Quadrant-I (e-Text)

Details of Module and its structure

Module Detail	
Subject Name	Education
Course Name	ICT in Education
Course Code	EDU504
Module Name/Title	Computer security: privacy, hacking, virus, spy ware, misuse, abuse, antivirus, firewall, and safe practices, fare use and piracy.
Module Code	IIE020
Pre-requisites	Basic knowledge of software, files and folders, e-mails, social media and web browsing
Learning Outcomes	1. After going through this lesson, the learners will be able- 2. To describe the concept of computer privacy and internet privacy. 3. To cite the examples of hacking from their day-to-day life experiences. 4. To differentiate between different types of virus, worm and spyware 5. To describe various practices of misuse and abuse of internet 6. To evaluate the uses of antivirus and firewall in computer security 7. To critically reflect on the safe practices to avoid hacking and corruption of the computer system or network 8. To describe software piracy and copyright infringement.
Keywords	Computer security, computer privacy, internet privacy, malware, virus, worm and spyware, anti-virus and firewall, software piracy

1. Development Team

Role	Name	Affiliation
Principal Investigator (PI)	Dr. S. K. Bawa	Central University of Punjab, Bhatinda
Subject Matter Expert (SME)	Dr. Shilpi Kumari	School of Education, MGAHV, Wardha (MH)

Table of Contents

Introduction

This module describes the concepts of computer security including computer and internet privacy, threats to computer security, safe practices of using the computer and internet, use of antivirus and firewall to maintain computer security and also highlights the copyright infringement due to software piracy and unfair use of the content of the websites.

Computer Privacy

Privacy is a term used to describe how much an individual feels safe in a location. Computer Privacy generally deals with the information which the user shares while s/he visits a web page. Thus, in order to secure computer privacy we must check the company or website privacy policy.

Computer privacy depends upon the way we use our computers. In order to protect our computer data not to be seen by other local or remote users, it is important to be aware about visibility of data on a computer. We should close any customized aspect of our sessions of our computer use, if we are using a public computer that is always on. We should log out any personal internet account and close any programme before we leave the computer. We should also logout our operating system account or shut down the system before leaving it.

Now a days, the operating system allows us to set up multiple accounts for different users on a computer. These accounts must be password protected. Thus, every user can keep their personal files and settings private and safe. Even the files and folders can be password protected using operating system's file explorer function.

Internet Privacy

With greater outreach of the internet, its use for searching and sharing the information has remarkably increased, but complex issue of internet privacy has also emerged parallel... how the information that a user shares while visiting a web page is utilized, who that the information is shared with or if that information is used to track the users. Thus, widespread use of the internet has inevitably led to intense debates about the use of user privacy. There are different steps that we must take up in order to enhance our internet privacy. These are as follows:

1. We should be aware about the functionality of the web browser that we frequently use. Our web browser can store the data that we enter or share while visiting a website like our username, password, e-mail address etc. Our browser can also keep the record of the weblinks that we have visited in the history. Hence, to maximise browser privacy, we should configure these settings and regularly clean the data from the web browser. Moreover we should also configure cookie settings.
2. Most people do not know what kind of information they should or should not post on the internet. For example: While doing online financial transaction we must be very careful that whether we are sharing our financial details with an authentic website.
3. With the emergence of social networking sites like facebook, twitter, instagram, pinterest etc. people have started leading a psudolife over the internet. In order to show how much luxurious or happy life they are spending and to be followed by more number of people, they put private information in public domain, which is liable to be misinterpreted or misused by malicious users.
4. Some stringent laws against the violation of internet privacy should be enforced so that the people those who violate these laws can be strictly punished.
5. We should use such passwords which are difficult to predict. We should not use the names of family members or pets as password.
6. We should not share the bank account details, debit or credit card no., PIN etc. with anybody under any circumstances and if, it is required, we must be sure that the website is an trustworthy website. While making online payment for online purchases, we should adopt more secure mode of online payment like pay pal particularly for overseas transaction.
7. We should click on any message in the junk or spam mail only when we are sure that it has been sent from a relevant source.
8. Check the weblink that we type in the URL bar has the format https://www.----------.

9. If we are searching for a website and we are being redirected to a webpage which is different from the one that we have requested for then we must clean the browser history and make the option of cookies turned off.

Hacking

Hacking in Networking and computing means access to another network or computer without having any prior permission of the owner with some technical effort. Hacking is called unauthorized intrusion on one's computer or network whereas the person who does hacking is called hacker. The hacker changes the security features of the system or network after getting access of the system. The hacker is technically very sound in his work and he has a depth of knowledge about the network or computer system, so that s/he can enter into someone else's network.

Ethical hacking: Hacking is considered to be serious crimes in many cases but if the hacking is done through permission from the organisation or a contract with the organisation then it is called legal and the term 'Ethical Hacker' is used for the such hacker. Ethical hacker has authorization to examine the target.

Types of Hackers

Black hat hacker: Black hat hackers are those hackers that *break* rules for personal purposes and illegally break others' computer security. Example - Theft of someone else's credit card number, breaking a computer network for money.

White Hat Hackers: White hat hackers are counted as good people, they are those hackers that access the system to fix the computer's weakness, or are those computer security experts, who ensure that the company's information and systems are safe.

Gray hat: These hackers are in a category which is in between white and black hat hackers, but they break the computer system without any authority, so that weakness regarding security of the system can be conveyed to the owner of the system.

Script kiddies: These are hackers which do not have too much technical expertise but they do hacking using others' tools.

Hacktivist: These hackers are religion wise or politically motivated so that any special message can be sent to a political or a religion related website.

Phishing and Pharming are the most common methods used by the hackers to attack the privacy of the internet users. In phishing a web page similar to the web page requested by the users is sent to the browser and the users can enter his/her credentials on this web page. In case of Pharming they are redirected to a completely different webpage which starts fetching the details of the users. The hacker has complete access to the fraudulent web page in both the cases.

Dark web i.e. the web used for buying drugs and weapons, illegitimate pornography etc. can be accessed through a special browser. Visiting these websites creates a greater risk of being attacked by hackers.

There are many websites which utilize cookies to sustain the user viewership. These send a piece of information to the user's web browser which has details about the preferences of the user, his/her comments, profile etc. thus when the user visits the website next time, s/he gets her/his preferences first. Though the cookies itself is not harmful, but the information that it carries if falls into the wrong hands, it may be misused like the user may get very personalised messages, advertisements, spam etc.

Malware and Spyware are also huge threats to user's computer security. These enter the user's system from internet and start sending the user's personal information to another location from time to time. This eventually leads to illegal data distribution.

Sometimes a trojan is sent to the user's system in the form an e-mail attachment (spam) or downloads links or files. When the user opens the e-mail attachment or downloads the file or click the link, the user's system gets encrypted and the data of the system become inaccessible to the user. The user gets the alert message that your system has been used for illegal activities and thus, the system gets locked. Now the system starts demanding the ransom for decryption of the data. This process is known as crypto virology using ransomware.

Computer virus

Computer virus is a small software programme that spreads from one computer to another computer and disrupts the computer operation. It requires a host, to attach and spread throughout the system. Viruses are executable files or attach themselves to other executable files of the system to operate and get transferred to other computers via e-mail. Viruses can be hidden in the form of attachments

of entertaining images, greeting cards, audio or video files. Computer viruses can corrupt or remove data on the computer, use an email programme to spread viruses on other computers, or even remove everything on the hard disk. It can also modify personal data, text files and even can bring the computer to a halt.

Worm

Worm is a computer code or a standalone malware that replicates itself in order to spread to other computers via network without user interaction. Most worms begin as an email attachment, which infects the computer when opened. This worm scans the infected computer for files, such as address book or temporary webpage, which includes email addresses. The worm uses the address to send the infected e-mail message and in the subsequent email messages, duplicate (or spoof) the "sender" address so that the infected message appears from the person you know. Worms are not always destructive for computers, but these usually increase network traffic, reduce computer and network performance and also raise stability issues.

Spyware

Spyware term is used for a group of malicious software including keyloggers, cookies, adware, system monitors, tracking cookies and Trojans. It is software that is installed on a computer without users' knowledge. Any software can be classified as spyware if it is downloaded without the user's authorisation. Besides violating the end user's privacy and it can cause serious harms to the system. Spyware can track internet search habits and even redirect our web browser to a different website from the website we mean. Spyware is mostly used for the purposes of tracking and storing internet users' movements on the web and serving up pop-up ads to the internet users. Whenever spyware is used for malicious purpose, its presence is hidden from the user. Spyware may be installed on our computer without our knowledge. These programs can change the configuration of our computer or gather advertising data and personal information. Some Spyware can also be installed in public computer intentionally to monitor the users. It can also interfere with the user's control of the computer by installing additional software or redirecting web browser. It can also change the computer settings thereby reducing the internet speed, unauthorised changes in software settings or changes in browser settings.

Trojan Horse

Trojan Horse is a malicious software program that enters the computer through a legitimate program such as a screen saver. After this, it places the code in the operating system, from which the hacker is able to access the infected computer. Trojans usually do not spread themselves. They are spread by viruses, worms or downloaded software. Trojan can delete copy, modify or block data and also disrupts the performance of the target computers or networks.

Adware

These are usually bundled with the free software, shareware and utilities downloaded from the internet or installed onto a user's device when the user visits an infected website.

Cookies

These are used to track users' internet browsing habits. An advertiser might use cookies to track what web pages a user usually visit and thus send him or her personalised messages or advertisements. For Example: an advertiser could track a user's browser history.

Keyboard Loggers

These are a type of system monitor that are often used by cybercriminals to steal user's personally identifiable information (PII). These can be also be used by employers to observe employees' computer activities and parents to supervise their children's internet uses.

Misuse and abuse of Internet

Today the internet is the lifeline of most of us. However, misuse of internet may create threat to one's computer security.

Hacking

Hackers can fetch the user's personal information like security passwords, security statements, personal profile, preferences and also their bank account details, in some of the cases, through phishing and pharming and also with the help of malwares and cookies and misuse it in a no. of ways.

Threat of identity

If we are a user of social networking site, we might have passion of having a long list of friends and we may be careless of the fact that all the friends in the list might not have genuine account. The pictures and other posts can be misused in a way that it can be posted on fake advertisement sites and porn websites etc.

Porn

It is one of the most shameful uses of the internet. Exposure of porn websites to minors may create a wrong impression of sexual intercourses in their mind and thus, they do not value the importance and purity of sexual intercourse,

Black Marketing of Pirated software

Pirated software are available in much less price than the original software, hence the users of the internet purchase pirated stuff without having an empathy towards those who actually work hard to produce the software originally and thus they encourage black market production of pirated software.

Spam or Junk e-mails

There are hackers who send junk mails or spam which are unwanted mails to many recipients at a time. It increases internet trafficking and when the user knowingly or unknowingly opens this mail or download the attachment contained in the mail, a lot of viruses enter the user's system.

Squandering

Internet has entered to every aspect of our life so deeply that we can't avoid to use it. However, many a times we forget our purpose of using the internet and instead of doing the work quicker, we get caught in the vicious circle of the offers in the form of pop up ads of online games, chat rooms, porn etc. and waste even more time.

Exposure to negativity

Exposure to negativity like porn websites, violence and criminal videos can direct the internet users particularly youngsters to create bombs, how to commit suicide, develop emotional physical relationship etc.

Cyber Bullying

There are many internet users who derive pleasure out of disturbing people. They may share their friends' pictures deliberately in wrong websites like porn or their friends' very personal details in social media.

Like every human creation, internet has also both pros and cons. The power to use the internet lies in the hands of the users. It is not invented to cause miseries to others. Thus, we should make precautionary use of the internet.

Anti-Virus

Antivirus software is a program that will detect viruses in the computer and delete them from the computer and also prevent them from entering the computer.

Since the viruses are different, the method of detecting these viruses would be different, hence antivirus uses different methods to scan and detect the viruses.

There are following methods of detecting the antivirus.

Signature-Based Detection: It is the simplest form of detection technique. It protects against known or common threats. A signature is a known pattern of a threat. For example: An e-mail with an attachment containing a known malware with an interesting subject.

Heuristic-Based Detection: It is designed to detect previously unknown threats as well as new variants of viruses already present in the 'wild'. It utilizes file emulation and file analysis technique to detect unknown threats.

Behavioural-Based Detection: In order to detect the viruses with modifications or encryptions, the signature lists require frequent updates and thus, many new viruses go undetected. Hence, security providers are turning their attention to behaviour based approaches for identifying new viruses. It analyses the behaviour and characteristics of programs running on a computer and shuts down activity that seems suspicious.

Sandbox Detection: It is the file emulation technique which allows file to run in a controlled virtual system or sandbox to see what it does and if the file acts like a virus, it is deemed as a virus.

File analysis technique: It deeply analyses the file to search for its intent, destination and purpose and if the file has instructions to delete certain files, it is considered to be a virus.

Firewall

Broadly speaking, a computer firewall can be used to enhance the security of computers connected to a network such as LAN or the internet. These are an integral part of a comprehensive security framework for one's private network. It separates our computer from the internet using a wall of code that inspects each individual's packet of data as it arrives at either side of the firewall. It provides further security by providing control over what types of system functions and processes have access to networking resources.

Types of Firewall

Packet Filtering: This is the original type of firewall which operates inline at junction points where devices such as routers and switches are functioning. It compares each packet of information received to a set of user-defined criteria such as allowed IP addresses, packet type, port number etc.

Circuit-level Gateways: Theses devices monitor the TCP handshakes across the network between the local and remote hosts to determine whether the remote system is considered trusted. However, these don't inspect the packets themselves.

Stateful Inspection Firewalls: It examines each of the packets across the network and also tracks whether or not the packet is a part of an established TCP session. Thus it offers more security than packet filtering or circuit level gateways alone.

Proxy firewalls: These are considered to be the most secure type of firewall because they prevent direct network contact with other systems because a proxy firewall has its own IP address, an outside network will never receive packets from the sending network directly.

Safe Practices

So as to ascertain the computer security, one has to adopt following safe practices while using the system or the network.

1. We should check whether or not the system's firewall is on or connected.
2. If we don't really need our files to be visible to other systems, we should disable file and media sharing completely.
3. We should always backup our data, which can protects us in a case of emergency like computer crash, data encryption (ransomware).
4. We should surf only those websites which have a green lock in the address bar and the code prefix 'https://' at the beginning of the URL particularly while visiting banking sites. If we are fond of online shopping, we must be very careful that we should not open the attachments or links in e-mail messages sent by the online shopping website.
5. We should keep ourselves refrained from the websites which lure the users with amazing deals like a deal for 90% off.

6. We should never reveal sensitive information particularly with our social media profile.
7. We should avoid opening unknown e-mails or spam and never download attachment or click links which are contained in them. We should also be careful for an e-mail from someone whom we know well and regularly communicate because, in some cases, it may have a suspicious link and unusual content, if his or her account is hacked.
8. We should be careful of using flash and other portable devices in public computers. It may contain a software that can load data from drives automatically.
9. We should be careful of the policies and rules regarding public computer usage.
10. The use of credit card numbers and important login information should be avoided on public computer,
11. Whenever we work on a public computer we should be careful while typing in usernames and passwords. We should always take a glance around to ensure that no passerby is watching us while feeding any security credentials. We should use such passwords which are difficult to predict. We should use a separate user login account while working on a public computer. We should close all the open pages and always log out from the system before leaving it and also shut down the system if it is not in use.
12. We should always keep our laptop in a locked bag or drawer when we are not using it particularly in airports, cafes or hotel rooms. We can use biometric Ids and link laptop to our cell phone via Bluetooth.

Fair Use and Piracy

In copy right law, fair use is more frequently discussed issue and this issue is often misunderstood. Hence, the internet user must ask a question to himself/herself that 'Is my use of the content of the website is a fair use?' The unauthorised use of copyrighted material constitutes an infringement of these rights. However, copyrighted material can be used by public for the purposes like criticism, comment, news reporting, teaching, scholarship or research. Fair use of copyrighted work is guided by following four factors:

1.) The purpose and character of the use

2.) The nature of the copyrighted work

3.) The amount and substantiality of the portion used in relation to copyrighted work as a whole.

4.) The effect of the use upon the potential market for the copyrighted work.

Piracy is the unauthorised distribution, theft, reproduction, copying, performance, storage, sale or other use of intellectual property (IP) protected under copyright law. It is a form of copyright infringement. It is an unauthorised duplication of copyrighted content that is then sold at substantially lower prices in the 'grey market.'

Software piracy is the act of illegally using, copying or distributing software without the ownership of legal rights. Majority of software purchased today as a single user license i.e. only one computer may have that software installed on it at one time. Copying that software to multiple computers or sharing it with friends without multiple license is considered software piracy, which is illegal.

In United States, computer works are considered as literary works, hence it comes under copyrighted material. Though the use of literary work for personal study, research or appreciation does not come under copyright law but in case of software it is different in many cases. For example: a person can download a piracy version of software or movie from the internet for personal study and research but he will be asked to delete the file within 24 hours and if he does not delete the file, it is against copyright law.

There are following five types of software piracy-

1.) Counterfeiting: This type of piracy is the illegal duplication of copyrighted packaged software.

2.) **Internet Piracy:** There are websites that make the software available for free download or in exchange of others. Internet auction sites also offer counterfeit software.

3.) End User Piracy: It includes using a single licensed copy of software and installing it on multiple computers, copying discs for installation or distribution, taking an advantage of upgrade offers without having a legal or original copy of the software to be upgraded.

4.) **Client-Server Overuse:** If we are using LAN and have installed the software on the server for multiple individuals to use, we must be sure that whether our license allows us to do so.

5.) **Hard-disk loading:** This occurs when a company sells the new computers with illegal copies of software for making the sell an attractive deal.

Internet service providers are liable for infringement conducted through various internet-related functions such as linking, media streaming, file sharing and storage. Fair use, however, involves the use of low resolution, 'thumbnail' copes of photographic images. Linking is an ubiquitous internet function. It includes two types of links-outline links and inline links. When a user click on an outline link, the browser displays a new website and when a user clicks on an inline link, the browser pulls the content example: an image file, textual material or audio streaming from another website into the linking website. Many website owners want their material disseminated as widely as possible but it may cause harm if it burdens the linked sites' server by increasing traffic to the website.

Conclusion

Hacking, misuse and abuse of the computer/internet are vital issues in the field computer security. Hacking is unauthorised intrusion on one's computer or network without permission. Misuse and abuse of the internet involves cyber bullying, black marketing of pirated software, surfing of porn websites etc. If we are computer or internet users we must be aware about some common threats to computer/internet security like viruses, worms and spyware. Virus is a malware which links itself to the executable files of a computer and gets transferred to other computers via e-mail. Worm is a computer code or standalone malware which replicates itself in order to spread to other computers via network without user interaction. Hence, to ensure computer security we must adopt common safety practices like always keeping the backup of our computer data, avoid opening the unwanted emails, turning off the cookies option of the web browser when not required, surfing only those websites which have a green lock in the address bar etc. We should also install antivirus and firewall in the system. The issue of software privacy is also prevalent in the cyber world which leads to violation of

copyright law. Besides software piracy, internet service providers may also infringe the law of copyright through linking, media streaming, file sharing and storage.

Glossary

Adware: These are usually bundles with free software, downloaded from the internet when the user visits an infected website.

Anti-virus: It is the software that detects virus in the computer and delete them from the computer and also prevents them from entering the computer.

Black Hat hackers: These are the hackers who illegally break others' computer security for personal purposes.

Computer privacy: It deals with the information that the user share while they visit a web page. It protects computer data not to be seen or stolen by other local or remote users.

Cookies: These are used by the advertisers to track user's internet browsing habit.

Cryptovirology: In this malware attack, the user's system gets encrypted and the data of the system becomes inaccessible to the user.

Cyber bullying: There are many internet users who derive pleasure out of disturbing people which is not only unethical but also cause monetary or psychological harm to them.

Dark Web: It is the web used for buying drugs, weapons, illegitimate pornography etc.

Firewall: It is a network security system that monitors and controls incoming and outgoing network traffic based on pre-determined security rules.

Grey Hat hackers: These are the hackers who break the computer system without any authority so that weakness regarding security of the system can conveyed to the owner of the system.

Hacking: Hacking means access to another network or computer without having any prior permission of the owner with some technical effort.

Hacktivist: These are politically and religion wise motivated hackers.

Internet Privacy: It concerns about how the information that a user shares while visiting a web page is utilized, who that the information is shared with or if that information is used to track the users.

Keyboard Loggers: These are system monitors which keep track of the user's computer activities and may steal user's personally identifiable information (PII).

Malware: These are the malicious software programmes which may destroy the system or increase internet trafficking. For example: Viruses, worms, spyware, adware etc.

Phising: It is one of the most common methods used by the hackers to attack the privacy of the internet users. In this case, a web page similar to the web-page requested by the users is sent to the browser.

Phraming: It is one of the most common methods used by the hackers to attack the privacy of the internet users. In this case, they are directed to a web page completely different from the web page which they have requested.

Pirated Software: These are the duplicate software which are available in much less price than the original software.

Porn: It is one of the most shameful uses of the internet. These websites contain sexual or vulgar images, audios and videos**.**

Ransomware: It is a Trojan horse which encrypts the user's data and starts demanding ransom from the user for decryption of the data.

Script Kiddies: These hackers do hacking using others' tools.

Spam: These are unwanted e-mails to many recipients at a time.

Spyware: It is the software which is installed on a computer without user's knowledge like keyloggers, cookies, adware etc.

Squandering: Many a times, we forget our purpose of using the internet and instead of doing the work quicker, we get caught in browsing online games, chat rooms, porn etc. forgetting what we actually have to do.

Trojan: It is a malicious programme which is hidden inside a legitimate programme and thus gains illegal access to the user's system.

Virus: Theses are executable files or they attach themselves to other executable files of the system to operate. These spread from one computer to another computer via e-mail.

Worm: It is a standalone software that replicates itself in order to spread to other computers via network without user interaction

Quadrant-IV

Multiple Choice Questions

1. What is sand box detection?
   a) signature based detection
   b) protects against known or common threats
   c) deals with the known malwares
   d) attacks viruses in a controlled virtual system

2.) What is behavioural based detection?
   a) deals with signatures of known threats
   b) deals with encrypted virus
   c) attacks viruses in a sandbox
   d) deals with the database of known

3.) How does heuristic-based detection work?
   a) utilizes file emulation technique
   b) attacks against database of the known viruses
   c) utilizes behavioural approaches
   d) attacks against the encrypted viruses

4.) Among the following security systems which prevents unauthorised access to a private network?
   a) Anti-virus
   b) Anti-malware
   c) Firewall
   d) Scanner

5.) How does a proxy firewall work?
   a) prevents direct contact of a private network with other systems
   b) monitors the TCP handsakes across the networks
   c) compares each packet of information against a set of user-defined criteria
   d) promotes direct contact between the private network with other systems

6.) What is Keyboard logger?
   a) Pirated software
   b) Porn websites
   c) Unwanted e-mails
   d) System monitors

7.) How does a Trojan Horse work?
   a) enters the system through a legitimate programme
   b) utility downloaded from the internet
   c) used by advertisers to track the user's preferences
   d) spread from one computer to another computer

8.) What do you mean by the term dark web?
   a) Websites related to advertisers
   b) Websites related to auction of the softwares
   c) Websites used for special chats and messages

d) Illegitimate websites

9.) What is the similarity between black hat hacker and grey hat hacker?
a) Both black hat and grey hat hackers break the computer security without any legal authorisation
b) Both break the rules of computer security for personal purposes
c) Both seek permission from the owner of the system
d) Installation of free software

10.) How does a ransomware work?
a) Encryption
b) Spread of viruses
c) Spread of Worms
d) Installation of free software

Answer 1-d, 2-b, 3-a, 4-c, 5-a, 6-d, 7-a, 8-d, 9-a, 10-a.

Web resources

https://techspirited.com/internet-privacy-issues
https://cyber.laws.com/hacking
https://www.techopedia.com/definition/26361/hacking
https://antivirus.comodo.com/blog/comodo-news/hacking-definition-and-its-types/
https://listaka.com/10-dangerous-ways-the-internet-is-being-misused/
https://www.computerhope.com/jargon/s/softpira.htm
https://www.symantec.com/en/uk/about/legal/anti-piracy/types-piracy
https://blog.nus.edu.sg/is1103grp203/2013/04/07/filevault2-in-mac-os-x/
https://techdifferences.com/difference-between-virus-and-worms.html
What is a Trojan Virus? | How to Prevent Trojan Horse Virus Attacks
New antivirus software looks at behaviors, not signatures
What is Heuristic Antivirus Detection? - Top Ten Reviews
https://www.toptenreviews.com › articles
https://searchsecurity.techtarget.com/feature/The-five-different-types-of-firewalls
https://personalfirewall.comodo.com/what-is-firewall.html
https://searchsecurity.techtarget.com/definition/proxy-firewall
https://www.google.com/amp/s/www.kaspersky.com/blog/6-tips-to-keep-your-home-computer-safe-and-secure/3071/amp/
https://www.bankinfosecurity.com/top-10-computer-safety-tips-a-697