TASK -11

Phishing:

Phishing is a concept of acquiring or stealing a credential information or data from a victim or third party to monetize that information in a illegal way.

The most common examples of phishing are used to support other malicious actions, such as account takeovers, ransomware attack, or business email compromise. Via email, text messages, phone calls and QR code.

Trick users into:

- Clicking malicious links
- Entering credentials
- Downloading malware

Security privacy

Respected sir/mam,
As per the new guidelines of our company we are decided to allot new password and username for all employees of our company.

We reset all the passwords of all the department employees.

click the link below, urgent allotting new password only open for 15 min due to company credentials.

If you are not claiming the password, your user account will be held for 1 week. so click the link below.
www.https://abccompany.in.

Form the security team.

A sample phishing email was created to simulate common social engineering techniques such as urgency, threats, and suspicious links. The email was analyzed to identify phishing red flags, including generic greetings, grammar errors, and misleading URLs. This activity helped in understanding how phishing attacks manipulate users and how they can be detected and prevented.

Analyzing my mail:

Urgency	“Only 15 minutes”
Threat	“Account will be held”
Greeting	Generic (sir/mam)
Link	Invalid / suspicious
Grammar	Errors present

How to find the a phishing email:

Domain name, if a company sending a email it must in their company domain name. like @abc.com.

If it is using a public domain like @goolge.com it is consider as phsing.

And If observer the keywords to manuplate the victims.

Do not click the link or open the file which is attached with the email.

Prevention techniques

- User awareness
- MFA
- Email filtering
- Never clicking unknown links