Jeric Punay
BSIT 4B SMP

Facebook Phishing Attack

A phishing attack also happened in Facebook, fake login pages are created by the cybercriminals and they send fake messages that look like Facebook to trick users into giving account credentials. Emails, messenger, and fake notifications are usually the ways that attackers use to hook their victims by clicking on malicious links. When the login details are given to the attackers, they will have the power to do identity theft, use the infected device to infect other devices, or do more social engineering attacks.

Step-by-Step Initial Response Procedure:

1. Detection/Identification:
   - Users report suspicious messages, friend requests, or emails claiming to be from Facebook and monitor system alerts for unusual login attempts.
   - Check for unusual activity on accounts, such as posts not made by the user or messages sent automatically.
2. Containment:
   - Immediately instruct affected users to change their Facebook passwords and enable two-factor authentication.
   - Block the phishing link or email at the organization's firewall or email gateway.
   - Temporarily disable compromised accounts until verified secure.
3. Notification:
   - Inform IT security team for incident response.
   - Notify management of potential data compromise.
   - Alert users within the organization about the phishing attempt and advise them not to click suspicious links.
4. Initial Remediation:
   - Remove the phishing messages or posts from affected accounts.
   - Scan affected devices for malware or keyloggers.
   - Advise users to log out of all active Facebook sessions and verify account settings.
5. Policy/Compliance Check:
   - Follow the organization's cybersecurity incident response policy.
   - Ensure compliance with data protection regulations regarding compromised user information (GDPR).
6. Documentation:
   - Record the phishing attempt details: source, method of attack, affected users, and actions taken.
   - Maintain logs of communications, containment steps, and remediation efforts for future reference.
7. Future Prevention:
   - Conduct user awareness training on recognizing phishing attempts.
   - Implement email and messaging filters to block suspicious links.
   - Enforce strong password policies and two-factor authentication for all users.