Lecture 2: Cyber Crime and Mitigation

- Types of Cyber Crime

1. Phishing

- **Modus Operandi**:
  Fraudulent emails or messages impersonate trusted entities to trick victims into revealing sensitive information like login credentials or financial data.
- **Impact**:
  - Loss of personal or financial data.
  - Unauthorized access to systems or accounts.
- **Severity Level**:
  Medium to High (depends on scale and sensitivity of stolen data).
- **Affected Cybersecurity Principles**:
  - **Confidentiality**: Sensitive information is exposed.
  - **Integrity**: Alteration of systems using obtained credentials.

---

2. Ransomware

- **Modus Operandi**:
  Malware encrypts the victim's data, demanding ransom for decryption. Often spreads through malicious links or software.
- **Impact**:
  - Data unavailability.
  - Financial loss due to ransom payments.
  - Disruption of operations.
- **Severity Level**:
  High (especially for businesses or critical infrastructure).
- **Affected Cybersecurity Principles**:
  - **Availability**: Data or systems become inaccessible.
  - **Integrity**: Threat of deleting or altering data.

---

3. Distributed Denial of Service (DDoS) Attacks

- **Modus Operandi**:
  Overwhelms a server or network with excessive traffic, making it unavailable to legitimate users.
- **Impact**:
  - Service outages.
  - Financial losses from downtime.
  - Reputation damage.
- **Severity Level**:
  Medium to High (depends on the target).
- **Affected Cybersecurity Principles**:
  - **Availability**: Disrupts legitimate access to services.

---

4. Identity Theft

- **Modus Operandi**:
  Cybercriminals steal personal data (e.g., Social Security numbers, credit card details) and impersonate victims for fraudulent activities.
- **Impact**:
  - Financial losses.
  - Damage to victim's credit reputation.
  - Legal complications.
- **Severity Level**:
  High.
- **Affected Cybersecurity Principles**:
  - **Confidentiality**: Exposure of personal data.
  - **Integrity**: False transactions or data entries.

---

5. Insider Threats

- **Modus Operandi**:
  Malicious or negligent employees misuse their access to steal data, sabotage systems, or leak confidential information.
- **Impact**:

    - Data breaches.
    - Loss of intellectual property.
    - Operational disruption.
- **Severity Level**:
  High.
- **Affected Cybersecurity Principles**:
    - **Confidentiality**: Exposure of sensitive information.
    - **Integrity**: Internal systems tampered with.
    - **Availability**: Potential downtime.

---

6. Social Engineering

- **Modus Operandi**:
  Manipulates individuals into divulging confidential information by exploiting human psychology. Common methods include pretexting, baiting, and tailgating.
- **Impact**:
    - Unauthorized access.
    - Data breaches.
    - Fraudulent activities.
- **Severity Level**:
  Medium to High.
- **Affected Cybersecurity Principles**:
    - **Confidentiality**: Information disclosed to unauthorized persons.

---

7. Malware Attacks

- **Modus Operandi**:
  Malicious software (e.g., viruses, worms, Trojans) infiltrates and damages systems or steals data.
- **Impact**:
    - System corruption or failure.
    - Data breaches.
    - Financial loss.

- **Severity Level**:
  High.
- **Affected Cybersecurity Principles**:
  - **Confidentiality**: Data exposure.
  - **Integrity**: System or data manipulation.
  - **Availability**: System failure or unavailability.

---

8. Cyber Espionage

- **Modus Operandi**:
  State-sponsored or corporate actors use advanced techniques to gather sensitive information from governments or organizations.
- **Impact**:
  - Loss of national security data.
  - Competitive disadvantage.
- **Severity Level**:
  Critical.
- **Affected Cybersecurity Principles**:
  - **Confidentiality**: Stealing classified information.

---

9. Financial Fraud (e.g., Carding, Wire Fraud)

- **Modus Operandi**:
  Steals financial credentials via malware, phishing, or data breaches and uses them for unauthorized transactions.
- **Impact**:
  - Financial loss.
  - Reputation damage.
  - Customer distrust.
- **Severity Level**:
  High.
- **Affected Cybersecurity Principles**:
  - **Confidentiality**: Exposure of financial data.

- **Integrity**: Manipulation of financial transactions.

---

10. Cryptojacking

- **Modus Operandi**:
  Malware infects devices to mine cryptocurrency using victim's computing resources.
- **Impact**:
  - Degraded system performance.
  - Increased operational costs.
- **Severity Level**:
  Medium.
- **Affected Cybersecurity Principles**:
  - **Availability**: Reduced system efficiency.

Phishing: Detailed Examples, Mitigation Strategies, and Case Studies

---

Detailed Examples of Phishing

1. **Email-Based Phishing**:
   - **Scenario**: A user receives an email claiming to be from their bank. The email urges them to update their account information via a provided link, which redirects them to a fake bank website. Upon entering credentials, the attacker captures the login details.
   - **Example**: In 2021, a phishing attack targeted Office 365 users, using fake emails with subject lines like "Action Required: Unusual Login Attempt." It tricked users into entering their credentials on a fake Office 365 login page.
2. **Spear Phishing**:
   - **Scenario**: A cybercriminal targets a specific individual, such as a company executive. The attacker researches the victim's organization and sends a personalized email with a malicious attachment disguised as a business proposal.
   - **Example**: In 2020, hackers sent spear-phishing emails to several executives at large companies, pretending to be suppliers affected by COVID-19 and requesting payments or sensitive details.
3. **Smishing (SMS Phishing)**:

- **Scenario**: An attacker sends an SMS pretending to be from a courier service, urging the recipient to click on a link to track their package. The link installs malware or leads to a fake login page.
- **Example**: In 2022, a smishing campaign impersonated DHL, leading victims to malware that stole their banking credentials.

4. **Vishing (Voice Phishing)**:
    - **Scenario**: A victim receives a phone call from someone claiming to be from the IRS, threatening legal action unless the victim shares sensitive information or pays immediately.
    - **Example**: The "Tech Support Scam" involved attackers calling users to fix non-existent computer issues for a fee, stealing payment details during the process.

Mitigation Strategies

1. For Individuals:

- **Awareness and Education**:
    - Be cautious of unsolicited emails or messages.
    - Verify the sender's authenticity by contacting the organization directly using official channels.
    - Avoid clicking on links or downloading attachments from unknown sources.
- **Password Hygiene**:
    - Use strong, unique passwords for each account.
    - Enable two-factor authentication (2FA) to secure accounts further.
- **Inspect Links**:
    - Hover over links to check the URL before clicking.
    - Look for HTTPS in the URL, though this alone is not foolproof.
- **Update Software**:
    - Keep browsers, operating systems, and antivirus software updated to protect against malware.

---

2. For Organizations:

- **Phishing Simulations**:

    - Conduct regular phishing training and simulations to educate employees about recognizing threats.

- **Email Security Solutions**:
    - Use advanced email filtering tools to detect and block phishing emails.
    - Implement Domain-based Message Authentication, Reporting, and Conformance (DMARC) to prevent spoofing.
- **Incident Response Plan**:
    - Create a protocol for employees to report

phishing attempts. Ensure there's a team ready to respond quickly to such incidents.

- **Network Segmentation**:
    - Limit access to sensitive data. Even if phishing succeeds, attackers won't gain unrestricted access to critical systems.
- **Endpoint Security**:
    - Deploy anti-malware and endpoint protection tools to detect malicious activities resulting from phishing attempts.

Case Studies on Phishing

Case Study 1: Targeted Phishing at Ubiquiti Networks (2021)

- **Incident**:
  Ubiquiti Networks, a major networking equipment manufacturer, was targeted in a phishing attack. Hackers gained unauthorized access to internal systems, including customer data stored on cloud-based services. The attackers used stolen credentials obtained through phishing.
- **Impact**:
    - Compromise of sensitive customer data.
    - Damage to the company's reputation.
    - Significant financial costs for investigation and mitigation.
- **Mitigation**:
  Ubiquiti implemented stronger security measures, including mandating 2FA for employee accounts, and enhanced their monitoring systems.

Case Study 2: The Google and Facebook Scam (2013-2015)

- **Incident**:
  A Lithuanian hacker impersonated a vendor and sent fake invoices to Google and Facebook employees. By using phishing emails that appeared legitimate, the attacker convinced employees to wire over $100 million to fraudulent accounts.
- **Impact**:
  - Loss of $100 million (though much of it was later recovered).
  - Highlighted vulnerabilities in vendor payment processes.
- **Mitigation**:
  - Both companies strengthened their vendor verification processes.
  - They implemented stricter controls for financial transactions, such as requiring multiple levels of approval.

Case Study 3: The RSA Data Breach (2011)

- **Incident**:
  Employees at RSA Security received a phishing email with the subject "2011 Recruitment Plan." The email contained a malicious Excel attachment with an exploit. Once opened, it allowed attackers to install malware and gain access to sensitive systems, including RSA's SecureID authentication technology.
- **Impact**:
  - RSA's SecureID technology was compromised, affecting major clients like defense contractors.
  - Financial losses estimated at $66 million for remediation and reputation damage.
- **Mitigation**:
  RSA upgraded its security infrastructure, focusing on endpoint monitoring and incident response. The breach also drove widespread industry adoption of advanced email filtering technologies.
