# Assignment No. 03

| | |
|---|---|
| Semester | B.E. Semester VII – Computer Engineering |
| Subject | Cybersecurity and Laws |
| Academic Year | 2024-25 |

| | |
|---|---|
| Student Name | Deep Salunkhe |
| Roll Number | 21102A0014 |
| Branch | BE-CMPN A |

**Scenario 1:**

**You receive an email that appears to be from your bank. The email states that there has been suspicious activity on your account and asks you to click on a link to verify your identity.**

**Q.1.1 How can you determine if the email is legitimate or a phishing attempt?**

To determine if the email is legitimate or a phishing attempt, consider the following:

- **Check the sender's email address:** Phishing emails often use addresses that are similar to the legitimate one but with slight variations (e.g., a different domain or added characters).
- **Look for generic greetings:** Phishing emails often use generic salutations like "Dear Customer" instead of your actual name.
- **Examine the content for urgency or threats:** Phishing emails often create a sense of urgency, such as claiming your account will be suspended if you don't act immediately.
- **Hover over links without clicking:** This reveals the actual URL. If it doesn't match the bank's official website or looks suspicious, it's likely phishing.
- **Look for spelling and grammar mistakes:** Legitimate companies usually have well-written communications, while phishing emails often contain errors.

- **Verify with your bank directly:** Contact your bank using a known and trusted method (like their official website or customer service number) to confirm if the email is legitimate.

**Q.1.2 What are some red flags to look for in the email that might indicate it's a phishing scam?**

- **Suspicious sender address:** Email from a domain that doesn't match the official one.
- **Unexpected requests for sensitive information:** Banks usually don’t ask for sensitive information via email.
- **Urgency and threats:** Messages claiming immediate action is needed to prevent negative consequences.
- **Poor language:** Spelling errors, grammatical mistakes, and awkward phrasing.
- **Unusual attachments or links:** Attachments you weren’t expecting or links that lead to suspicious URLs.
- **Generic greetings:** Use of phrases like “Dear Customer” instead of your name.

**Q.1.3 What should you do if you suspect that the email is a phishing attempt?**

- **Do not click on any links or download attachments:** These could be malicious.
- **Report the email to your bank:** Use their official communication channels.
- **Mark the email as spam:** This helps filter similar messages in the future.
- **Delete the email:** Safely remove it from your inbox.

**Q.1.4 How can individuals protect themselves from falling victim to phishing attacks in general?**

- **Be cautious with emails and messages:** Don’t trust unsolicited emails that ask for personal information.
- **Enable multi-factor authentication (MFA):** This adds an extra layer of security to your accounts.
- **Keep software up to date:** Ensure your operating system, browser, and antivirus software are up to date to protect against the latest threats.
- **Educate yourself and others:** Stay informed about phishing techniques and spread awareness.
- **Use anti-phishing tools:** Many email providers offer filters and tools to detect phishing attempts.

**Q.1.5 What actions should you take if you accidentally clicked on a phishing link and entered sensitive information?**

- **Change your passwords immediately:** Start with the account you believe was compromised, then others that use the same password.
- **Notify your bank or the relevant institution:** They can monitor for suspicious activity and help secure your account.
- **Monitor your accounts:** Keep an eye on your bank and credit card statements for any unauthorized transactions.
- **Report the phishing attempt:** Inform your email provider, bank, or other relevant authorities.
- **Consider a credit freeze:** If you shared financial information, a credit freeze can prevent identity theft.

**Scenario 2:**

**A major technology company, known for its cloud storage services, experiences a massive data breach. The breach affects millions of users, including individuals, businesses, and government agencies. The stolen data includes sensitive personal information, financial records, and proprietary business data.**

**Q.2.1 What immediate steps should the affected technology company take to respond to the data breach?**

- **Contain the breach:** Identify and close any vulnerabilities to prevent further data loss.
- **Assess the scope of the breach:** Determine what data was compromised and how many users were affected.
- **Notify affected parties:** Quickly inform users, regulatory bodies, and stakeholders about the breach.
- **Engage cybersecurity experts:** Bring in experts to assist with the investigation and strengthen security.
- **Provide support to affected users:** Offer resources like credit monitoring, identity theft protection, and dedicated customer support.

**Q.2.2 How can the affected users (individuals, businesses, and government agencies) protect themselves in the aftermath of the breach?**

- **Change passwords:** Immediately update passwords, especially for any accounts associated with the breached service.
- **Monitor accounts:** Regularly check bank, credit card, and other accounts for suspicious activity.
- **Enable MFA:** Add an extra layer of security to accounts to reduce the risk of unauthorized access.
- **Use identity theft protection services:** These can help detect and respond to potential fraud.
- **Be cautious of phishing scams:** Be extra vigilant, as attackers may use the breached information to target users with phishing attempts.

**Q.2.3 What legal and ethical responsibilities does the technology company have regarding the data breach and the compromised data?**

- **Compliance with data protection laws:** The company must follow laws such as GDPR, CCPA, or other relevant regulations, which may include notifying affected individuals and authorities within a specific timeframe.
- **Transparency:** The company has an ethical obligation to fully disclose the breach details, including what data was compromised and how it occurred.
- **Provide assistance to affected users:** The company should offer services like credit monitoring or identity theft protection, especially if sensitive data was compromised.
- **Take corrective action:** Implement stronger security measures to prevent future breaches and learn from the incident.
- **Legal recourse:** The company may face lawsuits from affected users, requiring it to compensate for damages caused by the breach.