname | mail.gepkozvetito.hu |
| Provider | Sybell Informatika Kft |
| ASN | 62449 |

**Figure 6.** Real location parameters of the fake sender

*3.2. Cyber hygiene instructions to ensure Internet users stay protected*

The following cyber hygiene instructions have to be included in the curriculum of military Internet users in order to ensure they stay protected from cyberattacks.

Create safe and secure passwords that are resistant to cracking

– For different accounts and registrations avoid using the same password.

– The passwords need to change on a regular basis.

– The passwords' length has to be at least 12 characters and longer.

– The passwords have to include a mix of capital and small letters, symbols and numbers.

– The passwords must avoid sequential numbers or personal information, such as date of birth or a pet's name.

– The default passwords on IoT (Internet of Things) devices need to be changed.

– The passwords is not written down and shared them with other internet users.

– It is recommended to use a password manager to generate, store, and manage all passwords in one secure online account

– Usage of multi-factor authentication access

– The essential accounts – such as email, social media, or banking apps – are protected with MFA (Multi-Factor Authentication) using an app like Google Authenticator or Authy.

– MFA backup codes is saved in a password manager.

Backing up data regularly on external discs and storages

– It is recommended to keep files secure and protected against data loss by backing up essential files offline, either on an external hard drive or in a cloud.

While communicating ensure privacy of information

– It is recommended not to post private information such as a home address, private pictures, phone number, or credit card numbers publicly on social media.

– Privacy settings in usage of social media are to be set to a high level.

– It is recommended to avoid quizzes, games, or surveys on social media that ask for sensitive personal information.

– It is recommended the user to keep a computer and phone locked with a password or PIN

– It is recommended not to disclose private information when using public Wi-Fi

– In case public Wi-Fi, it is recommended to maximize privacy by using a VPN (Virtual Private Network).

– Online transactions are to make via a secure website (URL starts with https://) with a padlock icon on the left of the address.

– Information about online privacy is exchanged with colleagues, friends and family members to help keep them safe as well.

Keep applications, system software, and firmware up to date

– It is recommended to update applications, web browsers, operating systems, and firmware regularly to ensure using the latest versions with possible security issues eliminated or patched.

– It to be set up a system features to ensure automatic software updates.

– It is recommended to delete applications no longer in use, but open security vulnerabilities only download apps from reputable or official sources.

Ensure security of routers

– Default name of home Wi-Fi routers, router's username and password need to be changed.

– It is recommended to keep router's firmware up to date.

– It is recommended to disable remote access, Universal Plug and Play, and Wi-Fi Protected Set-up.

– It is recommended to set up a separate network for guests to use.

– It is recommended to ensure that a router offers WPA2 or WPA3 encryption to protect the privacy of information sent via the network.

Protect against social engineering attacks

– It is recommended to avoid clicking on suspicious links or links, opening emails that look suspicious, downloading suspicious attachments from emails or not expected text messages, clicking on ads that promise free money, prizes, or discounts.

Using network protected software – firewalls

– It is recommended to use a correctly configured firewall to prevent malicious software from accessing a computer or network via the internet.

Encrypting devices

– It is recommended to encrypt devices and media as laptops, tablets, smartphones, removable drives, backup tapes, and cloud storage which contain sensitive data.

Remove all information from hard drives

– Before disposal of or sell a computer, tablet, or smartphone, make sure the hard drive is clean up to prevent any personal information from being accessed by others.

Ensuring high-quality antivirus protection

– It is recommended to use high quality antivirus software that scans for and removes computer viruses and other malicious software.

– It is recommended to keep the antivirus software up to date

In conclusion, cyber hygiene means developing and following a protective routine to keep personal and financial information secure when using computers, laptops or other mobile devices. Using strong passwords and changing them regularly, keeping software and operating systems up to date, cleaning hard drives, and using a comprehensive antivirus software like Kaspersky Total Security will help users stay ahead of the latest cyber threats.

## 4. Subject of the curriculum in cyber hygiene

In conclusion, human errors is among the leading causes of security breaches and data loss in a corporate military computer network. It has to be emphasized that cyber hygiene as a subclass of the cybersecurity is not only a task and obligation of each personnel from military staff but the institution command, and IT administrators, and the organization as a whole. One of the methods to upgrade protection is to educate users and increase their knowledge and skills in working with computer information and communication devices. Each curriculum in the scope of Cyber hygiene has to meet the following educational objectives.

*4.1. Objectives*

Each educational program aims, through the training provided in it, for the military employees to acquire knowledge, skills and practical experience that will allow them to ensuring the safety in military environment, the life and health of people in the troops, the protection of the military devices and equipment from cyberattacks by mastering theoretical knowledge and practical skills in:

– Recognizing vulnerabilities, threats and attacks in cyberspace;
– Types of cybercrimes and their participants;
– Peculiarities of cyber security in the military area;
– Relationships and information exchange between the military systems;
– Configuration and working with antivirus programs;
– Configuration and working with firewalls;
– Updating user operating systems;
– Backup and recovery of critical data;
– Safe use of internet browsers;
– Safe work on social sites;
– Security when working with e-mail;
– Safe operation when using wireless networks;
– Smart device security

*4.2. Exemplary curriculum of cyber hygiene, main topics and tasks*

1. Cyber threats and vulnerabilities in the army and military area
   1.1. Cybersecurity in the army and military area.
   1.2. Basic definitions related to cybersecurity. Vulnerabilities and threats in cyberspace.
   1.3. Cybercrimes, cybercriminals and their motives.
   1.4. Military institutions, units, equipment and weapons and their vulnerability to cyber attacks
2. Software instruments for protection of personal devices
   2.1. Types of computer malware and means of protection against them. Basic rules for working with antivirus programs.
   2.2. Firewalls for personal computers – purpose and use.
3. Protection of critical data
   3.1. Types of Updates for User Operating Systems. Ways to install and manage them.
   3.2. Backing up critical user data - means and methods. Create local and remote archives. Restore data from an archive.

4. Safe operation in a computer network
   4.1. Internet browsers - purpose and functionalities. Increasing security when working with internet browsers. Working safely in the Internet environment. Rules for using online payment platforms.
   4.2. Protection of users' personal data when using social networks. Confidentiality of shared data.
   4.3 Use of e-mail for business and personal correspondence. Protection against cyber-attacks distributed via e-mail.
5. Cybersecurity of mobile devices
   5.1. Use of wireless (mobile) devices for daily activities. Connecting to wireless networks. Basic security rules when using open access networks.
   5.2. Smart devices for personal use and as part of the ship's systems. Installing and updating applications. Communication protection when using smart devices.

## 5. Conclusions

Based on the analysis of main characteristics and components of the cyber hygiene as a subject of the educational plan in the cyber security for military staff, teaching questions and their instruments used to be solved are discussed. Based on institutional experience on education in cyber security, a sequence of activities to keep resilient and reliable cyber hygiene in army organizations is defined. Cyber hygiene software issues and institutional information security control functions are disclosed. Malware infection as a main cyber hygiene concern is analyzed. Fundamental cyber hygiene instructions to ensure military Internet users and institutions stay protected are defined. Exemplary curriculum with basic themes for education of military staff is presented.

## REFERENCES

BEDRICH, F., A cyber hygiene checklist can help prevent attacks on your business, Article and tools, BDC blog. Available at: https://www.bdc.ca/en/articles-tools/blog/cyber-hygiene-checklist-can-help-prevent-attacks-on-your-business.

EAD, W.M., ABBASSY, M.M., 2022. A General Cyber Hygiene Approach for Financial Analytical Environment. In: Derindere Köseoğlu, S. (eds) Financial Data Analytics, Contributions to Finance and Accounting. Springer, pp.369-384. DOI: 10.1007/978-3-030-83799-0_13.

FS-ISAC, 2021. An Attractive target: why cyber hygiene matters, TLP WHITE, Available at: https://www.fsisac.com/hubfs/Resources/WhyCyberHygieneMatters.pdf.

KASPERSKY LAB GLOBAL RESEARCH AND ANALYSIS TEAM, 2014. “Syrian Malware, the ever-evolving threat, Version 1.0. Available at: https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits.

KASPERSKY LAB, 2023. Top tips for cyber hygiene to keep yourself safe online. Available at: https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits.

OLIVARES-ROJAS, J. C., REYES-ARCHUNDIA, E., GUTIERREZ-GNECCHI, PATIÑO, A. N., JACOBO, J. C., MORENO, I. M., 2022. A methodology for cyber hygiene in smart grids. DYNA. January – February 2022, vol. 97, no. 1, pp. 92.97. DOI: 10.6036/10085. Available at: https://www.revistadyna.com/search/a-methodology-for-cyber-hygiene-in-smart-grids.

RSI SECURITY, 2021. The top 11 rules of cyber hygiene for government agencies, available on https://blog.rsisecurity.com/the-top-11-rules-of-cyber-hygiene-for-government-agencies/.

SINGH, D., MOHANTY, N., P, SWAGATIKA, S., KUMAR, S., 2020. Cyber-hygiene: The key concept for cyber security in cyberspace, *Test Engineering and Management* vol. 83, pp. 8145 – 8152.

SUCH, J., M., CIHOLAS, P., RASHID, A., VIDLER, J., SEABROOK, T., 2022. Basic cyber hygiene: Does it work? Lancaster E-Prints, *Feature article*, Available at: https://core.ac.uk/reader/224767750.

THE INTERNET ORGANIZED CRIME THREAT ASSESSMENT (IOSTA), 2015, ISBN 978-92-95200-65-4. ISSN 2363-1627. DOI 10.2813/03524.

TREVORS, M.; WALLEN, C. M., 2017. *Cyber hygiene: A baseline set of practices*. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213, Available at: https://resources.sei.cmu.edu/asset_files/presentation/2017_017_001_508771.pdf.

TYAS, A. T., 2022. *What is cyber hygiene and why is it.* Available on https://www.upguard.com/blog/cyber-hygiene.

✉ **Prof. Boyan Mednikarov, DSc.**
ORCID iD: 0000-0003-4247-897X
**Prof. Yuliyan Tsonev**
ORCID iD: 0000-0001-5602-4747
**Dr. Borislav Nikolov, Assist. Prof.**
RID: AAZ-6105-2021
**Prof. Andon Lazarov[1], DSc.**
ORCID iD: 0000-0003-2115-4415]
Nikola Vaptsarov Naval Academy
Varna, Bulgaria
E-mail: [1]a.lazarov@naval-acad.bg