

## Up SPAIN y la ciberseguridad en el trabajo

### **La trampa ha sido el primer ejercicio práctico de una serie de seminarios de concienciación en materia de ciberseguridad puestos en marcha por Up SPAIN**

De esta iniciativa se desprenden varias conclusiones, entre las que destacan los errores más habituales que puede cometer un empleado en su puesto de trabajo y que podría llegar a comprometer tanto la información confidencial de la empresa como sus propios datos personales:

Dar información confidencial por Internet y no investigar sobre la identidad de quien solicita esos datos.

No leer bien los emails, su contenido, así como los enlaces que pueden llevar a una 'trampa'.

Instalar programas cuando se desconoce quién es el fabricante o el desarrollador; el software que se descarga desde Internet es otra de las principales fuentes de virus.

Conectarse a redes wifi abiertas. Se corre el riesgo de que un tercero pueda monitorizar la actividad, copiar las contraseñas o conseguir cualquier otra información personal.

Crear contraseñas fáciles de adivinar. Hay que idear claves de acceso complejas que sean difíciles de piratear.

No actualizar los programas. Hay que contar con los últimos parches desarrollados para el software instalado en un ordenador.

Prescindir de un antivirus.

No hacer copias de seguridad.

Los riesgos de no atender a estas recomendaciones son muy altos, según explica el experto en TIC y ciberseguridad Pedro José Vela, consejero delegado de Bomonte Tecnologías, y responsable de dirigir la sesión práctica La trampa en Up SPAIN. En algunos casos, se podría incluso llegar a hablar de fraudes millonarios, tanto a las empresas como a los propios empleados.

Las cifras no son alentadoras. Según el último Informe de Investigación de 2018, el 58% de los ataques a empresas se dirige a pymes. Además, el 73% de las brechas de seguridad está relacionado con agentes externos a las organizaciones; a la vez que otro de los grandes problemas es que siete de cada diez de estos ataques tardan meses en descubrirse. Se estima que se producen 309.854 incidentes diarios.

Por eso, en opinión de este experto, es vital atender a dónde pueden encontrarse las principales brechas en materia de ciberseguridad:

Fugas de información a través del uso descuidado de pendrives, tablets y teléfonos inteligentes.

Robos de información y fraudes.

Falta de formación y concienciación.

Inexistencia de planes de gestión de los incidentes de seguridad.

Muy baja inversión en ciberseguridad.  
Falta de planificación de continuidad de negocio.  
Contraseñas débiles y accesos a servicios compartidos sin permisos.  
Incapacidad de detectar un ataque de forma rápida y autónoma.  
Utilización de sistemas operativos caducos en puestos de trabajo y servidores.  
Uso de software creado a medida sin suficientes garantías de seguridad.

En el caso de Up SPAIN, el ejercicio para concienciar a la plantilla sobre esta realidad consistió en simular ataques reales, utilizando la técnica del phishing, también conocido como suplantación de identidad para lograr de forma fraudulenta datos confidenciales, desde una contraseña hasta datos bancarios. El cibercriminal, conocido como phisher, se hace pasar por una persona o empresa de confianza, por ejemplo, a través de un correo electrónico.

Se hace creer a los usuarios que están descargando o ejecutando un programa seguro, cuando en realidad están utilizando un enlace malicioso. De esta manera, una vez que el usuario se descarga el contenido, el cibercriminal tiene acceso al dispositivo de la víctima.

“Como era de esperar -según explica Carlos Ávila, responsable de Sistemas de Up SPAIN-, los sistemas implantados en la compañía pudieron detectar este último paso y, aunque real, no fue efectivo. Aun así explicamos esta técnica ampliamente utilizada en el seminario mediante un caso real sin las contramedidas efectivas”. “Para Up SPAIN la seguridad es vital y poder concienciar a nuestros colaboradores de su importancia nos puede ahorrar muchos disgustos”, concluye Ávila.

**Datos de contacto:**

Departamento de Comunicación y Marketing  
913814332

Nota de prensa publicada en: [Madrid](#)

Categorías: [Nacional](#) [Telecomunicaciones](#) [E-Commerce](#) [Ciberseguridad](#) [Recursos humanos](#)

---

**NotasdePrensa**

<https://www.notasdeprensa.es>