CSC-370
E - Commerce
(BSc CSIT, TU)

Ganesh Khatri
kh6ganesh@gmail.com

Security Threats in E-commerce

- There's no doubt that the online retail market is booming.
- However, this success often attracts unwanted attention, and cyber-criminals have an ever-more sophisticated collection of methods to exploit gaps in online store security.
- As online stores become more advanced, it's important to keep up with the significant security risks that come with it.
- Let’s explore the different types of threats in eCommerce and best methods to avoid them.

Security Threats in E-commerce

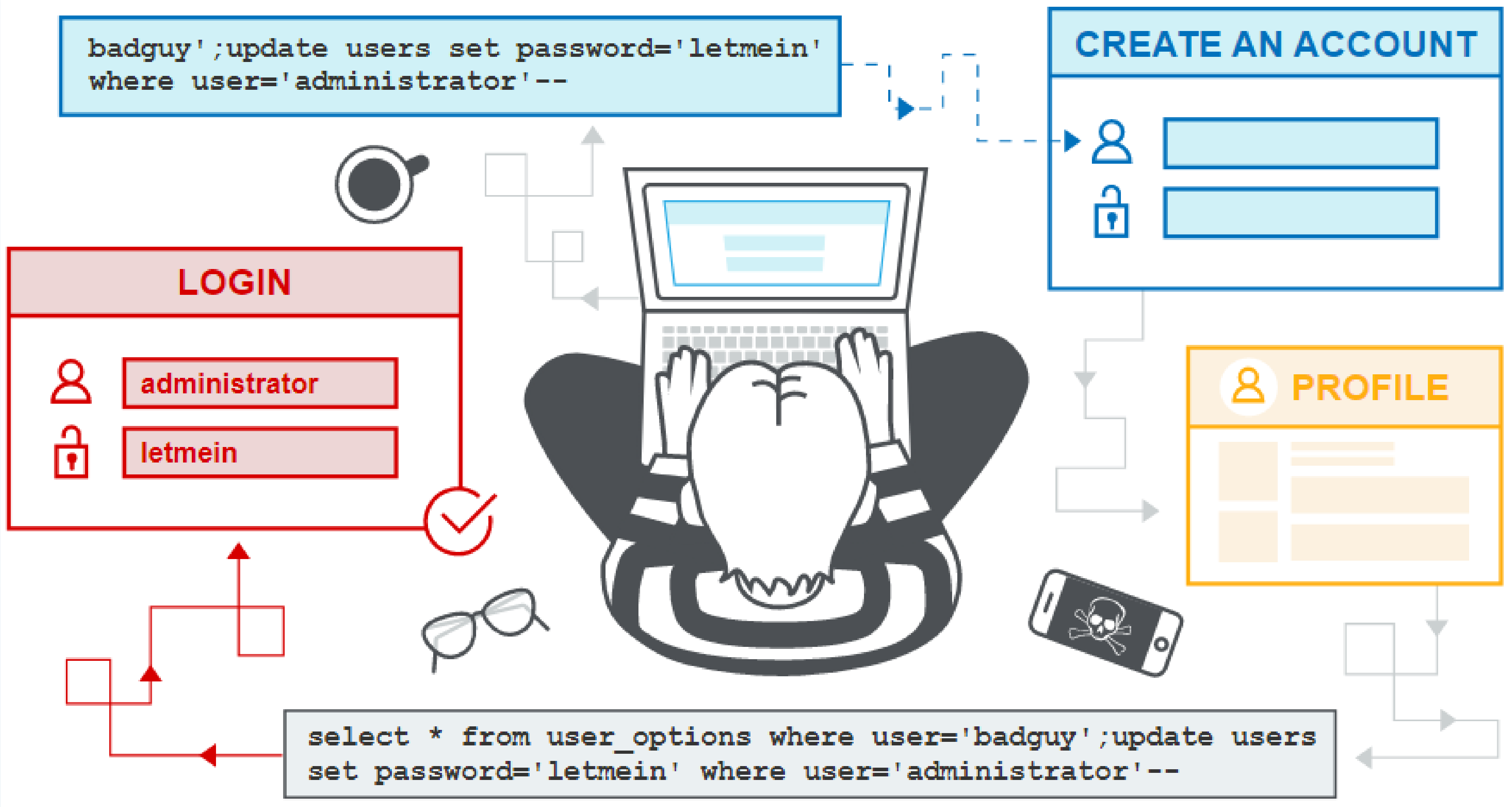
- Various security threats in eCommerce are :
  1. Vulnerabilities in eCommerce application
  2. Adware
  3. Spyware
  4. Social engineering
  5. Phishing
  6. Credit card fraud and Identity theft
  7. Spoofing and Pharming
  8. Client and Server Security
  9. Data Transaction Security

1. Vulnerabilities in eCommerce application

- These types of threats are due to different weaknesses or weak coding of applications. Different types of vulnerabilities are :
- **SQL Injection :**
  - SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database.
  - It generally allows an attacker to view data that they are not normally able to retrieve.
  - This might include data belonging to other users, or any other data that the application itself is able to access.
  - In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

1. Vulnerabilities in eCommerce application

- **SQL Injection :**



```
badguy';update users set password='letmein'
where user='administrator'--
```

```
select * from user_options where user='badguy';update users
set password='letmein' where user='administrator'--
```

1. Vulnerabilities in eCommerce application

- **SQL Injection :**
  - A successful SQL injection attack can result in unauthorized access to sensitive data, such as passwords, credit card details, or personal user information
  - The majority of SQL injection vulnerabilities can be found quickly and reliably using different web vulnerability scanners like Burp Suite.
  - SQL injection can be detected manually by using a systematic set of tests against every entry point in the application.
  - SQL Injection can be prevented by avoiding the quotes(‘ ’) from SQL queries. Normally it can be done using prepared statements.
  - Eg : $stmt = $pdo->prepare(“SQL query”);
  - There are various other techniques to avoid it depending upon different languages.
  - One more popular method is “Parse Tree Validation Method to avoid SQL Injection”

1. Vulnerabilities in eCommerce application

- **Buffer Overflows :**
  - Buffers are memory storage regions that temporarily hold data while it is being transferred from one location to another.
  - A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer.
  - As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations
  - Attackers exploit buffer overflow issues by overwriting the memory of an application.
  - This changes the execution path of the program, triggering a response that damages files or exposes private information.
  - For example, an attacker may introduce extra code, sending new instructions to the application to gain access to IT systems

1. Vulnerabilities in eCommerce application

- **Buffer Overflows :**
  - Developers can protect against buffer overflow vulnerabilities via security measures in their code, or by using languages that offer built-in protection
  - modern operating systems have runtime protections as well like data execution prevention, Address space randomization etc
  - Security measures in code and operating system protection are not enough.
  - When an organization discovers a buffer overflow vulnerability, it must react quickly to patch the affected software and make sure that users of the software can access the patch

1. Vulnerabilities in eCommerce application

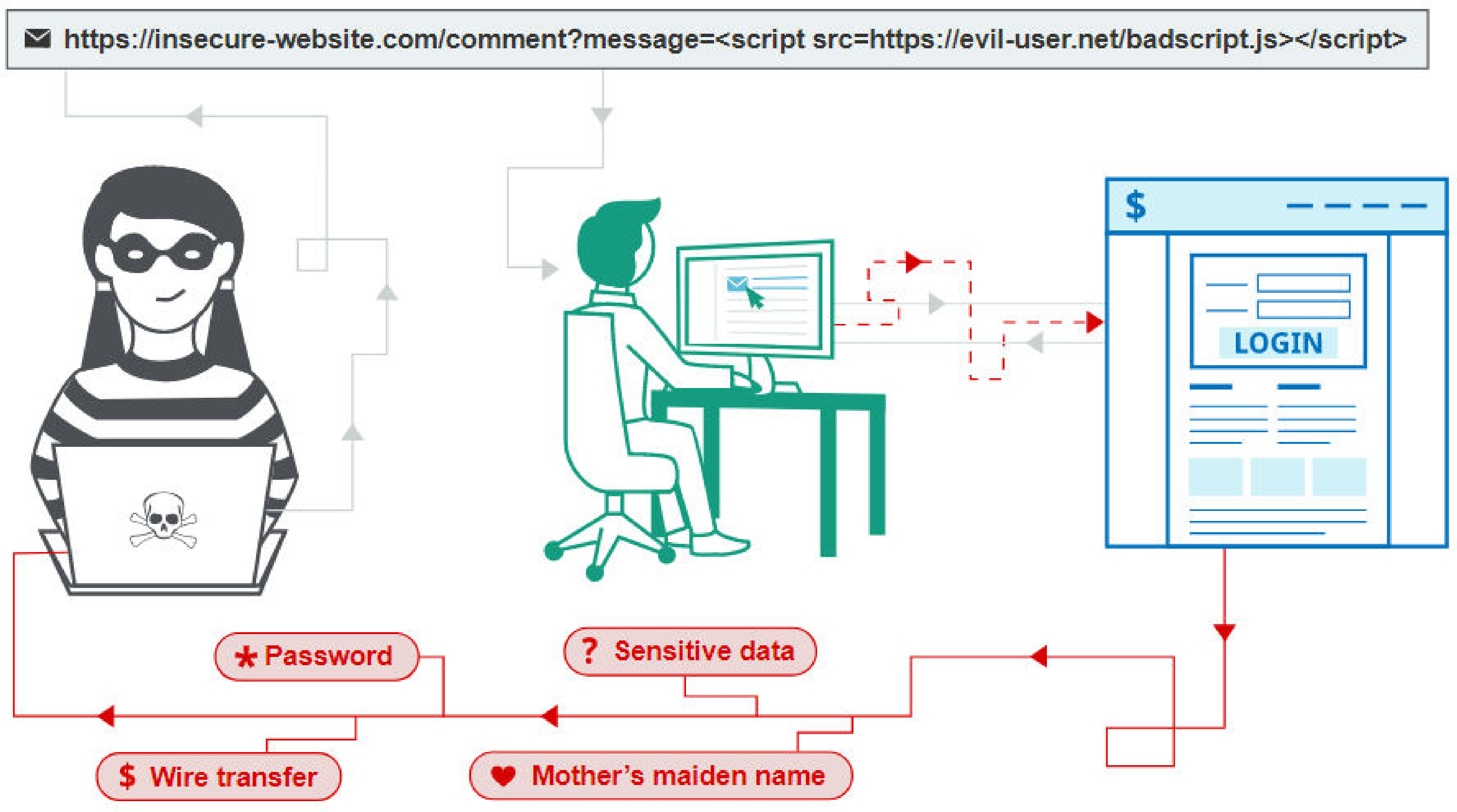
- **Remote Command Execution :**
  - Remote code execution is always performed by an automated tool. These attacks are typically written into an automated script
  - Remote arbitrary code execution is most often aimed at giving a remote user administrative access on a vulnerable system.
  - The attack is usually prefaced by an information gathering attack, in which the attacker uses some means such as an automated scanning tool to identify the vulnerable version of software.
  - Once identified, the attacker executes the script against the program with hopes of gaining local administrative access on the host
  - This is usually through the lack of proper input validation or verification.
  - For ecommerce platforms, this remains the most prevailing weakness that anyone can experience

1. Vulnerabilities in eCommerce application

- **Cross-site Scripting :**
  - Cross-site scripting (XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application.
  - It allows an attacker to circumvent the same origin policy, which is designed to separate different websites from each other
  - Cross-site scripting vulnerabilities normally allow an attacker to masquerade as a victim user, to carry out any actions that the user is able to perform, and to access any of the user's data.
  - If the victim user has privileged access within the application, then the attacker might be able to gain full control over all of the application's functionality and data.
  - Cross-site scripting works by manipulating a vulnerable web site so that it returns malicious JavaScript to users.
  - When the malicious code executes inside a victim's browser, the attacker can fully compromise their interaction with the application

1. Vulnerabilities in eCommerce application

- **Cross-site Scripting :**


https://insecure-website.com/comment?message=<script src=https://evil-user.net/badscript.js></script>
$
LOGIN
Password
Sensitive data
Wire transfer
Mother's maiden name

1. Vulnerabilities in eCommerce application

- **Cross-site Scripting :**
  - There are 3 types of XSS attacks.

1. Reflected XSS :

- is the simplest variety of cross-site scripting.
- It arises when an application receives data in an HTTP request and includes that data within the immediate response in an unsafe way.
- If your website has URL of type https://insecure-website.com/status?message=All+is+well then an attacker can easily construct an attack like this : https://insecure-website.com/status?message=<script>/* Bad Stuff */<script>
- If the user visits the URL constructed by the attacker, then the attacker's script executes in the user's browser, in the context of that user's session with the application.
- At that point, the script can carry out any action, and retrieve any data, to which the user has access.

1. Vulnerabilities in eCommerce application

- **Cross-site Scripting :**
  - There are 3 types of XSS attacks.

  2. Stored XSS :

  - Stored XSS (also known as persistent or second-order XSS) arises when an application receives data from an untrusted source and includes that data within its later HTTP responses in an unsafe way
  - Suppose a website allows users to submit comments on blog posts, which are displayed to other users.
  - Users submit comments using an HTTP request like the following

    http://vulnerable-website.com/postId=3&comment=This+post+was+extremely+helpful.&name=Carlos+Montoya&email=carlos%40normal-user.net
  - After this comment has been submitted, any user who visits the blog post will receive the following within the application's response
    <p>This post was extremely helpful.</p>

1. Vulnerabilities in eCommerce application

- **Cross-site Scripting :**
  - There are 3 types of XSS attacks.

2. **Stored XSS :**
   - Assuming the application doesn't perform any other processing of the data, an attacker can submit a malicious comment like this:
     `<script>/* Bad stuff here... */</script>`
   - Within the attacker's request, this comment would be URL-encoded as
     `comment=%3Cscript%3E%2F*%2BBad%2Bstuff%2Bhere...%2B*%2F%3C%2Fscript%3E`
   - Any user who visits the blog post will now receive the following within the application's response:
     `<p><script>/* Bad stuff here... */</script></p>`

1. Vulnerabilities in eCommerce application

- **Cross-site Scripting :**
  - There are 3 types of XSS attacks.

  2. DOM-based XSS :

  - DOM-based XSS arises when an application contains some client-side JavaScript that processes data from an untrusted source in an unsafe way, usually by writing the data back to the DOM

2. Adware

- Adware, often called advertising-supported software by its developers, is software that generates revenue for its developer by automatically generating online advertisements in the user interface of the software or on a screen presented to the user.
- Some security professionals view it as the forerunner of the modern-day PUP (potentially unwanted program).
- Typically, it uses a method to either disguise itself as legitimate, or piggyback on another program to trick you into installing it on your PC, tablet, or mobile device

3. Spyware

- Spyware is a type of malicious software or malware that is installed on a computing device without the end user's knowledge.
- It invades the device, steals sensitive information and internet usage data, and relays it to advertisers, data firms or external users.
- Any software can be classified as spyware if it is downloaded without the user's authorization.
- Spyware is controversial because, even when it is installed for relatively innocuous reasons, it can violate the end user's privacy and has the potential to be abused
- Spyware is one of the most common threats to internet users.
- Once installed, it monitors internet activity, tracks login credentials and spies on sensitive information.
- The primary goal of spyware is usually to obtain credit card numbers, banking information and passwords.

3. Spyware : How to prevent?

- Maintaining strict cybersecurity practices is the best way to prevent spyware. Some best practices include the following
  - only downloading software from trusted sources
  - reading all disclosures when installing software
  - avoiding interaction with pop-up ads
  - staying current with updates and patches for browser, OS and application software

4. Social engineering

- Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables.
- In cybercrime, these “human hacking” scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems.
- Attacks can happen online, in-person, and via other interactions
- Scams based on social engineering are built around how people think and act. As such, social engineering attacks are especially useful for manipulating a user’s behavior.
- Once an attacker understands what motivates a user’s actions, they can deceive and manipulate the user effectively.
- Social engineering attacks rely on actual communication between attackers and victims. The attacker tends to motivate the user into compromising themselves, rather than using brute force methods to breach your data

4. Social engineering : How does it work?

- The attack cycle gives these criminals a reliable process for deceiving you. Steps for the social engineering attack cycle are usually as follows :
  - **Prepare :** by gathering background information on you or a larger group you are a part of
  - **Infiltrate :** by establishing a relationship or initiating an interaction, started by building trust.
  - **Exploit the victim :** once trust and a weakness are established to advance the attack
  - **Disengage :** once the user has taken the desired action
- This process can take place in a single email or over months in a series of social media chats.
- It could even be a face-to-face interaction but it ultimately concludes with an action you take, like sharing your information or exposing yourself to malware

5. Phishing

- Phishing is a kind of social engineering attack.
- Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords
- The information is then used to access important accounts and can result in identity theft and financial loss

5. Phishing : Common Features of Phishing Emails

- **Too Good To Be True :**
  - Attractive offers and eye-catching or attention-grabbing statements are designed to attract people's attention immediately. For instance, many claim that you have won an iPhone, a lottery, or some other lavish prize. Just don't click on any suspicious emails. Remember that if it seems to good to be true
- **Sense of Urgency :** -
  - A favorite tactic amongst cybercriminals is to ask you to act fast because the super deals are only for a limited time. Some of them will even tell you that you have only a few minutes to respond. When you come across these kinds of emails, it's best to just
- **Hyperlinks :** -
  - A link may not be all it appears to be. Hovering over a link shows you the actual URL where you will be directed upon clicking on it. It could be completely different or it could be a popular website with a misspelling.

5. Phishing : Common Features of Phishing Emails

- **Attachments :**
  - If you see an attachment in an email you weren't expecting or that doesn't make sense, don't open it! They often contain payloads like ransomware or other viruses. The only file type that is always safe to click on is a .txt file.
- **Unusual Sender :** Whether it looks like it's from someone you don't know or someone you do know, if anything seems out of the ordinary, unexpected, out of character or just suspicious in general don't click on it!

6. Credit card fraud and Identity theft

- **Credit card fraud** :
  - is a potential consequence of identity theft.
  - Here, a thief steals your credit card information and then makes purchases in a store or online.
  - Suppose, most credit card companies have a liability limit of $50.
  - This means that even if a thief has charged thousands of dollars to your card, you'd likely only have to pay $50.
  - More often than not, credit card companies simply wipe out any charges that are the result of fraud
- **identity theft :**
  - involves much more than a few fraudulent charges.
  - Identity thieves can steal your personal information to open a new line of credit, open a new credit card, or obtain a false ID in your name.
  - Unlike credit card fraud, there's no liability limit. That means you might end up paying for all the damage caused by an identity thief.

7. Spoofing and Pharming

- **Spoofing**
  - describes a criminal who impersonates another individual or organization, with the intent to gather personal or business information
- **Pharming**
  - is a malicious website that resembles a legitimate website, used to gather usernames and passwords
  - pharming is a advance technique to get users credentials by making effort to entering users into the website
  - In order words, it misdirects users to a fake website that appears to be official and victims gives their personal information by fault.
  - In pharming, fake website is created which appears to be official. Users then access the website and request is popped up regarding username and password and other credentials
- **Note :** Differences between Phishing and Farming : https://www.geeksforgeeks.org/difference-between-phishing-and-pharming