

5. SECURITY AND SAFETY ON THE INTERNET (9 hours approx)

1. Introduction

2. Learning objectives

3. Online Dangers

3.1 Misinformation, Disinformation

3.1.a Main information sources (wikipedia etc.)

3.1.b Media backgrounds (CNN, Fox News, Sputnik News etc.)

3.1.c How to fact check information?

3.1.d How to identify false information?

3.1.e Recognizing sponsored content

3.1.f Recognizing malvertising

3.1.g AI and Misinformation, Disinformation

3.2 Filter Bubbles

3.2.a Understanding the concept of 'echo chamber', how to avoid it?

3.3 Malware, Viruses, Worms

3.4 Cybermobbing/Cyberbullying

3.5 Scams (telephone/text/email etc.)

3.6 Phishing/Pharming

3.7 Darknet

3.8 Ransomware

4. Protecting against online dangers

4.1 Protecting Devices (e.g., passwords, anti-virus software)

4.2 Protecting Personal Data and Privacy (protecting documents and personal information, awareness on sharing biometric data, cookies)

4.3 Protecting against online dangers (e.g., recognizing dangerous emails, phishing, malvertising, etc.)

4.4 Protecting the Environment

5. Wrapping up

6. Reflection

7. Resources

8. Bibliography

1. Introduction

Security and Safety on the Internet

Using digital technologies involves a range of potential threats and may expose individuals to harmful content and inappropriate online behavior. Being digitally competent includes the ability of recognizing and reflecting on these threats and using digital technologies both effectively and in a secure and responsible manner, minimizing the risk of harm to oneself and others.

Digital safety involves understanding the consequences of one's actions online and being able to distinguish between reliable and unreliable sources of information. It is important to be able to critically evaluate online content, identify and avoid scams, and protect oneself from online predators.

Having responsible online behavior is an important aspect of Media Information (digital) Literacy. Protecting devices, content, personal data, and privacy in digital environments, safeguarding physical and psychological health and being aware of digital technologies for social well-being and social inclusion, but also being informed about the environmental impact of digital technologies and their use, are the main aspects of safely navigating the digital world.

2. Learning Objectives

The competences to be achieved by the adults over 45 years old, after following the content of this module – learning station are to understand risks and threats in digital environments and learn how to avoid them while using any kind of these devices and while navigating through the Internet.

How to protect personal data and therefore health and well-being of the person using a digital device.

To learn how to

3. Online Dangers

3.1 Misinformation, Disinformation

Social networks define so much of people's daily lives that their users are starting to have to deal with risks as in real life.

Since they are one of the most dominant means of informing the world, misinformation and disinformation thrive.

Starting from how the search engines works while navigating the internet and the websites that pop up as the first results, we can talk about the main information sources.

Main Information Sources (Wikipedia etc)

Media Backgrounds (CNN, Fox News, Sputnik News etc)

How to fact check information?

How to identify false information?

Recognizing sponsored content

Recognizing maladvertising

AI and Misinformation, Disinformation (ChatGPT how it works, where does it find the data in order to provide answers to the questions?)

3.2 Filter Bubbles

Understanding the concept of 'echo chamber', how to avoid it?

What is an 'echo chamber'?

An echo chamber is a setting where people are only exposed to ideas and information that they already believe in and find compelling.

Echo chambers have the power to spread false information (misinformation) and warp people's perspectives, making it harder for them to debate tough subjects in uncomfortable discussions and take into account other points of view. Confirmation bias, or the propensity to favour information that confirms preexisting ideas, is a contributing factor in them.

Echo chambers can occur in any setting where information is shared, online or offline.

At the moment where social media allows information to spread much faster, it is easier for someone to become embedded in an echo chamber.

Difference between 'echo chamber' and filter bubbles

The book "The Filter Bubble: What the Internet Is Hiding From You" has led us to realize that our Google searches provide different results than those of other people who are performing the same exact search. We now know that we receive the result that Google's algorithm determines is most relevant to us specifically, so the result that someone else sees may be completely different.

Based on that we can now determine what is a filter bubble.

The new Internet is built on a very simple foundation.

The latest iteration of Internet filters attempts to draw conclusions based on what you appear to enjoy, what you've really done, and what other people who share your interests find appealing.

They are the prediction engines; they are in the process of developing and perfecting a theory about you, your personality, and your future desires. When combined, these engines provide each of us a personalized universe of information, or "filter bubble," that radically changes the way we interact with concepts and data.

How to avoid 'echo chamber' concept in a social group or a website?

Do they typically present a single viewpoint on a subject?

Is there insufficient proof or rumours to substantiate that opinion?

When facts contradict that opinion, are they disregarded?

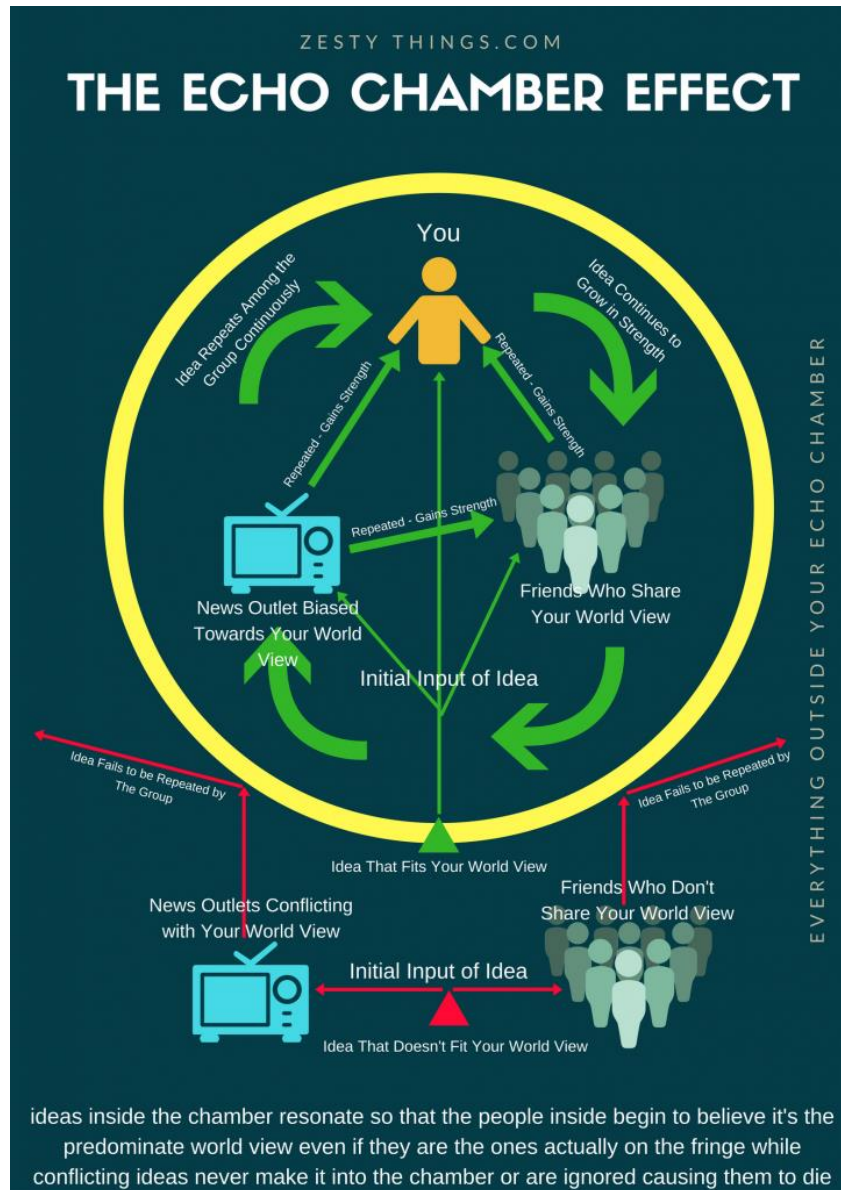
If the answer to all 3 questions above is **yes**, then the social group or website is forming an 'echo chamber'.

After realizing that we are involved in this kind of environment then we can take some decisions that may help us to avoid it.

First of all, by learning about the confirmation bias, which is the first step to accept that we are facing a problem that needs to be solved. Confirmation bias is the propensity to see fresh information as supporting preexisting theories or beliefs.

Except for that, we should develop the practice of examining a variety of news sources to make sure we are obtaining accurate, comprehensive information. Engage with those that have varying opinions, and be sure to address novel concepts with kindness, respect, and factual information.

Video:



Bibliography:

- 1) **The Filter Bubble: What The Internet Is Hiding From You, Eli Pariser**
- 2) <https://edu.gcfglobal.org/en/digital-media-literacy/what-is-an-echo-chamber/1/>
- 3) <https://www.thepacer.net/the-destructive-nature-of-echo-chambers/>

3.3 Malware, Viruses, Worms

Malware

Malicious software

Malware, which stands for malicious software, is a particular kind of application or program designed to annoy or harm users. Malware can be used for a variety of things, such as stealing private data, stopping a computer's functioning, or gaining access to a person's computer system. Malware can conceal its identity and endure for extended periods of time. It can take information from computer users and spy on them without their awareness throughout this period.

The internet has become a venue for malevolent activity due to its increased use. Code that can be executed and replicated is known as malicious code. It strengthens their ability to survive.

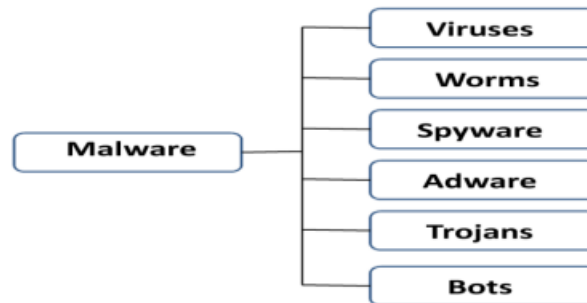


Figure-1. Classification of Malware.

Viruses

When malware replicates into other executable code when it is executed, it is called a virus, and the code is considered infected. When the compromised code executes, it has the ability to infect fresh programs. One of a virus's main distinguishing features is its ability to replicate itself into executable code already in existence.

Worms

A computer worm is a stand-alone malicious computer software that spreads over a network by taking advantage of holes in policies or security flaws in commonly used services. A worm's design is extremely similar to that of a virus; both have the same behavior or attack technique. Worms are regarded as a subtype of viruses by certain classification systems. However, worms are independent entities that do not attach themselves to other files or applications. They are equipped with all the necessary code to fulfill their intended functions and evade detection.

Difference between viruses and worms:

A virus and a worm vary primarily in that a virus must be activated by the host or victim interacting with the infected file. Worms, on the other hand, are standalone harmful programs that, from the moment they get access to a system, may replicate, and spread on their own. In other words, worms may execute or propagate their code across your system without the need for activation or human involvement.

Video: https://www.youtube.com/watch?v=y8a3QoTg4VQ&ab_channel=thecuriousengineer

Bibliography:

- 1) SURVEY AND BRIEF HISTORY ON MALWARE IN NETWORK SECURITY CASE STUDY: VIRUSES, WORMS AND BOTS Saif Uldun Mostfa Kamal, Rana Jabbar Abd Ali, Haider Kamal Alani and Esraa Saad Abdulmajed Faculty of Information Science and Technology, National University of Malaysia (UKM), Malaysia
- 2) <https://www.kaspersky.com/resource-center/threats/computer-viruses-vs-worms>
- 3) Computer Viruses and Malware, John Aycock

3.4 Cybermobbing/Cyberbullying

What is cyberbullying?

Cyberbullying is bullying that takes place over digital devices like cell phones, computers, and tablets. Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content.

Cyberbullying includes:

- sending,
- posting,
- or sharing negative, harmful, false, or mean content about someone else
- sharing personal or private information about someone else

causing embarrassment or humiliation.

Some cyberbullying crosses the line into unlawful or criminal behavior.



Joking VS Bullying

All friends joke around with one other, but especially when it comes to the internet, it may be difficult to discern when someone is only having fun or attempting to harm you. Sometimes they'll brush it off with a "don't take it so seriously" or "just kidding" comment.

The joke is over the line, though, if it makes you feel offended or that they are laughing at you rather than with you. Bullying may occur if you are still unhappy about it after you have begged the other person to stop.

Furthermore, bullying that occurs online may draw unwelcome attention from a variety of sources, including total strangers.

In general, if anything happens that makes you unhappy, you shouldn't have to put up with it, wherever it may occur.

Report cyberbullying

➔ To a Trusted Adult

Most likely the parents of the child that is abused on the Internet.

➔ To Online Service Providers

The terms of service established by social media sites and internet service providers are very strict towards behaviors that don't respect all users, cyberbullying is part of these behaviors.

Inform the social media platform about cyberbullying so they can take appropriate action against people who violate the terms of service.

➔ To Law Enforcement

Cyberbullying sometimes goes beyond all limits and is actually considered a criminal activity. Some actions that immediately need to be reported to the law enforcement are: life and violent threats, stalking, child pornography, overstepping into someone private life in a way that they are exposed to the Internet through photos, recordings, etc.

➔ To Schools

When cyberbullying occurs within the ages that school plays a huge part, it should be reported to some trusted teacher, that will then take the required actions to help the child/teenager that is a victim.

Video: https://www.youtube.com/watch?v=vtfMzmkYp9E&ab_channel=StopBullyingGov

Bibliography:

- 1) <https://www.unicef.org/turkiye/en/cyberbullying-what-it-and-how-stop-it>
- 2) <https://www.stopbullying.gov/cyberbullying/what-is-it>

3.5 Scams (telephone/text/email)

According to the Cambridge dictionary, as a **scam** we define a dishonest plan for making money or getting an advantage, especially one that involves tricking people.

Economic crimes, or scams, are often carried out by well-organized and knowledgeable criminals.

Scams are successful, because they mimic the actual thing and catch you off guard when you're not expecting it.

Scammers use recent technological advancements, popular goods and services, and noteworthy occasions to fabricate tales that seem plausible in order to trick you into parting with your money or personal information.

Prior to acting, always **pause**, consider, and double-check. Because you're in a rush, something appears like a terrific offer you shouldn't pass up, or it seems like it's from someone you trust, scammers hope you won't notice these warning flags.

Different ways of scamming:

- Phishing
- Fake Antivirus
- Social Media Scams
- Telephone Scams
- Email Scams

- Online Shopping and Finance Scams
- Online Dating or Relationship Scams

Video:

Bibliography:

- 1) <https://www.scamwatch.gov.au/protect-yourself/ways-to-spot-and-avoid-scams>
- 2) <https://dictionary.cambridge.org/dictionary/english/scam>
- 3) <https://bitdefender.gr/blog/scam-guide/>

3.6 Phishing/Pharming

More assaults are conducted each month in an effort to trick online users into thinking they are speaking with a reliable source in order to acquire login passwords, account information, and identity data in general. This assault technique, sometimes referred to as "phishing," is most frequently started by sending emails including links to impersonate websites that collect data.



Hackers can swiftly gather personal data from online publications such as professional profiles, social networking sites, and other publications in order to determine the triggers that individuals react to



How to detect a phishing email

1. Email sent from public email domain

Most organisations/businesses have their own email domain. If the domain is "@gmail.com" it may be considered as suspicious.

2. Too good to be true

If a message proposes a huge offer - reward for the recipient it probably is fake.

Something that is very eye-catching should be considered suspicious and not trust-worthy.

3. Suspicious Attachments/ Hyperlinks


Every email sent by a scammer has a payload. This will either be a link to a fake website or an infected attachment that you are requested to download.

These payloads are designed to intercept sensitive data, including account numbers, credit card numbers, phone numbers, and login passwords.

4. Urgent Action needed

Cybercriminals sometimes use the excuse that the amazing discounts are only available for a short period of time, which is one of their favorite strategies.

More info here: <https://www.phishing.org/what-is-phishing>











Pharming

Cybercriminals utilize pharming, a fraud, to infect servers or personal PCs with harmful programs. Its name, which combines the terms "farming" and "phishing," alludes to a new, more intricate method that hackers employ to get private data.

Pharming is an exploitative technique wherein a server is poisoned or individual workstations are infiltrated. Website redirection code is used by both choices, although it's implemented differently.

Differences between Pharming and Phishing

Parameters	 Pharming	 Phishing
 Definition	More advanced technique to get users credentials by leading users into a fraud website	Attacker tries to gain access to sensitive information of users by means of illegal electronic communication
 Objective	Redirect traffic from one website to an identical-looking one to steal information	To scam people one at a time using email or instant messaging
 Category	Similar in nature to email phishing	E-mail fraud
 Process	Personal and private information is obtained through domain spoofing, DNS cache poisoning, DNS hijacking, etc.	Attacker tricks the victims into giving out personal information by email, fax, or message
 Technique	DNS server is poisoned, and users are redirected to a different website	Fraudulent email contains a link to a website seeking personal details from users
 Medium	Local hosts file, websites, home router, DNS server, etc.	Email, fax, and instant messaging

Bibliography:

- 1) Learning to detect phishing emails, Authors: Ian Fette, Norman Sadeh, Anthony Tomasic, 2007
- 2) <https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email>
- 3) <https://www.phishing.org/what-is-phishing>
- 4) <https://cofense.com/knowledge-center/how-to-spot-phishing/>
- 5) <https://www.pandasecurity.com/en/mediacenter/what-is-pharming/>
- 6) 1st picture:
<https://www.propertycasualty360.com/2019/05/24/how-effective-employee-education-and-training-combats-phishing-attack-risk-414-155823/?slreturn=20231009104027>
- 7)

3.7 Darknet

Search engines like Google, Yahoo, and Bing are unable to index material on the deep web, and the dark web (darknet) is part of the deep web. Because it is purposefully concealed, the dark web cannot be accessed using a regular browser. Anyone with access to The Onion Router (TOR) browser can access the deep web. TOR is a virtual, encrypted tunnel that enables anonymous internet access by hiding users' identities and network activity. The dark web is essentially an online marketplace for anything, including and not restricted to credit card information, forged documents, drugs, weapons, and obscene pornography. It even offers services for hiring someone to commit murder.

When referring to the Internet most of the time we talk about the Surface Web, as it is the place that everyone has access to through a simple web browser, like Google Chrome, Mozilla Firefox, etc. What we are leaving out of the conversation is the Deep Web and therefore the Darknet (Dark Web) which is a small part of it, most speculate that it is about 5% of it.

To get access to the Deep Web, it is important to know about cyber security, and how to protect yourself from any potential online danger that you may face in this part of the Internet. TOR (The Onion Router) browser provides anonymity to its users, by hiding their identity and network activity, and therefore it is needed to access the dark web.

This anonymity is practically why TOR is being used either from cybercriminals or ordinary citizens who are concerned with their privacy while navigating through the Internet in general. For instance, dissidents may utilize the dark web to communicate with one another if they are afraid of facing political persecution from their governments.

The dark web is purposefully concealed, and this is why it cannot be accessed through a regular browser. It is essentially an online marketplace for anything, including and not restricted to credit card information, forged documents, drugs, weapons, obscene pornography and even hire services for murder.

Illegal purchases are further facilitated by the existence of anonymous payment systems (virtual currencies).

The darknet in addition to offering a safe refuge for illegal transactions, provides a secure space for like-minded people to interact and share thoughts and experiences on abnormal themes and behaviors like extremism and terrorism.

As it is mentioned in the article “An Overview of Darknet, Rise and Challenges and Its Assumptions”, these connections are made only between trusted peers sometimes called “friends” (F2F) using non – standard protocols and ports.

Surface Web vs. Deep Web vs. Dark Web

Surface Web

- Searchable websites
- E-commerce sites
- News sites
- Public blogs and forums



Deep Web

- Websites requiring a login
- Email accounts
- Online banking accounts
- Subscription services



Dark Web

- Sites requiring access through Tor
- Websites not indexed on search engines
- .onion domains
- Decentralized marketplaces



Myths for Dark Web Debunked



Dark Web is 96% of the Internet

There is still a widespread misperception that the phrases "deep web" and "dark web" may be used interchangeably. Actually, less than 1% of the whole deep web is made up of the dark web.

All illegal content is easily accessible

Even though the dark web is notorious for supporting illicit conduct, not all of its websites may be accessed just because you can access the dark web.

Tor is the Only Dark Web Service

Although the term "dark web" has come to refer to Tor, there are other services that operate as extra layers of anonymous traffic on top of the standard Internet.

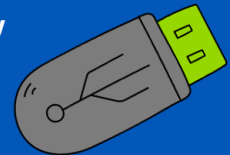


It's illegal to visit the dark web

Using Tor or accessing the Dark Web are not illegal. Naturally, it is against the law to commit crimes under false pretenses, such as gaining access to photos of child abuse, encouraging terrorism, or selling contraband like firearms.

The Dark Web Offers Complete Anonymity

Even while Tor provides a high level of anonymity, there are still methods for a user to unintentionally betray who they are.



Stay safe online!



Bibliography:

- 1) An Overview of Darknet, Rise and Challenges and Its Assumptions, Zakariye Mohamud Omar, Jamaluddin Ibrahim, 2020, Faculty of Information and Communication Technology, International Islamic University Malaysia (IIUM), Kuala Lumpur, Malaysia
- 2) The Darknet and the Future of Content Distribution Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman
- 3) <https://cyberalert.gr/darknet/>
- 4) <https://us.norton.com/blog/how-to/how-can-i-access-the-deep-web> (picture)
- 5) Privacy-preserving deanonymization of Dark Web Tor Onion services for criminal investigations, Ângelo, Daniel José Ferreira
- 6) <https://www.domaintools.com/resources/blog/dark-web-myths-and-misconceptions/>
- 7) <https://www.soscanhelp.com/blog/dark-web-myths>
- 8) <https://www.thinkuknow.co.uk/professionals/our-views/the-dark-web/>

3.8 Ransomware

Ransomware is a **type of cyberattack** method where malicious software is used at exorbitant prices to hold a victim's computer hostage until a payment is made. The supposed secrecy of encipherment transactions makes bitcoin cash redemption a popular request from ransomware attackers. Users are blocked by the per-ware for a specified period of time, after which user data or refunds are erased.

Ransomware is a type of malware that uses a deadline to force its victims to pay a specific amount digitally. Attackers disseminate these ransoms using a number of web servers and a paid service known as ransomware-as-a-service (RaaS) [7]. RaaS indicates that all that is required for participation is the desire to disseminate ransomware (often via botnet email), not any specialized programming skills. After registering, the affiliate only has to download a specially made binary ransomware. The original JavaScript-written ransomware in the world, Ransom32, is the source of these modifications. The development of the onion router (TOR) and a thriving dark web underground economy has made it much simpler for experienced hackers to provide their services to up-and-coming novice hackers who don't seem to have the infrastructure or the skills to spread ransomware widely enough to take advantage of already-existing capabilities to launch a ransomware campaign. Long before the concept of RaaS emerged, attackers would rent out their botnet, which they had used to gather a large number of prey hosts, to anybody looking to start a spam campaign or perform a DDoS assault on a target.

Nonetheless, these assailants follow certain procedures in order to launch a successful and efficient attack on their target (s). Under typical conditions, their procedures are known to adhere to a set of precise processes.

→ Should I pay the ransom?

The paying of ransom demands is not supported, encouraged, or condoned by law enforcement. Even if you manage to pay the ransom, there's no assurance that you'll be able to access your computer or data.

The infection will remain on your machine.

You'll be funding illegal organizations.

You're more likely to come under attack later on.

You should thus always keep a current offline backup of your most crucial files and data.

In order to stop ransomware attacks in the future, it's critical to attempt to determine how the attackers initially got access to your network.

Prevent Ransomware

Sixteen best practices to protect devices and systems from ransomware.



- 1 Protect ports and settings
- 2 Download a VPN
- 3 Install antivirus software
- 4 Secure backup files
- 5 Verify download sites
- 6 Set up secure configuration settings
- 7 Implement cybersecurity training
- 8 Use an Intrusion Detection System
- 9 Harden endpoints
- 10 Update systems
- 11 Enable zero trust security
- 12 Only click trusted links
- 13 Authorize email security
- 14 Keep personal information private
- 15 Apply network segmentation
- 16 Create an incident response plan

Video: https://www.youtube.com/watch?v=-KL9APUjj3E&ab_channel=Simplilearn

Bibliography:

- 1) A Comprehensive Survey on Ransomware Attack: A Growing Havoc Cyberthreat, Aditya Tandon and Anand Nayyar
- 2) <https://pandasecurity.com/en/mediacenter/avoid-ransomware/>
- 3) https://www.ncsc.gov.uk/ransomware/home#section_3
- 4) <https://nationalcrimeagency.gov.uk/who-we-are/publications/672-ransomware-extortion-and-the-cyber-crime-ecosystem/file>
- 5) A brief study of Wannacry Threat: Ransomware Attack 2017, Savita Mohurle & Manisha Patil, International Journal of Advanced Research in Computer Science
- 6) <https://cyberalert.gr/ransomware/>

4. Protecting against online dangers

4.1 Protecting Devices (e.g., passwords, anti-virus software)

Apart from safeguarding and eliminating malware infections such as Trojan, virus, worm, bot, rootkit, and backdoor infections, some significant threats that users of anti-virus software need to be protected against are:

- Session Hijacking
- Man-In-The-Middle attacks
- Phishing
- Malware downloads
- Theft of credentials and identity theft
- Execution of malicious links
- Visit to unsafe sites
- Cross-Site-Scripting attacks
- Identify and fix / warn on security vulnerabilities
- Recording of user's key strokes and activities
- Expectations from Anti-Virus Software and their Vendors

Bibliography:

- 1) https://link.springer.com/chapter/10.1007/978-1-4302-6383-8_7#Sec20
- 2)

4.2 Protecting Personal Data and Privacy (protecting documents and personal information, awareness on sharing biometric data, cookies)

4.3 Protecting against online dangers (e.g., recognizing dangerous emails, phishing, malvertising, etc.)

4.4 Protecting the Environment