Task 2 Solutions workshop

Daniel Felipe, Pau Gazapo y Daniel Cebriano.

Problem 01: Phishing Scams

The Case

You receive an email claiming to be from your bank, asking you to click a link and "verify your account details." The link leads to a fake website that steals your credentials.

The Solution

Never click on links in unsolicited emails. Always verify the sender's address and contact the bank directly through their official app or website.

Problem 02: Weak Credentials

The Case

An employee uses "123456" as their email password. A hacker guesses it easily and accesses sensitive work emails.

The Solution

Use strong, complex passwords that include a mix of letters, numbers, and symbols. Avoid reusing passwords across different accounts.

Problem 03: Malware Infection

The Case

You download a free music file from an untrusted website, and it installs malware that locks your files until you pay a ransom.

The Solution

Only download files from reputable and official sources. Install and keep an antivirus program updated to scan downloads automatically.

Problem 04: Ransomware

The Case

A company employee opens an attachment in a suspicious email, triggering ransomware that encrypts all company files. The hacker demands $5,000 to unlock them.

The Solution

Do not open attachments from unknown senders. Maintain regular offline backups of all important data so files can be restored without paying the ransom.

Problem 05: IT Support Scam

The Case

A scammer calls pretending to be "IT support" and convinces an employee to share their login credentials.

The Solution

Verify the identity of the caller. Remember that legitimate IT support will never ask for your password over the phone.

Problem 06: Public Wi-Fi Risks

The Case

You connect to free Wi-Fi at a coffee shop. A hacker intercepts your unencrypted browsing traffic and steals your credit card details.

The Solution

Avoid accessing banking or sensitive sites on public Wi-Fi. If necessary, use a Virtual Private Network (VPN) to encrypt your connection.

Problem 07: Data Breaches

The Case

A retail company’s database is hacked, leaking thousands of customer emails and payment details.

The Solution

Companies must use strong encryption for stored data and perform regular security audits. Customers should change their passwords immediately if a service they use is breached.

Problem 08: Session Hijacking

The Case

While accessing your bank account over public Wi-Fi, a hacker intercepts your session and monitors all your transactions.

The Solution

Ensure the website uses HTTPS (look for the padlock icon). Use a VPN or your mobile data network instead of public Wi-Fi for financial transactions.

Problem 09: Outdated Software

The Case

A user ignores updates on their operating system. Hackers exploit an old vulnerability to take control of the device.

The Solution

Enable automatic software updates for your operating system and applications to patch security vulnerabilities as soon as they are fixed.

Problem 10: Social Media Risks

The Case

Your social media profile is hacked, and the attacker uses your personal information to open fake credit card accounts.

The Solution

Limit the amount of personal information you share publicly on social media. Use strong privacy settings and unique passwords for your accounts.

Problem 11: HTTP vs HTTPS

The Case

You purchase items from an HTTP website. Hackers intercept your credit card details during the transaction.

The Solution

Never enter credit card information on a website that does not use HTTPS. Look for the secure padlock icon in the browser address bar.

Problem 12: Spyware

The Case

You download a pirated software version, and it secretly installs spyware that tracks your keystrokes.

The Solution

Avoid pirated software and cracked versions. Purchase legitimate software from official developers to ensure it is free of malicious code.

Problem 13: App Permissions

The Case

A mobile game requests access to your microphone, camera, and contacts, potentially spying on you.

The Solution

Review app permissions carefully before installing. Deny access to features that are not necessary for the app's functionality. example: calculator does not need your contacts).

Problem 14: Insider Threats

The Case

A disgruntled employee leaks confidential company data to competitors.

The Solution

Implement the principle of "least privilege," ensuring employees only have access to the data necessary for their specific job. Revoke access immediately when an employee leaves.

Problem 15: Lack of 2FA

The Case

Your email account is hacked because you didn't enable 2FA. The attacker gains access to linked services like social media and cloud storage.

The Solution

Enable Two-Factor Authentication (2FA) on all your accounts. This adds a second layer of security, requiring a code from your phone in addition to your password.