**RESTART: Resiliencia y formación para Pymes**

**Caso de estudio**

**(Resultado del proyecto 3 - Tareas 3.1. y 3.2)**

|  |  |
| --- | --- |
| **Autor del caso de estudio:** | Internet Web Solutions |
| **Nombre del módulo al que se asigna el caso de estudio:** | Módulo 3: Ciberseguridad en la oficina (desde casa) |
| **Título del caso de estudio:** | Phishing + SMS: los riesgos del smishing |
| **Descripción del caso de estudio:** | Como ya sabes tras haber estudiado el módulo “Cybersecurity in the (home) office, el phishing es el ataque más común a las MSMEs europeas, y estos pueden varias según el medio utilizado para el ataque. En este caso de estudio nos centramos en el smishing, la técnica del engaño a través de SMS.  Este caso de estudio ha sido extraído del Instituto Nacional de Ciberseguridad en España (INCIBE), que proporciona una serie de historias reales relacionadas con la ciberseguridad como medida para concienciar a las empresas sobre la importancia de contar con las medidas de contingencia necesarias.  **¿Qué pasó?**  Un empleado del departamento de administración de una pyme era el encargado de gestionar la recepción y envío de paquetería de la empresa por medio de los servicios de distintas empresas de mensajería. De forma diaria, se enviaban y recibían paquetes en alguno de los departamentos de la empresa, por lo que éste empleado se encontraba esperando una caja con materiales para el departamento de producción.  Ese día, el empleado recibió un SME en su teléfono móvil corporativo de la que parecía ser una empresa de paquetería. En el SMS se indicaba que era necesario descargar una aplicación a través de un link proporcionado en el mensaje, para gestionar la entrega, por lo que el empleado procedió a hacerlo.  Días más tarde, los compañeros encargados de los pagos de facturas, alertaron al empleado de que la factura de su teléfono corporativo era mucho mayor de lo habitual. Esto fue debido a que durante todo el mes se habían enviado una enorme cantidad de SMS desde el dispositivo sin que el empleado lo supiera.  **¿Por qué pasó?**  El empleado fue víctima de smishing. El SMS provenía de un remitente falso, y al pinchar en el enlace y descargar la aplicación, había infectado su teléfono con el malware “FluBot”, un troyano que se instala en dispositivos Android con el objetivo de robar información bancaria haciéndose pasar por empresas de paquetería que te instan a hacer una acción inmediata para no perder el paquete. Además, el malware utiliza la agenda de contactos del teléfono para enviar más SMS falsos e infectar a un número mayor de dispositivos, ejecuta comandos de manera remota y evita que el usuario pueda desinstalar la aplicación.  **¿Cómo pudo haberse evitado?**  Aunque al final el teléfono del empleado fue restaurado por el departamento de informática de la empresa, todo esto podría haberse evitado con medidas como:   * La implementación de políticas de ciberseguridad en la empresa para controlar y limitar el uso de los dispositivos corporativos y las aplicaciones instaladas. * No instalando aplicaciones de orígenes desconocidos. * Sospechando de los mensajes que incluyen enlaces o documentos adjuntos. * Contando con todas las actualizaciones de seguridad del sistema operativo y antivirus activado y actualizado. |
| **Link para más información:** | <https://www.incibe.es/protege-tu-empresa/blog/historias-reales-smishing-se-colaron-mi-movil-corporativo-sms> |
| **Grupo objetivo del caso de estudio:** | Microempresas, pequeñas y medianas empresas (MiPymes)  Empleados de MiPymes  Ecosistema de EFP de la UE  Organizaciones de apoyo a las empresas |
| **Competencias y habilidades ESCO** | |
| * Habilidades y competencias transversales * Habilidades sociales y emocionales * Pensamiento crítico * Pensamiento analítico * Resolución de problemas * Autogestión * Gestión de negocio * Adaptabilidad * Resiliencia * Creatividad * Networking * Iniciativa * Flexibilidad * Sinceridad * Comprensión de la complejidad * Cooperación * Empatía * Innovación * Liderazgo      * Habilidades * Habilidades tecnológicas * Marketing de producto * Marketing digital * Habilidades digitales * Comunicación * Cooperación * Inteligencia emocional      * Conocimiento * Gestión de negocio * Aprendizaje y formación online * Publicidad * Computación en la nube * Big data * Comercio electrónico * Inteligencia Artificial * IoT * Alfabetización digital * Ciberseguridad * Minado y análisis de datos * Sostenibilidad * Bienestar * Cambio climático * Gestión de redes sociales | |