Co-funded by the Erasmus+ Programme of the European Union

InCyT Training Modules

Information Security for Managers Unit 3 – Weeks 5 Unit (Module) name: Information Security Management 3	
Learning Activities	❑ **Webinar** ❑ **Exercises** ❑ **Workshop** ❑ **Presentation** ❑ **Other**
Learning Responsible	• George Matache et al.
Learning Activity Goals	1 General terminology 2. Confidentiality, Integrity and Availability (CIA) 3. Rules and standards 4. Information security management 5. How does malware work? 6. Top cyber threats 7. Types of attacks 8. Secure Web Server – SSL 9. Sending and received e-mails 10. Asset management
Skills to be Gained	• TS3 Network Security • TS4 Penetration (exploitable vulnerabilities) testing • SS3 Cognitive and behavior analysis
Duration of Learning activity	2 weeks
Learning requirements	***What is needed?*** • Internet access • Internet Browser • MS Office365

Brief information about the module

Description

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

Businesses are often so concerned with their day-to-day operations that they forget to invest heavily in network security. Others understand the need for comprehensive network security but have a lenient strategy in regard to their IT, which can be just as detrimental in the event of a data leak. Understanding what network security entails, as well as the best practices that you can adhere to that will ensure your company's network is secure from the numerous outside threats looking to infiltrate your network, is essential to keeping your data, and ultimately your business, safe.

It is utmost important that the training on cyber security for SMEs – managers and employees – is concrete and interactive – as well has hands-on because the small SMEs do not have time, motivation nor resources to spent on this issue why it is very important that the training is relevant and manageable for the managers who participate. Hence, this module is plan on basis of this.

Information security management (ISM) defines and manages controls that an organization needs to implement to ensure that it is sensibly protecting the confidentiality, availability, and integrity of assets from threats and vulnerabilities. Malware, or "malicious software," is an umbrella term that describes any malicious program or code that is harmful to systems.

Hostile, intrusive, and intentionally nasty, malware seeks to invade, damage, or disable computers, computer systems, networks, tablets, and mobile devices, often by taking partial control over a device's operations. Like the human flu, it interferes with normal functioning. The motives behind malware vary. Malware can be about making money off you, sabotaging your ability to get work done, making a political statement, or just bragging rights. Although malware cannot damage the physical hardware of systems or network equipment, it can steal, encrypt, or delete your data, alter or hijack core computer functions, and spy on your computer activity without your knowledge or permission.

Malware is described and defined, introducing its many different types, and explain how it works. We also describe the warning signs of an infected device and explain how to prevent it. The learners could be informed about such aspects by reading the corresponding text, watching streaming webinars and solving exercises at own pace and through live audience interaction with continuous feedback and gamification knowledge check.

Content of the Learning Material

Especially if you have a company that is very dependent on your IT systems working and being secure. Cyber security threats are on the rise.

Cyber-attacks continued to increase in the EU in 2020 and 2021 and especially 2022, both in terms of their sophistication and number, and in terms of their impact. The EU is working on several fronts to protect citizens and businesses from cybercrime and to ensure a safe, open and secure cyberspace.

In 2022, we will see state-sponsored groups targeting the cryptocurrency industry, while cybercriminals will take advantage of investors by crafting digital wallets with built-in backdoors. We are likely to see an increase in attacks against payment systems and more advanced mobile threats.

Approximately half (47 per cent) of the population (in Denmark) between the ages of 16 and 89 have had cybercrime close to their lives in the form of fake e-mails, fraud, hacking or identity theft. The same applies to 11 per cent. of Danish private companies. 8 per cent of the companies have experienced that access to digital services has been blocked and 3 per cent. have had data deleted or destroyed. Phishing is the most pervasive problem, but unfortunately we also see a radical increase in the number of fake websites as more and more people shop and work from home.

The core of ISM includes information risk management, a process that involves the assessment of the risks an organization must deal with in the management and protection of assets, as well as the dissemination of the risks to all appropriate stakeholders. This requires proper asset identification and valuation steps, including evaluating the value of confidentiality, integrity, availability, and replacement of assets. As part of information security management, an organization may implement an information security management system and other best practices found in the ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27035 standards on information security. However, this kind of certification is often too resource demanding for SMEs why we prepare for an agile cyber security practice:

Information Security & Internal Control Systems

- General terminology
- CIA triad
- Anatomy of an Attack (Attack Surface Reduction)
- Cyber Security Frameworks

Information Security Management
Email & Office
Devices

A key challenge for the SMEs is malware, which is an umbrella term for any type of "malicious software" that's designed to infiltrate your device without your knowledge. There are many types of malware, and each works differently in pursuit of its goals. However, all malware variants share two defining traits: they're sneaky, and they're actively working against your best interests.

Is malware a virus? Yes and no. While all computer viruses are malware, not all malwares are viruses. Viruses are just one type of malware. You'll hear a lot of people using the two terms interchangeably, but from a technical point of view, viruses and malware are not the same thing. Think about it this way: Malware is malicious code. Computer viruses are malicious code that spreads across computers and networks.

How does malware work?

All malware follows the same basic pattern: The user unwittingly downloads or installs the malware, which infects the device.

Most malware infections occur when you inadvertently perform an action that causes the malware to be downloaded. This action might be clicking a link in an email or visiting a malicious website. In other cases, hackers spread malware through peer-to-peer file sharing services and free software download bundles. Embedding a bit of malware in a popular torrent or download is an effective way to spread it across a wide user base. Mobile devices can also be infected via text messages.

Another technique is to load malware into the firmware of a USB stick or flash drive. Because the malware is loaded onto the device's internal hardware (rather than its file storage), your device is unlikely to detect the malware. This is why you should never insert an unfamiliar USB drive into your computer.

Once the malware has been installed, it infects your device and begins working towards the hackers' goals. What separates the various types of malware from each other is how they go about doing this. So how does malware work? What is a malware attack?

Top cyber threats

Drive-by exploits can automatically exploit existing vulnerabilities in software installed on a PC without interacting with the legitimate user; they expanded their scope in 2012 to mobile terminals as well. it focuses almost entirely on compromising legitimate websites. vulnerabilities in the browser, its plugins, or the operating system can be exploited to install malware on the PC without the user's knowledge the infection can be initiated by simple internet browsing.

Worms are self-replicating programs; use the network of computers to send their own copies to other nodes (computers in the network), managing to do this without the intervention of any user, unlike a computer virus, a computer worm does not need to be attached to an existing program, it causes damage to the network, even just by taking up bandwidth.

Trojan presents itself in the form of legitimate programs, which, in reality, are created with the aim of stealing confidential data, or to allow unauthorized users or programs access to the infected system; constitute the vast majority of infections (80%).

Malware represents any program whose function is to cause software or hardware damage to a computer (e.g., viruses) – as described above.

Track ware are the programs that use some web browser vulnerabilities to send a server or people information about the sites accessed, the information searched and the browsing habits of the user; Viruses aim to infect as many personal computers as possible, while spyware aims to spread across the Internet, Viruses usually have a dangerous payload, they want to cause damage to the infected computer, while spyware only slows down computer processes, adds popups and destabilizes the browser and has other "annoying" effects.

SQL Injection (Code Injection) occurs when an attacker can insert any data into an SQL query sent to a database; by injecting the syntax, the logic of the statement is modified so that it performs a different action, is the most common vulnerability. The best SQL injection defence strategy is based on implementing strong input validation routines so that the attacker cannot enter data other than what the application needs.

Spyware it is generally defined as a program that takes advantage of the vulnerabilities of a system for the benefit of a third party, it can slow down your computer, make it vulnerable to virus infection, and collect confidential information such as usernames for various applications, passwords, and credit card/bank account information.

A keylogger is a small "smart" program that hackers place on your computer without you noticing. Here it can lie for several months or years and keep an eye on every single keystroke you make on the keyboard. All data is sent to the hackers, who can then use different algorithms and tools to get the best out of your data. Over time, they find out different things about your behaviour and, not least, where you use different passwords, you have entered on the keyboard. It can then be used to take over your entire digital identity in a matter of minutes.

Adware is a sub-category of spyware and is a program that advertises products or services. Often these ads appear even after the program has been uninstalled.

Exploitation kits are automated software that assists less experienced attackers in compromising systems by exploiting client-side vulnerabilities, particularly those in web browsers or applications that can be accessed by websites; relies on drive-by download attacks, where malicious code is injected into compromised websites; can exploit vulnerabilities in the browser or its plugins.

Botnet represents a set of computers that are under the control of an attacker; A botnet can be used for multiple purposes: Distributed Denial of Service - DDoS attacks, spamming, identity theft, malware distribution, infecting computer systems; they can run on multiple operating systems; in 2012 the "Flashback" botnet managed to infect approximately 600,000 Apple computers.

Denial of Service is an attempt to affect the availability of computer systems/services or electronic communications. The target system is attacked by sending a very large number of illegitimate requests, which consume its hardware or software resources, making it unavailable to legitimate users. The main motivations for DDoS attacks are hacktivism, vandalism and fraud. Compromise of confidential information; refers to data security breaches that have occurred through the disclosure (whether intentional or unintentional) of confidential information by internal or external agents; Information leakage is usually achieved through hacking, malware distribution, social engineering attacks, physical attacks, or abuse of privileges

Rogue ware/scareware is type of threat that takes the form of fake software; A particular case of rogue ware/scareware is fake security software that once installed in the system provides false security alerts and invites the user to purchase a special disinfection tool. This type of threat propagates through various methods such as social engineering techniques, trojans, exploitation of vulnerabilities (especially java).

Ransomware is one of the most dangerous and aggressive forms of cybercrime. The hackers use a piece of extremely complex code to lock down the functionality of a computer or computer-controlled system. The owner of the system is then contacted by the hacker with a demand for a ransom to reactivate the system or "unlock" information in the system. In the mild cases, it is about family photos or the company's accounts, in the serious cases, it can be about vital systems, such as; control systems in factories, or an internet-connected pacemaker.

Types of attacks

Targeted attacks

- target a specific person or organization
- aims to either collect personal/confidential data or compromise target computer systems
- generally, has a phase in which the attacker informs himself through various techniques (e.g. social engineering) about the targeted IT system and then triggers the attack

- often his actions appear legitimate because they appear to be coming from a trustworthy person

Theft/Losses/Physical Destruction

- due to the increased mobility offered by laptops, smart phones or tablets, this type of threat is about to become a major one
- consistent data backup and content encryption can be a solution to limit actual data loss or disclosure of confidential data to outsiders

Identity theft

- is a real threat in an increasingly online environment
- access credentials or personal data are the target of attackers today
- once in their possession, the attacker can carry out fraudulent transactions (especially financial) or obtain confidential data

Information leak

- intentional or unintentional disclosure of information to an unauthorized person
- information such as geolocation and phonebook contacts can easily fall into the hands of attackers and be used for fraudulent purposes

Search Engine Manipulation (SEP)

- manipulates search engines to display search results that contain references to malicious websites. Thus, an infected web page redirects the users to malicious sites and if the victims access the respective sites, they infest their computers with malware
- Fake digital certificates
- are used by attackers to digitally sign resources (websites, applications, source codes, etc.) used in various cyber-attacks in order to pass undetectable to the end user
- are often used to sign malicious web applications such as e-banking or e-commerce, which use the HTTPS protocol
- can be created or stolen by exploiting vulnerabilities in the PKI (Public Key Infrastructure) systems of certification authorities that issue digital certificates for secure websites.

Secure Web Server – SSL

The protocol that implements public key encryption is called SSL (Secure Socket Layer), developed by Netscape. This protocol is used by browsers and web servers to transmit data securely, so it was created to be used by the HTTP protocol.

Connecting to a secure web server is done by mentioning the https protocol instead of http in the URL - that is, access to the secure web page is indicated by the protocol, and not the name of the server.

A secure web server offers: Secure transfer of information: the data transmitted between the server and the navigator cannot be decrypted in case of their interception.
Server authentication: If the web server has received a certificate from a certification authority (CA).

Security check list

Desktop and Mobile Firewall
Start by securing your outer perimeters by making sure your than
point's (digital devices') firewalls work. It sounds basic, but it is also in the very basics that you have to start. There are typically three to four different types of firewalls on your network:
• Firewall on your operating system (Android, iOS, Windows, etc.).
• Firewall on your antivirus/security program.
• Firewall on your internet router.
• Firewall on your ASA box or intelligent switch (Typically only larger companies).

Backup
Backup should really be at the top of the list, like it shouldn't be news. Backup can save you from having to pay a ransom to have your data unlocked. However, make no mistake about the size of the company, most of the attacks with this type of malware are aimed at small businesses and individuals.

Rules for safer browsing
- use the latest browser version
- orient yourself towards other types of browser (eg Google Chrome, Opera, Firefox, Safari, etc.), especially when accessing potentially unsafe web pages;
- most malware affects Microsoft Internet Explorer (used by over 50% of users)
- check the real destination of the links by passing the mouse cursor over it and viewing the real address in the lower left part of the browser
- be careful what plugins you install, often they come with malicious software
- do not click on links in pop-up windows
- check for "https://" at the beginning of the web address before entering personal information
- regarding making an online purchase, greater attention must be paid to the security level of the page, if one opts for online payment with a bank card

Sending and receiving e-mail

- avoid sending or receiving sensitive information by e-mail;
- avoid social engineering or phishing attempts
- look for an email provider that offers strong anti-spam filtering
- do not respond to spam and avoid cascade or pyramid emails
- do not respond to spam and avoid cascade or pyramid emails
- do not use the same name for your personal and work e-mail account; the use of distinct names for these accounts reduces the risk of them being the target of a computer attack
- avoid storing critical information in personal e-mail accounts or in other networks outside the institution/company where you work

The truth is that email has never traditionally been a secure medium for communication. After all, only criminals really need to concern themselves with securing their communications. This is an extremely common, yet entirely flawed, way of thinking, and Snowden himself has famously discredited this type of mentality.

Arguing that you don't care about privacy because you have nothing to hide is like arguing that you don't care about free speech because you have nothing to say.

While many people may still subscribe to the mindset that they have nothing to be concerned about if they have nothing to hide, the reality is that there is plenty to be concerned about, and there are plenty of concrete reasons for people to encrypt their email communications and protect their privacy. This is true whether you're an investigative journalist, dissident, whistle-blower, or just an ordinary average citizen.

Why anyone would need to send a secure email?

To protect against threats posed by cybercriminals

Have you ever sent sensitive personal information in an email and thought, 'welp, I sure hope that email doesn't somehow end up in the wrong hands? This is a truly disconcerting thought, because if someone other than the intended recipient(s) gets their hands on the email – especially if that someone happens to be a cybercriminal – the results could potentially be catastrophic.

Sending an email containing sensitive personal data like your medical information, financial account information, social security number, address, or phone number, can be extremely risky because cybercriminals need only a minimal amount of personal data to exact maximum harm. With access to sensitive personal data like this, cybercriminals can compromise your online profiles, drain your bank accounts, and even steal your identity.

To prevent email providers from monitoring emails and sharing data with advertisers
Email providers have been known to monitor and scan users' email messages to facilitate targeted advertising efforts. Though in 2017 Gmail apparently discontinued the practice of scanning emails for advertising purposes, that doesn't necessarily mean that Google has ceased scanning emails for other purposes. For example, Gmail's "Smart Reply" feature offers relevant suggestions for quick, canned replies to an email you've received based on the contents of its message. So, if you don't want your email provider to scan or monitor your email messages for advertising or any other purposes, then you'll want to send secure emails that effectively keep the contents of those messages private and inaccessible to anyone other than you and the party you are communicating with via email.

Mass surveillance encroaches on our civil liberties and fundamental rights to privacy.
Such unwarranted surveillance is unduly invasive and a direct affront to our civil liberties and our fundamental rights to privacy. When you send a secure email, you can encrypt your communication so that only you and the other party you're securely communicating with can access the content of the message.

Sending an encrypted email preserves your privacy and effectively makes it impossible for government entities to snoop on your secure email communications. This is especially important for those whose job responsibilities require complete confidentiality in their communications, but it's also vital for anyone who generally doesn't want the government trampling on their privacy rights.

To protect against government surveillance efforts
As we mentioned earlier, mass government surveillance practices are extensive. And this is true not just under authoritarian regimes like in China or Iran, but also in the United States, the UK, Australia, Canada, Germany, and other Western countries as well.
Mass surveillance is not an aberration, it's the norm and it can be pernicious to the point of being illegal.

This is why sending secure emails is critical, particularly if the email you're sending contains sensitive personal information.

How to send a secure email
Now that you know the reasons why you'd want to send a secure email, we're guessing you'll probably want to know how to actually do it. There are a couple of ways to go about doing so, each with certain inherent advantages and disadvantages, but the bottom line is that if you're going to send a secure email, then your email message will need to be encrypted. When you encrypt an

email message, you're essentially scrambling the contents of that message and making it impossible for anyone without the encryption key to unscramble the message.

What options that are available to you if you want to send a secure email?

Encrypt emails in popular email clients
Many of the big-name web-based email providers will allow users to encrypt their emails using either one of the two main email encryption protocols, S/MIME or OpenPGP. The downside is that it may not always be a simple or straightforward process to do so directly from within your web-based email provider's interface, and you may have to pay for it.

For example, if you want to send a secure email on Gmail, you will first need to enable S/MIME encryption by signing into Gmail using a GSuite administrator account. GSuite accounts are primarily for business purposes, but you could theoretically set up an account for your personal use. The other issue with this is that the recipient(s) you are emailing will also need to have S/MIME encryption activated in order for this to work.

Similarly, Outlook also supports S/MIME encryption, and you'll need to enable it manually, but before you do so, you'll need to obtain a certificate (or digital ID) from your organization's administrator. This, admittedly, isn't the most streamlined process, nor is it likely to be a very practical solution for most personal email users. Check out our how to encrypt outlook emails for more information about this.

You can, however, bypass these issues by installing a free third-party tool like Mailvelope to encrypt your emails with ease. Mailvelope works with many of the most popular email services like Gmail, Yahoo!, Outlook, Hotmail, and GMX. But again, the recipient(s) of your encrypted email message will also need to be using similar PGP/OpenPGP software to decrypt the email and read the contents.

Use a dedicated secure email provider
If you don't want to go through the trouble of manually enabling S/MIME or OpenPGP encryption on your traditional web-based email account, a much easier way to send a secure email is to create an account with a secure email provider.

With a secure email provider like ProtonMail, you'll be able to send secure, encrypted emails to others regardless of whether they use the same secure email provider that you use, and your recipient(s) will also be able to respond securely. Many secure email providers implement OpenPGP encryption to secure users' emails and will allow users to easily send and receive secure, encrypted emails with others who have OpenPGP encryption enabled with their email clients. If your recipient

does not have PGP enabled, then you'll still be able to send an email securely to that recipient that can only be opened using a shared secret.

Basically, when you use a secure email provider you'll be able to easily protect sensitive messages by encrypting them, all on a platform that is typically as simple to use as the big-name email providers like Gmail, Yahoo!, or Outlook. But unlike those big-name providers, a secure email provider won't annoy you with advertisements or monitor your emails (since it can't even access them thanks to end-to-end encryption).

The downside is that, in order to access a secure email provider's full slate of features, expanded storage, and unrestricted messaging, you'll need to pay. Many of the best secure email providers do, however, offer a free tier (with certain limitations) that will allow you to send and receive secure emails for free. If you're only going to be sending a limited number of secure emails, then a free option could certainly be a viable solution, but if you're planning on conducting the majority of your email correspondence in a secure manner, then purchasing a premium subscription will be necessary.

When you receive an email, pay attention to

- the identity of the sender is not guaranteed: it checks the relationship between the sender and the content of the message;
- do not open attachments coming from unknown persons or associated with legitimate accounts, but with messages with suspicious subject and content. They may contain malicious software (malicious software or malware, such as worms, trojans, spyware, forms of adware, etc.);
- if it is absolutely necessary to open an attachment, even from legitimate e-mails, it must first be downloaded and scanned with the installed antivirus solution and then opened with the associated application;
- in the case of e-mails containing links, do not directly access that link in the body of the message; possibly, that link can be copied and opened from another browser tab;
- do not respond to e-mails containing requests for personal or confidential data (eg PIN code and bank card number).

How do you know that your e-mail was "accessed" by unknown persons?

- your contacts say they received spam emails from you;
- you receive many emails with errors;

- messages appear in the "sent" folder without you sending them;
- the account location history in the login operation does not correspond to your current activity.

Password security. The attacks aim to identify the password and access the information restricted by that password. The most used attack methods of this type are "dictionary attacks" and "brute force".

"Dictionary attack" aims at the unauthorized access of some resources or computer systems, by successively trying the passwords / decryption keys found in a predefined list of words or phrases.

A "brute force" attack is a method of unauthorized access to a computer system or of decoding encrypted content (such as passwords) using "brute force" calculation - through programs that apply the trial-error method. The method consists in successively trying all possible combinations of characters, without an elaborate algorithm.

Measures: captcha system, access timing after a number of failed accesses.

- use unique IDs and passwords and do not communicate them to other users;
- the length of the password and its complexity must be chosen so that it is difficult to guess but easy to remember;
- periodic change of passwords (at an interval of 1-3 months);
- using different passwords for different applications;
- the use of multiple authentication methods (PIN, fingerprint, alert messages, etc.);
- avoiding using similar passwords at home and at work.

Do not use:

- the name of you, someone else in the family or your favorite animal,
- elements of your address: building name, street, country,
- the name of the institution, the project, etc.,
- phone number, registration number
- the name of the favorite star or character (or of the film, book, etc.),

- dictionary words;
- the name of the account for which you set the password;

Methods that give a false feeling of strong passwords

- phonetic method: "I know for sure I have a Blu-Ray DVD!": St1u100%km1DVDBLr!
- first letter method: "I know for sure I have a Blu-Ray DVD!": "sSka1DVDBr!"
- substitution method (usually vowels): Replace certain letters with numbers symbols within a word. For example, change apple to @ppl3.
- reverse and substitution method: "I love vacations": "r0d@3l11d3cn0c"
- upper/lower case, number/symbol and substitution method: "I love holidays": "@D0rC)nC3d11L3"
- customization of methods according to websites in order to create a personal password generation system: Gmail - "G@D0rC)nC3d!1L3MAIL", Yahoo - "YA@D0rC)nC3d!1L3HOO", Wizzair - "WIZZ@D0rC)nC3d!1L3AIR".

Do not use these methods! While they represented once the norm, CPU power made them mostly irrelevant. Today's password cracking tools capabilities reduce the effectiveness of the methods mentioned earlier.

A better way to create passwords is to use whole phrases, while including upper-case, lower-case, numbers, and preferably special characters. In that way automated scripts that easily use archaic methods, like the ones discussed, need a huge amount of effort to brute force or guess your password. The new method is called "passphrases" and it can reach up to 100 characters or more.

The passphrase is considered to be superior to the password because it is easier to remember and harder to hack. It is easier to remember a random phrase with 4 to 8 words instead of a complex string of letters, numbers and special characters 30 characters long. Even the most advanced password cracking tools are not able to brute force a passphrase that uses random words and is of significant length.

How to create a passphrase

- Combine a group of words into a sentence that makes sense to you, but not to others
- Do not use common phrases or famous quotes
- Add spaces within and between the words
- Use capital letters and capitalize some of the words
- Add punctuation and special characters that make sense to you

- Use unusual spellings of words

Another way to develop a passphrase is to link to a personal story or private memory. Keywords can be used to tell the story.

Overall, in this unit module

How To Effectively Use The Cyber Kill Chain in Your Cybersecurity Strategy

Detect – Analyze and find the intrusion attempts.

Deny – Stop the attacks as they happen.

Disrupt – Stop the data communication

Degrade – Reduce and limit the efficacy of the attack.

Deceive – Lead the attackers in the wrong direction.

Contain – Conceal and restrict the attack's reach so that it only affects a portion of the organization.

Questions:

Questions Discussion Forum to be answered with a short explanation. Answers will be discussed with the mentor during the mentoring sessions

- What is Malware
- Which are the main cyber threats
- Which is the role of Secure Web Server - SSL
- Explain some rules for safer browsing
- Present some measures to secure sending and receiving of e-mail

Self-assessment questions. After answering the learner can see the results and compare them with these saved on the platform

- Malware
- The main cyber threats
- Rules for safer browsing
- Measures to secure sending and receiving of e-mail

Attachments (PowerPoint presentation, handouts, prints, links, video…):

See Powerpoint and Video files

References:

- What is Cyber Security?

URL: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

- Malware, or malicious software

URL: https://www.malwarebytes.com/malware

- Cybersecurity for everyone.

https://www.avast.com/c-malware

- Malware Removal Software 2022; Secure your personal data

URL: Malware

- What are Cyber Security Threats?

URL: https://www.imperva.com/learn/application-security/cyber-security-threats/

- 21 Top Cybersecurity Threats and How Threat Intelligence Can Help

URL: https://www.exabeam.com/information-security/cyber-security-threat/

- Sending and receiving e-mail

URL: https://www.ibm.com/docs/en/i/7.1?topic=mail-sending-receiving-e

- Create and send email

URL: https://support.google.com/a/users/answer/9259846?hl=en

The Cyber Kill Chain: The Seven Steps of a Cyberattack

URL: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/