ASSIGNMENT 12

1. *According to the ENISA Threat Landscape report for 2023, what emerges as the primary threat within cyberspace? Why is this particular threat deemed particularly alarming? Furthermore, based on the insights provided in the document, what strategies are recommended to effectively mitigate this threat?*

ANS:

The European Union Agency for Cybersecurity (ENISA) recently released its annual Threat Landscape Report for 2023. The report identifies the top threats, major trends, threat actors, and attack techniques expected to shape the cybersecurity landscape in the coming years. In this blog, we will summarize the key findings of the report and offer actionable recommendations to mitigate these threats

The ENISA Threat Landscape Report is an annual report that provides a comprehensive overview of the cybersecurity threat landscape. The report is based on a thorough analysis of various sources, including open-source intelligence, expert opinions, and data from multiple organizations. The report aims to provide insights into emerging threats and trends in the cybersecurity landscape and help organizations improve their cybersecurity posture.

Ransomware still gets top of the podium, accounting for 34% of EU threats. Ransomware attacks are expected to continue to rise in frequency and sophistication. Attackers increasingly use advanced techniques such as double extortion and supply chain attacks to target organizations. The report also highlights that ransomware attacks are becoming more targeted, with attackers focusing on high-value targets with particular emphasis on the Industrial and Manufacturing sectors. Disrupting manufacturing processes or seizing control of industrial systems can result in significant financial losses and operational downtime, making it an attractive target.

Supply chain attacks are becoming more prevalent and sophisticated, with threat actors misusing legitimate tools primarily to prolong their cyber espionage operations. The extent of the impact of supply chain attacks emerges as a substantial concern in relation to the upcoming EU parliamentary elections. This is because such attacks affected public administration by 21% and digital service providers by 16%.

DDoS attacks continue to be a persistent threat. They are the second most prevalent EU threat. DDoS attacks are getting larger and more complex, are moving towards mobile networks and IoT, and are used to provide support of additional means in the context of a conflict.

Phishing is once again the most common vector for initial access. But the new model, social engineering, is also emerging, an approach that consists of deceiving victims in the physical world.

OR

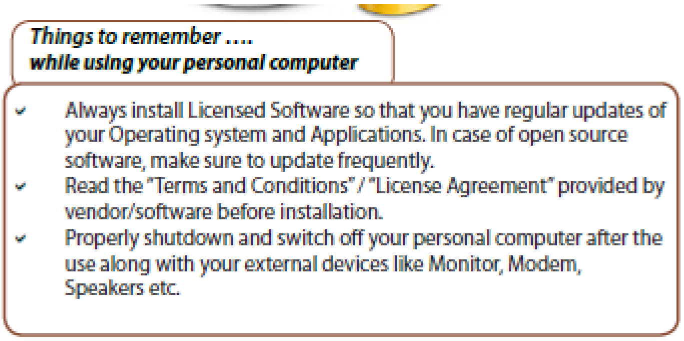
At the core of the ETL 2023 are eight principal threat categories that encapsulate the main challenges in cybersecurity:

1. **Ransomware**:**Description**: Attackers seize control of a target's assets, demanding ransom for their release. This threat remains significant, evidenced by numerous high-profile incidents.**Motivation**: Financial gain, disruption, ideological motives.
2. **Malware**:**Description**: Malicious software designed to perform unauthorized actions that compromise the confidentiality, integrity, or availability of a system.**Motivation**: Financial gain, espionage, sabotage.
3. **Social Engineering**:**Description**: Techniques that exploit human error to gain unauthorized access to information or services.**Motivation**: Identity theft, financial fraud, corporate espionage.
4. **Threats against Data**:**Description**: Incidents that lead to the unauthorized disclosure, alteration, loss, or destruction of personal data.**Motivation**: Financial gain, espionage, sabotage.

5. **Threats against Availability - Denial of Service (DoS)**:**Description**: Attacks that disrupt service access by overwhelming targets with excessive requests.**Motivation**: Financial extortion, competitive advantage, activism.
6. **Threats against Availability - Internet Threats**:**Description**: Disruptions that result in outages, affecting electronic communications.**Motivation**: State censorship, cyber warfare, criminal activities.
7. **Information Manipulation**:**Description**: Efforts to influence public opinion or political processes through deceptive practices.**Motivation**: Shaping public opinion, undermining democratic processes.
8. **Supply Chain Attacks**:**Description**: Attacks that target vulnerabilities in the supply chain to compromise multiple entities.**Motivation**: Unauthorized access to data, compromising critical infrastructure, espionage.

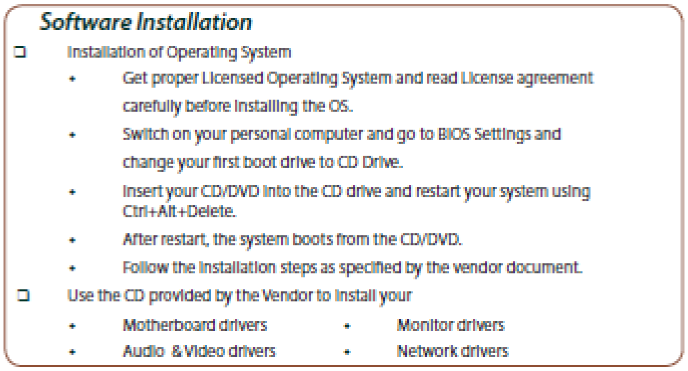
2. Visit the website www.csk.gov.in and outline some of the recommended best practices for securing personal computers.

ANS;



Things to remember ….
while using your personal computer

- ✓ Always install Licensed Software so that you have regular updates of your Operating system and Applications. In case of open source software, make sure to update frequently.
- ✓ Read the "Terms and Conditions" / "License Agreement" provided by vendor/software before installation.
- ✓ Properly shutdown and switch off your personal computer after the use along with your external devices like Monitor, Modem, Speakers etc.



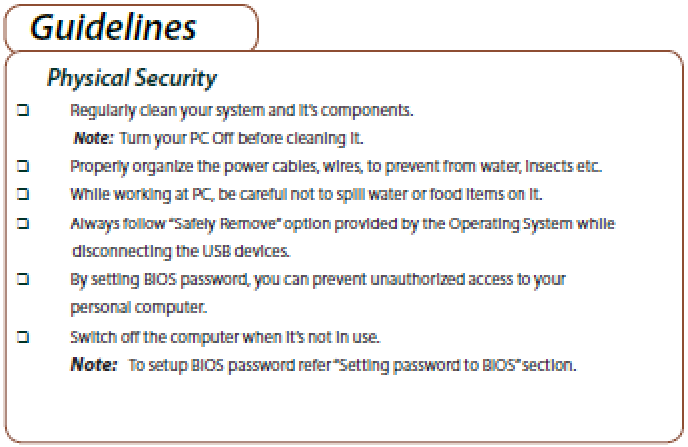
Software Installation

□ Installation of Operating System

- Get proper Licensed Operating System and read License agreement carefully before installing the OS.
- Switch on your personal computer and go to BIOS Settings and change your first boot drive to CD Drive.
- Insert your CD/DVD into the CD drive and restart your system using Ctrl+Alt+Delete.
- After restart, the system boots from the CD/DVD.
- Follow the installation steps as specified by the vendor document.

□ Use the CD provided by the Vendor to install your

- Motherboard drivers
- Audio & Video drivers
- Monitor drivers
- Network drivers



Guidelines

Physical Security

□ Regularly clean your system and it's components.
Note: Turn your PC Off before cleaning it.

□ Properly organize the power cables, wires, to prevent from water, insects etc.

□ While working at PC, be careful not to spill water or food items on it.

□ Always follow "Safely Remove" option provided by the Operating System while disconnecting the USB devices.

□ By setting BIOS password, you can prevent unauthorized access to your personal computer.

□ Switch off the computer when it's not in use.
Note: To setup BIOS password refer "Setting password to BIOS" section.

Internet Security:

❑ Follow Internet Ethics while browsing.

❑ Check the copyright issues before using the content of Internet.

❑ Always access the site which uses https (Hyper Text Transfer Protocol Secure) while performing Online transactions, Downloads etc, which is secure.

❑ If the site uses SSL, verify the Certificate details like Who is the owner, Expiry date of the certificate etc to confirm whether it is trusted or not.

You can do this by clicking the lock icon.

❑ Use only Original Websites for downloading the files rather than Third Party websites.

❑ Scan the downloaded files with an updated Anti-Virus Software before using it.

❑ Install and properly configure a Software firewall, to protect against mali-cious traffic.

Data Security

❑ Enable Auto-updates of your Operating System and update it regularly.

❑ Download Anti-Virus Software from a Trusted Website and install. Make sure it automatically gets updated with latest virus signatures.

❑ Download Anti-Spyware Software from a Trusted Website and install. Make sure it automatically updates with latest definitions.

❑ Use "Encryption" to secure your valuable information.

Note: *For encryption password is required, always remember the password used while encrypting it, else data would not be available thereafter.*

❑ Strong password should be used for "**Admin**" Account on computer and for other important applications like E-mail client, Financial Applications (accounting etc).

❑ **Backup :** Periodically backup your computer data on CD / DVD or USB drive etc.. In case it may get corrupted due to HardDisk failures or when reinstalling/format ting the system.

❑ **Recovery Disk:** Always keep recovery disk suplied by Manufacturer / Vendor of the Computer System to recover the Operating System in the event of boot failures due to system changes such as uncerificated Drivers/unknown Software publisher.

❑ Startup programs should be monitored / controlled for optimal system performance.

Browser Security:

❑ Always update your Web Browser with latest patches.

❑ Use privacy or security settings which are inbuilt in the browser.

❑ Also use content filtering software.

❑ Always have Safe Search "ON" in Search Engine.

e-Mail Security:

Always use strong password for your email account.

❑ Always use Anti-Spyware Software to scan the eMails for Spam.

❑ Always scan the e-Mail attachments with latest updated Anti-Virus and Anti-Spy ware before opening.

❑ Always remember to empty the Spam folder.

Wireless Security:

- ❑ Change default Administrator passwords.
- ❑ Turn On WPA (Wi-Fi Protected Access) / WEP Encryption.
- ❑ Change default SSID.
- ❑ Enable MAC address filtering.
- ❑ Turn off your wireless network when not in use.

Modem Security:

- ❑ Change the default passwords.
- ❑ Switch off when not in use.

Do's

Read the vendor document carefully and follow the guidelines to know how to setup the personal computer

- *Connect*
  - I. Keyboard
  - II. Mouse
  - III. Monitor
  - Iv. Speakers and
  - v. Network Cable …... to CPU (Central Processing Unit) as directed in vendor document.
- Connect CPU and Monitor to Electrical Outlets.

Dont's

- ❑ Do not install pirated software such as
  - Operating System Software (Windows, Unix, etc..).
  - Application Software (Office, Database..etc).
  - Security Software (Antivirus, Antispyware..etc).

Note: Remember, some Pirated Software themselve can be rogue programs.

- ❑ Do not plug the computer directly to the wall outlet as power surges may destroy computer. Instead use a genuine surge protector to plug a computer.
- ❑ Don't eat food or drink around the PC.
- ❑ Don't place any magnets near the PC.
- ❑ Never spray or squirt any liquid onto any computer component. If a spray is needed, spray the liquid onto a cloth and then use that cloth to rub down the component.
- ❑ Don't open the e-Mail attachments which have double extensions.

Setups

BIOS (Basic Input / Output System) Settings :

❑ Computers BIOS is the first program that runs when computer is started. You can tell the BIOS to ask for a password when it starts, thus restricting access to your computer.

+To enter the BIOS setup program, sometimes called CMOS setup:

❑ Turn on or reboot your computer. The screen will display a series of diagnostics and a memory check. A message will come "Hit the <DEL> key to enter the BIOS setup program" will appear. [It's not always the DEL key some BIOS's use F2 or F10 or any other key combination, check your motherboard manual for more details].

***Note:** Some BIOS versions use a graphical type menu with icons (a GUI) or have a text interface, the principle however is exactly the same.*

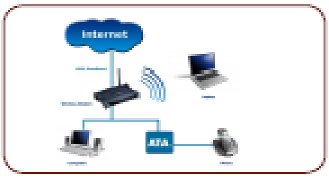
❑ There are two options that relate to passwords, Supervisor Password and User Pass word, these relate to controlling access to the BIOS Setup Program and the Machine Boot respectively.

***Note:** Not all BIOS's have this password feature, your bios may not have it in which case you won't be able to restrict access to your computer in this way.*

❑ Select USER PASSWORD and you'll be prompted to enter a password.You should now enter a password of up to eight characters (most BIOS's are limited to eight characters unfortunately). I recommend you to use the full eight but take care that you choose something you'll not forget. The BIOS will then prompt you to confirm the password, just type the same thing again. Now you'll want to set your system to ask for that password every time it boots, so select the BIOS FEATURES SETUP option, to see a menu. It's the Password Check option if you are interested in, so select it and change the setting to "ALWAYS". Now navigate back to the main menu and select SAVE & EXIT SETUP. Your machine will then reboot and you'll be prompted for the password. Each and everytime you boot you'll be asked for password you chose.

***Note:** This method of restricting access to your computer is not completely foolproof, there are ways around it. But it will stop or at least delay the majority of casual attempts to get access.*

***Note:** If you forget your BIOS password, consult your motherboard manual or if you don't have one, consult the website of the BIOS manufacturer.*



How to connect a Wireless Modem to a Desktop Computer....

Instructions to be followed while connecting the Wireless Modem

❑ Make sure you have the necessary equipment. Your wireless modem package should include the wireless modem (or wireless adapter); an installation CD-ROM with a manual; an Ethernet cable (or a USB cable if you have a wireless USB modem); a wireless antenna (conforming to wireless standards such as 802.11a, 802.11b, or 802.11g); and a power adapter. Call the retailer or the manufacturer of your wireless modem if any of these items are missing.

❑ Read the manual to learn how the equipment functions. For example, use the wireless antenna to connect to the wireless network ; use the Ethernet cable (or USB cable) to connect the computer to the modem.

❑ Attach your wireless antenna to the modem.

❑ Hook up an Ethernet cable from your computer to a LAN/Ethernet port on the modem. Or, if you have a wireless USB modem, connect the USB cable to the USB port of the computer.

❑ Connect the power adapter to the power connector of the modem, plug it in and switch it on.

Setting Up the Wireless Modem

□ Open your Web browser and enter the URL of the modem's administrative site. If you can't find it in the users' manual, call the modem manufacturer's/vendor's customer service.

□ Log in to the administrative site by entering the user name and password provided in the user manual. Again, if you cannot locate these, call the modem manufacturer's/vendor's customer service. Usually the default username and password is "**Admin**."

□ Select the Internet connection type. There are four types of Internet connection: "Dynamic IP Address," "Static IP Address," "PPPoE/PPPoA" and "Bridge Mode." Call your Internet service provider (ISP) to ask which setting best suits their wireless service.

□ Choose "Dynamic IP Address" to get an IP address automatically from the ISP's server. For every wireless Internet connection you make, you receive an IP address. In some cases the IP address is dynamic (it changes every time you connect to the Internet), and in other cases it is static (the IP address remains the same even after you disconnect and reconnect to the Internet). If the address is dynamic, you will have to choose this setting so that the modem automatically takes the IP from the ISP's server whenever a new wireless connection is established. Enter your modem's MAC Address (usually found at the back of the modem) and other details. Refer to the user manual or call the modem manufacturer's / vendor's customer service to get these details.

□ Select "Static IP Address" if you are provided with a static IP. You will need to fill in the fields for "VPI," "VCI," "IP Address," "Subnet Mask," "ISP Gateway Address," "Server Address," "Primary DNS Address," "Secondary DSN Address" and "Connection Type." These details can be otained from your ISP.

□ Opt for "PPPoE/PPPoA" if your ISP uses this type of connection. DSL users may use this connection. Enter your user name, password and other details. These will be provided by your ISP.

□ Select the "Bridge Mode" if your ISP uses this connection type. Enter the relevant details provided by your ISP.

□ Finish the process by clicking on the icon that says "Finish" or "OK" or something similar. Your modem should be set up now.

□ Enter any URL address in your browser's address window to check whether Internet is comming or not.

Source:

http://www.ehow.com/how_5006042_connect-modem-computer.html
http://www.ehow.com/how_2007332_install-wireless-modem.html