DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Boletín protección de datos

Boletín del Departamento de protección de datos y Seguridad de la Información de la Diputación Provincial de Valencia

Boletín N.º 31| Enero 2023

INGENIERÍA SOCIAL

Í N D I C E

INGENIERÍA SOCIAL

EN LA ADMINISTRACIÓN PÚBLICA

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

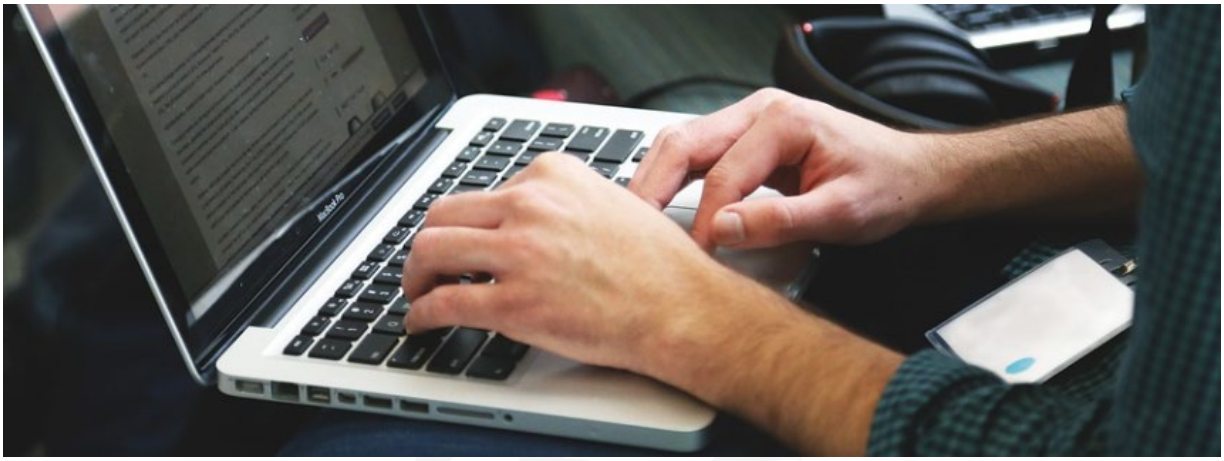
Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirse a nuestro Boletín informativo accede al siguiente enlace

INTRODUCCIÓN



Uno de los pilares fundamentales de la protección de los datos personales es la **seguridad en el tratamiento** de estos datos. En particular, el artículo 32 del Reglamento General de Protección de datos establece que se deberán aplicar "*medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo"*.

Las medidas de seguridad protegen los datos personales de posibles ataques tecnológicos, mitigando el riesgo de que se materialicen las amenazas a las que se encuentran expuestos. Sin embargo, cabe destacar que durante el año 2022 el 82% de las brechas tecnológicas involucraron el **factor humano**.

Estos datos ponen de manifiesto que la vía más fácil para comprometer una organización de cualquier tipo – incluido el sector público – es conseguir que sus propios usuarios legítimos abran puertas a los ciberatacantes o incluso ejecuten directamente las acciones que el ciberatacante desea. Para lograrlo, se han desarrollado **técnicas de ingeniería social**.

A estos efectos, en una de las publicaciones de la Agencia Española de Protección de Datos, se define "ingeniería social" como "la acción de engañar o chantajear a una persona para que revele información o emprenda una acción que pueda usarse para comprometer o afectar negativamente un sistema o, lo que es su fin último, una organización o un Estado".

En el presente boletín se abordarán las diferentes técnicas de ingeniería social y sus peculiaridades.

"INGENIERÍA SOCIAL: acción de engañar o chantajear a una persona para que revele información o emprenda una acción que pueda usarse para comprometer o afectar negativamente un sistema o, lo que es su fin último, una organización o un Estado".

PRINCIPALES TÉCNICAS DE INGENIERÍA SOCIAL

Pretexting

- Base de cualquier ataque de ingeniería social
- Consiste en elaborar un escenario/historia ficticia, donde el atacante tratará de que la víctima comparta información que, en circunstancias normales, no revelaría.

Phishing

- Busca "pescar" a las víctimas
- Con carácter general, se emplean correos electrónicos con archivos adjuntos infectados o links a páginas fraudulentas con el objetivo de tomar el control de sus equipos y robarles información confidencial.

Sextorsión

- Chantaje que busca amenazar a la víctima con distribuir supuestamente contenido comprometido de ella a sus contactos (aunque no exista dicho contenido), sino accede a las peticiones del ciberdelincuente, generalmente a realizar un pago

Baiting

- Utiliza un cebo con software malicioso a la vista de sus víctimas para que ellos mismos infecten sus dispositivos

Smishing

- Es una variante del "phishing" pero que se difunde a través de SMS
- Se pide al usuario que llame a un número de tarificación especial o que acceda a un enlace de una web falsa

Vishing

- Consiste en llamadas telefónicas mediante las cuales el atacante se hace pasar por una organización o persona de confianza para que la víctima revele información privada.

Shoulder surfing	•Se basa en mirar "por encima del hombro" •Al atacante le basta con observar lo que escribe o tiene en pantalla otro usuario para obtener información muy útil
Quid pro quo	•Se promete un beneficio a cambio de información de carácter personal. Suelen ser compensaciones en formato regalo (merchandising, dinero o acceso gratuito a programas de pago)
Dumpster diving	•Se refiere al acto de "husmear en la basura" para obtener documentos con información personal o financiera
Redes sociales	•Las técnicas de engaño más comunes a través de las redes sociales son mediante cupones de descuento, juegos y concursos donde el usuario cree que puede ganar algo.

Los ciberataques basados en técnicas de ingeniería social pueden ser simples o complejos.

El primer grupo utiliza solamente lo que se conoce como *sesgos congnitivos básicos* e inherentes a la naturaleza humana. En base a estudios e investigaciones, las personas tomamos alrededor de 35.000 decisiones de media al día, de las cuales solamente 91 son conscientes. El resto las toma el cerebro con atajos mentales o sesgos cognitivos, entre los que se encuentran hacer o no “clic” en un enlace *ransomware* que recibimos por correo electrónico. Por ejemplo, el “efecto de verdad ilusoria” provoca que, como al cerebro le resulta más sencillo procesar información que ha experimentado anteriormente, se tenga una sensación que nos puede llevar a malinterpretar una señal como un contenido verdadero. De esta manera, los ciberatacantes pueden realizar ataque sde phishing aprovechando este sesgo. **La cultura de la ciberseguridad en el sector público debe incorporar el enfoque de pensar y revisar antes de hacer clic en un enlace**.

El segundo grupo se ajusta a las peculiaridades de cada persona u organización. Es el más peligroso porque a menudo las medidas de seguridad tradicionales no son suficientes para detener estos ataques.

En conclusión, es muy relevante la concienciación y formación continua de los empleados de las entidades públicas, pues estos ciberataques pueden comprometer información personal de los ciudadanos.

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES FRENTE A UNA RECLAMACIÓN POR HABER RECIBIDO UN ATAQUE DE PHISHING

La Agencia Española de Protección de Datos (AEPD) - Expediente Nº: E/06661/2021 - procedió al archivo de las actuaciones tras la reclamación de un particular a una notaría por haber recibido mediante una dirección de correo electrónico desconocida y un archivo adjunto. En el cuerpo del correo contenía el contenido literal de dos correos enviados por la Notaría con la que contrató servicios anteriormente e incluía sus datos personales.

En el presente caso, de la documentación aportada por la NOTARÍA en el curso de estas actuaciones de investigación ***no se desprende que, con anterioridad a la brecha de seguridad, careciera de medidas de seguridad razonables en función de los posibles riesgos estimado****s.*

*La NOTARÍA reconoce que la causa que ha podido generar el incidente se deriva de la actuación del malware "***MALWARE.1". Dicho malware se propaga por correo electrónico al descargarse archivos adjuntos.*

Añade, no obstante que, "no consta que nadie del despacho hubiera abierto dichos archivos adjuntos".

*La NOTARÍA identifica dos equipos afectados por el incidente y expresa que para solucionar el incidente "se llevó a cabo un análisis de seguridad y neutralización del virus infectado haciéndose uso de las herramientas específicas y software antivirus-EmoCheck y ***MALWARE.1-Stopper-".*

Asimismo, no existen evidencias de que no hubiera actuado de forma diligente una vez conocida la brecha de seguridad, ni que las medidas adoptadas con posterioridad al incidente aquí analizado no fueran adecuadas.

Así, después de producirse la brecha de seguridad, la NOTARÍA manifiesta que ha reforzado las medidas de seguridad implantadas:

- *Revisiones informáticas generales en el ámbito del mantenimiento periódico contratado.*
- *Actuaciones de aviso y advertencia desde Gerencia a los empleados de la Notaria ante circunstancias similares que puedan estar produciéndose, habiéndose dado indicaciones precisas relativas a extremar las precauciones ante correos sospechosos, no debiéndose proceder a la apertura de sus archivos adjuntos en modo alguno.*
- *Revisiones relativas a protección de datos de carácter personal, especialmente en lo tocante a la responsabilidad proactiva ("accountability") y al análisis y control de las medias técnicas y organizativas implantadas."*

Cabe destacar la buena disposición de la NOTARÍA en el sentido de que, en cuanto ha tenido conocimiento del incidente, ha puesto en marcha las medidas oportunas para evitar que se pueda repetir en el futuro. En consecuencia, la AEPD consideró que la NOTARÍA había adoptado todas las medidas que estaban a su disposición para impedir y minimizar el impacto de la brecha de seguridad ocurrida.

MATERIAL COMPLEMENTARIO

- Publicación de la AEPD "Sin privacidad no hay ciberseguridad". Consulta la publicación en este enlace.
- Infografía sobre técnicas de ingeniería social publicada por OSI (Oficina de Seguridad del Internauta. Consulta la Infografía en este enlace.
- Ciberconsejos para los ataques de "phishing" publicado por el Centro Criptológico Nacional. Consulta la Publicación en este enlace.
- Declaración sobre el papel de un enfoque basado en el riesgo en la protección de datos del Grupo de Trabajo del artículo 29. Consulta la Publicación en este enlace.

NOTICIAS

- **La AEPD impone una sanción por infracción del artículo 5.1.f) (integridad y confidencialidad) y 5.2 del RGPD (responsabilidad proactiva)**

  El reclamante detectó que su SIM no funcionaba correctamente y se habían realizado tranferencias sin su consentimiento. Se debía a que el ciberatacante había duplicado su tarjeta SIM.

  La compañía telefónica alegó que la pérdida de disposición y control de los datos personales se produce bien en un momento anterior a su participación (por ejemplo, mediante prácticas de phishing o ingeniería social) o bien en un momento posterior a su participación, por lo que considera que no se le pueden achacar.

  La AEPD considera que en los procedimientos seguidos por la compañía para gestionar las solicitudes de cambio de SIM se identifican vulnerabilidades, constatándose la falta de responsabilidad proactiva y la deficiencia en las medidas de seguridad aplicadas, lo que constituye una infracción de los principios básicos de protección de datos.

  Consulta la publicación en este enlace.