Cyber Security: Types of threats

### 1.  Malware:

Short for “malicious software,” malware comes in several forms and can cause serious damage to a computer or corporate network. There are various forms of malware ranging from viruses and worms to Trojans and beyond. Malware is often seen as a catch-all term that refers to any software designed to cause damage to a computer, server, or network.

Antivirus software is the most known product to protect your personal devices against malware and is a great start to prevent potential threats. While for enterprises, protecting your endpoint is essential to quickly detect, prevent, and correct advanced threats to your business.

### 2. Computer Worm:

The distinctive trait of a worm is that it can self-replicate and doesn’t require human interaction to create copies and spread quickly and in great volume. Most worms are spread though tricking internet users and are designed to exploit known security holes in software. Since many employees use their phones for work-related tasks when they are not within the perimeter of their corporate firewall, businesses are at a high risk for potential worms. If a machine is infected, the worm can: corrupt files, steal sensitive data, install a backdoor giving cybercriminals access to your computer, or modify system settings to make your machine more vulnerable.

### 3. Spam:

Spam refers to unsolicited messages in your email inbox. From the sender’s perspective, spam is a great way to get their message across in an efficient and cost-effective way. While spam is usually considered harmless, some can include links that will install malicious software on your computer if the recipient clicks on it.

How do you recognize malicious spam? First off, if you don’t recognize the sender’s address, don’t open it. Also, if the email addresses you in a generic way, i.e. “Dear customer”, “Hi there” etc., don’t engage. Be aware of the embedded links and check if they have odd URL’s by hovering over them to see where it wants to direct you and if the destination URL matches the destination site you expect.

### 4. Phishing

Created by cybercriminals attempting to solicit private or sensitive information, phishing schemes tend to be the starting point of nearly all successful cyberattacks. Phishing schemes can disguise itself in many forms, whether its posing as your bank or a common web service, with the sole purpose to lure you in by clicking links and asking you to verify account details, personal information, or passwords. Many people still associate phishing threats with emails, but the threat has evolved beyond your inbox. Hackers are now employing text messages, phone calls, phony apps, and social media quizzes to trick an unwitting victim.

### 5. Botnet:

Botnet malware is a network of computers that have been hijacked or compromised, giving hackers the ability to control infected computers or mobile devices remotely. When the malware is launched on your computer or mobile device, it recruits your infected device into a botnet, and the hacker is now able to control your device and access all your data in the background without your knowledge.

A botnet can consist of as few as ten computers or hundreds of thousands, and when bots come together, they are a force to be reckoned with. If a botnet hits your corporate website, it can make millions of requests at once ultimately overloading the servers knocking the website offline, slow web traffic, or affect performance. As many businesses are aware, a website that is offline or has a long lag time can be very costly, resulting in a loss of customers or a damaged reputation.