**FIELD: COMPUTER SCIENCE**

***▪ List significant cybersecurity vulnerabilities***

1**) Weak passwords**; Passwords access personal information stored in different accounts and your computer. If someone get access to this information, they can act as you in all your online activities.

**2) Insider threats;** This happen when someone close to an organization with authorized access misuse negatively impact the organization’s critical systems. This person can be a contractor, partner and third- party vendor not necessarily an employee.

**3) Missing data encryption;** Unencrypted data is highly vulnerable to several risk. That easily readable information may be exposed to hackers and this poses a high risk of data loss.

**4) Brocken algorithms;** For an end-user, a broken algorithm could mean an authorized to one’s account, leading to the theft of personal sensitive data.

**5) URL redirection;** Open Redirection Attacks takes advantage of web applications that fail to validate the input URL properly. Attackers manipulate data to redirect users to a malicious website than a trusted one.

**6) Unrestricted file uploads;** Unrestricted file uploads can lead to complete system takeover, an overloaded file system and client-side attacks depending on what that application does with the uploaded file where it is stored.

**7) Code downloads;** Unintentional download of malicious codes to your computer device may leave you open to a cyberattack. You don’t have to click on any untrusted link.

**8) Websites without SSL;** websites without SSL are at high risk of data loss. The site security is at high risk without encryption. SSL protects websites from phishing scams and data breaches.

**9) Computer viruses;** Some computer viruses are designed to harm your computer by damaging program, deleting files or reformatting the hard drive. Others simply replicates themselves flooding a network with traffic making it impossible to perform any network activity.

**10) Spyware;** Accepting a prompt or a pop-up without reading it may cause your device to become infected by spyware. Spyware can course operating system to crash, make the computer to overheat and disable internet security software which eventually courses permanent damage to the computer

**11) Phishing;** Phishing messages manipulate a user, causing them to perform actions like installing a malicious file. Phishing attacks uses text messages, email and phone calls to trick people into sharing sensitive data.

**12) Ransomware;** Ransomware can encrypt important files and render them useless. This can lead to a serious problem for business such as loss of confidential company information.

**13) Malware;** Malware programs access sensitive data and copy it. Some highly advanced malware automatically copy data and send it to the server that an attacker can then use to steal information. Sometimes this makes your connection to slow down. Malware can be invisible and have no unknown effects and run on your computer undetected if it’s well written.

**14) Fileless attacks;** A fileless attack triggers existing software to perform unauthorized activities. The attackers gain control of targets without relying on executable files.

**15) Man in the middle (MitM) attacks;** A cybercriminal secretly standing between the user and the system obtains a sensitive data. Without the user knowing interacts with untrustworthy site and relinquishes log in credentials and compromising data.

**16) Malicious apps;** Malicious apps exploit device vulnerabilities therefore allowing access to all resource permissions and also manipulating users into downloading malware that allows cybercriminal to access personal information.

**17) Denial of service attacks;** In these attacks, input sent takes advantage of bugs in the target that eventually destabilize the system rendering it functional.

**18) Zero-day exploits;** In a widely operating systems, data used by entire organization in the company can be left open for cybercrime until cybersecurity team identifies and releases a solution.

**19) Unpatched software;** Use of outdated software puts you at risk data loss because they may lack security patches making your system to be easily targeted by hackers.

**20) Application Misconfiguration;** Application misconfiguration can lead to security breaches hence exposing confidential information to attackers. As a result, the consequences can be severe.

**21) Wi-Fi vulnerability;** Using public Wi-Fi means everyone can easily access everything you do online. Your browsing history may be triggered.

**22) Firewalls;** When a cybersecurity solution that is supposed to protect your computer from unwanted traffic either coming in or going out is interrupted as a result of weak password, network resources may be configured.