**RESTART: Resilience and Training for SMEs**

**Case study**

**(Project Result 3 - Task 3.1. & Task 3.2)**

|  |  |
| --- | --- |
| **Author of the case study:** | Internet Web Solutions |
| **Name of the module to which the case study is assigned:** | Module 3: Cybersecurity in the (home) office |
| **Title of the case study:** | Phishing + SMS: the risks of smishing |
| **Description of the case study:** | As you already know from the module "Cybersecurity in the (home) office", phishing is the most common attack on European MSMEs, and these can vary depending on the method used for the attack. In this case study we focus on smishing, the technique of phishing via SMS.  This case study has been extracted from the National Institute of Cybersecurity in Spain (INCIBE), which provides a series of real stories related to cybersecurity as a measure to raise awareness among companies about the importance of having the necessary contingency measures in place.  **What happened?**  An employee in the administration department of an SME was in charge of managing the receiving and sending of the company's parcels through the services of different courier companies. On a daily basis, parcels were sent and received in the company, so this employee was waiting for a box with materials for the production department.  On that day, the employee received an SMS on his corporate smartphone from what appeared to be a parcel delivery company. The SMS indicated that it was necessary to download an application via a link provided in the message, in order to manage the delivery, so the employee proceeded to do so.  Days later, colleagues in charge of bill payments alerted the employee that his corporate phone bill was much higher than usual. This was because a huge number of SMS messages had been sent from the device throughout the month without the employee's knowledge.  **Why did it happened?**  The employee was a victim of smishing. The SMS came from a fake sender, and by clicking on the link and downloading the app, he had infected his phone with the "FluBot" malware, a Trojan that installs itself on Android devices with the aim of stealing banking information by posing as a parcel delivery company urging you to take immediate action to avoid losing the package. In addition, the malware uses the phone's address book to send more fake SMS messages and infect more devices, remotely executes commands and prevents the user from uninstalling the application.  **How could it have been avoided?**  Although the employee's phone was eventually restored by the company's IT department, all of this could have been avoided by measures such as:   * Implementing cybersecurity policies in the company to control and limit the use of corporate devices and installed applications. * Not installing applications from unknown sources. * Being suspicious of messages that include links or attachments. * Having all security updates of the operating system and antivirus activated and updated. |
| **Link for further information:** | <https://www.incibe.es/protege-tu-empresa/blog/historias-reales-smishing-se-colaron-mi-movil-corporativo-sms> |
| **Target group of the case study:** | Micro, Small & Medium Enterprises (MSMEs)  Employees of MSMEs  The EU VET ecosystem  Business support organizations |
| **ESCO competencies and skills** | |
| * Transversal skills and competences * Social and emotional skills * Critical thinking * Analytical thinking * Problem-solving * Self-management * Business management * Adaptability * Resilience * Creativity * Networking * Initiative * Flexibility * Openness * Understanding complexity * Cooperation * Empathy * Innovation * Leadership      * Skills * Technological skills * Product marketing * Digital marketing * Digital skills * Communication * Cooperation * Emotional intelligence      * Knowledge * Business management * Online learning and training * Advertising * Cloud computing * Big data * E-commerce * Artificial intelligence * IoT * Digital literacy * Cybersecurity * Data mining and analysis * Sustainability * Well-being * Climate change * Social media management | |