EL CORREO ELECTRÓNICO
Principales fraudes y riesgos

Phishing

Se basa en la **suplantación de una empresa o entidad fiable** como un banco o entidad pública. La **finalidad es hacerse con claves de acceso o información sensible** como pueden ser datos fiscales o bancarios.

Scam

Su objetivo es **perpetrar engaños y estafas** a sus receptores y obtener tanta información personal, de la empresa o bancaria como puedan. El gancho, en este caso, suele girar en torno a falsos premios de lotería, herencias millonarias, ofertas de empleo que requieren de desembolsos, etc.

Sextorsión

Extorsión con un supuesto vídeo privado o de contenido comprometedor, amenazando con difundirlo a todos sus contactos de correo electrónico y redes sociales, a no ser que realice el pago de una cantidad económica.

Malware

Código malicioso que podría infectar los dispositivos. Los emails podrían contener algún tipo de **archivo adjunto o enlaces a webs donde una vez descargado y ejecutado el fichero infectará el dispositivo.**

Cómo detectar correos fraudulentos

- **Remitentes desconocidos:** comprobando el remitente del correo se puede saber que la comunicación es fraudulenta. Hay que sospechar de los mensajes cuyo remitente sea desconocido y verificarlo por otro medio, como el teléfono.
- **Documentos adjuntos maliciosos:** por norma, ninguna entidad envía documentos adjuntos en el correo. Esta es la forma mas habitual que usan los ciberdelincuentes para infectar los equipos con malware.
- **Ingeniería social en el cuerpo y asunto:** se trata de generar un sentimiento de alerta o urgencia e instar al usuario a que realice una determinada acción de forma inmediata, como abrir un adjunto malicioso, acceder a una web ilegítima o realizar un pago.
- **Enlaces falseados:** las entidades legítimas por lo general no envían enlaces en sus comunicaciones oficiales y solicitan al usuario que acceda al sitio web, utilizando su navegador web o la aplicación específica.
- **Comunicaciones impersonales:** las entidades legítimas en las comunicaciones suelen usar el nombre y apellidos del destinatario, haciendo que la comunicación sea más personal.
- **Remitentes falseados y firma:** los ciberdelincuentes falsifican la dirección del remitente haciendo que, a simple vista, no se identifique el correo como fraudulento. Esta técnica se conoce como *email spoofing,* y para comprobar si el correo es legítimo es necesario analizar las cabeceras del mismo.
- **Mala redacción:** las faltas de ortografía y la utilización de expresiones poco habituales son una señal bastante certera de que ese mensaje es fraudulento.

Otros riesgos del email

CC y CCO

Enviar correos electrónicos a múltiples destinatarios usando la opción de CC (Carbon Copy) o en copia, en vez de la opción de CCO o copia oculta (o BCC, Blind Carbon Copy), es uno de los incidentes de fuga de información.

Función de autocompletado

Es recomendable revisar bien el destinatario antes de enviar un email. La función de autocompletado puede sugerirnos un correo similar y no darnos cuenta.

Descarga automática de imágenes

Las imágenes son usadas para monitorizar si un correo ha sido abierto o no. Tener habilitada la descarga automática de imágenes es un riesgo para tu privacidad y seguridad.

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
protege tu empresa
Twitter @ProtegeEmpresa
Facebook protegetuempresa
Linkedin Protege tu empresa de INCIBE
YouTube INCIBE