



## LOS FRAUDES ONLINE MÁS COMUNES

- Los ciberdelincuentes atacan al punto más importante de la cadena de ciberseguridad: **las personas.**
- **El correo electrónico o las páginas web** son las principales vías para producir incidentes.
- Se aprovechan del **desconocimiento de los empleados** en nuevas tecnologías y el uso de ingeniería social.

Una vez más, el INCIBE recuerda a las empresas los métodos de actuación más utilizados por los ciberdelincuentes, los cuales se aprovechan especialmente del desconocimiento de las personas sobre las nuevas tecnologías.

Los ataques más comunes son:

- **Email spoofing:** suplantan la identidad de una organización mediante un correo de un remitente falso. Envían *phishing* y *malware* para robar credenciales de acceso a información bancaria o confidencial.
- **Sextorsión:** chantajea a las víctimas con un supuesto vídeo de contenido íntimo, marcando un plazo límite para realizar algún pago y evitar su difusión.
- **Suplantación de proveedores:** con el objetivo de solicitar el número de cuenta, creando nombres de dominio muy similares a los del legítimo proveedor.
- **Hotlinking:** generalmente utilizan imágenes de una web empresarial para suplantar un producto y beneficiarse de la reputación de la marca.
- **Suplantación de marca e imagen corporativa:** crean una copia de la web legítima donde venden productos que nunca envían.
- **E-skimming:** roban información bancaria y personal de los usuarios de tiendas online legítima.

Así mismo, insiste en que **el conocimiento es una de las principales defensas** que ayudarán a mejorar la ciberseguridad de los empleados y el negocio.

Se adjunta infografía del INCIBE sobre los fraudes online más frecuentes.