**PROBLEM STATEMENT:**

**8.**Write an Article on cybersecurity and recent attacks which you came across in media and news and research on that news, and explain the any topic which you learned in this course and mention what you learned.

**SOLUTION:**

**What is Cyber Security?**

**Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing.**

**ARTICAL ON CYBER SECURITY:**

**From virtual bank heists to semi-open attacks from nation-states, the last couple of years has been rough on IT security. Here are some of the major recent cyber attacks and what we can learn from them.**

**Simply put, a cyber attack is an attack launched from one or more computers against another computer, multiple computers or networks. Cyber attacks can be broken down into two broad types: attacks where the goal is to disable the target computer or knock it offline, or attacks where the goal is to get access to the target computer's data and perhaps gain admin privileges on it.**

**8 types of cyber attack:**

**To achieve those goals of gaining access or disabling operations, a number of different technical methods are deployed by cybercriminals. There are always new methods proliferating, and some of these categories overlap, but these are the terms that you're most likely to hear discussed.**

**1. Malware**

**2. Phishing**

**3. Ransomware**

**4. Denial of service**

**5. Man in the middle**

**6. Cryptojacking**

**7. SQL injection**

**8. Zero-day exploits**

**Cyber attack prevention**

**Looking for tips on how to prevent falling prey to cyber attacks like these? CSO has you covered:**

**• How small businesses can fend off cyberattacks and data breaches**

**• If you do suffer a cyberattack, here are some tips for responding and working with law enforcement**

**• Point-of-sale terminals are a vector for malware and data theft — be sure yours are secure**

**• The government and businesses can work together to fight cyber attacks.**

## I AM LEARNING SO MUCH NEW THINGS IN THIS COURSE.SPECIAL ONE IS PHISHING ATTACK.WHY I AM CHOOSSING PHISHING ATTACK.THIS IS THE FIRST HACKING ATTACK IN MY LIFE.

## Phishing definition:

**Phishing is a cyber attack that uses disguised email ,facebook ,instagram as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need — a request from their bank, for instance, or a note from someone in their company .**

**What really distinguishes phishing is the form the message takes: the attackers masquerade as a trusted entity of some kind, often a real or plausibly real person, or a company the victim might do business with. It's one of the oldest types of cyberattacks, dating back to the 1990s, and it's still one of the most widespread and pernicious, with phishing messages and techniques becoming increasingly sophisticated**.

# 8 types of phishing attacks and how to identify them :

## 1.Phishing: Mass-market emails:-

The most common form of phishing is the general, mass-mailed type, where someone sends an email pretending to be someone else and tries to trick the recipient in doing something, usually logging into a website or downloading malware. Attacks frequently rely on email spoofing, where the email header—the from field—is forged to make the message appear as if it were sent by a trusted sender.

## 2. Spear phishing: Going after specific targets:-

Phishing attacks get their name from the notion that fraudsters are fishing for random victims by using spoofed or fraudulent email as bait. [Spear phishing](https://www.csoonline.com/article/3334617/what-is-spear-phishing-why-targeted-email-attacks-are-so-difficult-to-stop.html) attacks extend the fishing analogy as attackers are specifically targeting high-value victims and organizations. Instead of trying to get banking credentials for 1,000 consumers, the attacker may find it more lucrative to target a handful of businesses. A nation-state attacker may target an employee working for another government agency, or a government official, to steal state secrets.

Spear phishing attacks are extremely successful because the attackers spend a lot of time crafting information specific to the recipient, such as referencing a conference the recipient may have just attended or sending a malicious attachment where the filename references a topic the recipient is interested in.

## 3. Spear phishing: Going after specific targets:-

Phishing attacks get their name from the notion that fraudsters are fishing for random victims by using spoofed or fraudulent email as bait. [Spear phishing](https://www.csoonline.com/article/3334617/what-is-spear-phishing-why-targeted-email-attacks-are-so-difficult-to-stop.html) attacks extend the fishing analogy as attackers are specifically targeting high-value victims and organizations. Instead of trying to get banking credentials for 1,000 consumers, the attacker may find it more lucrative to target a handful of businesses. A nation-state attacker may target an employee working for another government agency, or a government official, to steal state secrets.

Spear phishing attacks are extremely successful because the attackers spend a lot of time crafting information specific to the recipient, such as referencing a conference the recipient may have just attended or sending a malicious attachment where the filename references a topic the recipient is interested in.

## 4. Business email compromise (BEC): Pretending to be the CEO:-

Aside from mass-distributed general phishing campaigns, criminals target key individuals in finance and accounting departments via [business email compromise (BEC)](https://www.csoonline.com/article/3441136/business-email-compromise-attacks-cost-millions-losses-doubling-each-year.html) scams and CEO email fraud. By impersonating financial officers and CEOs, these criminals attempt to trick victims into initiating money transfers into unauthorized accounts.

Typically, attackers compromise the email account of a senior executive or financial officer by exploiting an existing infection or via a spear phishing attack. The attacker lurks and monitors the executive’s email activity for a period of time to learn about processes and procedures within the company. The actual attack takes the form of a false email that looks like it has come from the compromised executive’s account being sent to someone who is a regular recipient. The email appears to be important and urgent, and it requests that the recipient send a wire transfer to an external or unfamiliar bank account. The money ultimately lands in the attacker’s bank account.

## 5.Clone phishing: When copies are just as effective:-

Clone phishing requires the attacker to create a nearly identical replica of a legitimate message to trick the victim into thinking it is real. The email is sent from an address resembling the legitimate sender, and the body of the message looks the same as a previous message. The only difference is that the attachment or the link in the message has been swapped out with a malicious one. The attacker may say something along the lines of having to resend the original, or an updated version, to explain why the victim was receiving the “same” message again.

## 6. Vishing: Phishing over the phone:-

Vishing stands for “voice phishing” and it entails the use of the phone. Typically, the victim receives a call with a voice message disguised as a communication from a financial institution. For instance, the message might ask the recipient to call a number and enter their account information or PIN for security or other official purposes. However, the phone number rings straight to the attacker via a voice-over-IP service.

## 7. Smishing: Phishing via text message:-

Smishing, a portmanteau of "phishing" and "SMS," the latter being the protocol used by most phone text messaging services, is a cyberattack that uses misleading text messages to deceive victims. The goal is to trick you into believing that a message has arrived from a trusted person or organization, and then convincing you to take action that gives the attacker exploitable information (like bank account login credentials, for example) or access to your mobile device.