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 7| Enero 2021

PHISHING

Í N D I C E

	Pág.
Tema central: Phishing	2-6
¿Qué es el phishing?	2
¿Cómo actúan los ciberdelincuentes?	2
¿Cuáles son las técnicas más habituales?	3
Phishing en tiempos de pandemia	4
¿Puede suponer una brecha de seguridad en mi organización?	5
¿Cómo protegernos contra el phishing?	6
Material complementario	7
Noticias de actualidad	7

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: dpdssi@dival.es

SUSCRIPCIONES

Si deseas suscribirse a nuestro Boletín informativo accede al siguiente enlace

¿QUÉ ES EL *PHISHING*?

Entre los riegos con los que nos podemos encontrar cuando hacemos uso de Internet está el *phishing*, una de las técnicas de ingeniería social más usadas por los ciberdelincuentes para obtener información personal de los usuarios suplantando a una persona o entidad.

La técnica consiste en el envío de un mensaje o la realización de una llamada por parte de un ciberdelincuente a un usuario simulando ser una personal o una entidad de confianza (banco, institución pública, etc.) con el objetivo engañarle y manipularle a fin de que acabe realizando alguna acción que ponga en peligro sus datos o los de la organización a la que pertenece.

¿CÓMO ACTUAN LOS CIBERDELINCUENTES?

Te envían un correo electrónico, SMS, MMS, un mensaje mediante alguna herramienta de mensajería instantánea o incluso realizan una llamada, donde se hacen pasar por una persona o entidad legítima.

Te piden que accedas a un enlace de apariencia legítima, que descargues un documento o que verifiques una serie de datos.

Acabas accediendo a páginas web falsificadas donde, creyendo estar en un sitio de toda confianza, introduces la información solicitada.

La información (por ejemplo, contraseñas o datos bancarios) va a parar a manos del estafador, que habitualmente utiliza para causarte pérdidas económicas, a ti o a la organización a la que perteneces.

"LA TÉCNICA DEL PHISHING CONSISTE EN EL ENVÍO DE UN MENSAJE POR PARTE DE UN CIBERDELINCUENTE A UN USUARIO SIMULANDO SER UNA PERSONA O ENTIDAD DE CONFIENZA (BANCO, INSTITUCIÓN PÚBLICA, ETC.), CON EL OBJETIVO ENGAÑARLE Y MANIPULARLE, A FIN DE QUE ACABE REALIZANDO ALGUNA ACCIÓN QUE PONGA EN PELIGRO SUS DATOS O LOS DE LA ORGANIZACIÓN A LA QUE PERTENECE."

¿CUÁLES SON LAS TÉCNICAS MÁS HABITUALES?

SPEAR PHISHING

Método de ataque personalizado en una persona u organización

PHISHING REDIRECTOR

Método de ataque basado en campañas masivas

SMISHING (SMS)

Método de ataque por medio de mensajes de texto

VISHING

Método de ataque por medio de una llamada telefónica

PHISHING EN TIEMPOS DE PANDEMIA

En el contexto de pandemia en el que nos encontramos, los ciberdelincuentes están aprovechando para lanzar ataques de *phishing.*

El *modus operandi* es siempre muy similar: los ciberdelincuentes tratan de suplantar organizaciones legítimas con información relevante sobre el COVID-19 como el Ministerio de Sanidad, una Consejería de Sanidad de una Comunidad Autónoma, Fuerzas del Orden, Organizaciones Internacionales, simulando prestar ayuda y consejo, o incluso fingiendo ser la organización en la que trabajas.

Lo hacen a través de mensajería instantánea y también a través de emails. En la mayoría de los casos te pedirán que abras un archivo con urgencia o sigas un enlace de internet para obtener la información. Si se sigue el enlace y se descarga y ejecuta un archivo adjunto, se tratará de algún tipo de malware que permita a los ciberdelincuentes tomar el control de tu dispositivo, acceder a tu información y datos personales e incluso cifrar esos datos.

Los enlaces de internet incluidos en estos mensajes o correos electrónicos también te pueden llevar a páginas web que suplantan la identidad de otras organizaciones para robar tus credenciales de acceso a un servicio u otra información personal.

Por ejemplo, el pasado mes de octubre de 2020, fue detectada una campaña de envío masivo de correos electrónicos maliciosos que intentaban suplantar la identidad del Ministerio de Sanidad mediante la duplicación de la imagen corporativa y el uso de dominios de correo inexistentes, como @mscbs.gob.es. Estos correos contenían información relacionada con términos como el coronavirus, la COVID-19, Estado de Alarma y otros.

"EN EL CONTEXTO DE PANDEMIA EN EL QUE NOS ENCONTRAMOS, LOS CIBERDELINCUENTES ESTÁN APROVECHANDO PARA LANZAR ATAQUES DE PHISHING".

¿CÓMO PROTEGERNOS CONTRA EL PHISHING?

Estas son algunas de las medidas que la Agencia Española de Protección de Datos (AEPD), el Centro Criptológico Nacional (CCN) y el Instituto Nacional de Seguridad (INCIBE) nos recomiendan seguir para evitar ser víctimas del *phishing:*

Si el mensaje te pide hacer alguna acción extraña: ignóralo y bórralo.

Si el mensaje te obliga a tomar una decisión en unas pocas horas, es mala señal. Contrasta directamente si la urgencia es real o no con el servicio a través de otros canales.

Comprueba el dominio del correo remitente y que su nombre coincida con su cuenta de correo.

Evita abrir archivos adjuntos si desconoces el remitente o no se espera el documento.

Verifica el enlace web al que remite el mensaje. A veces, los ciberdelincuentes son capaces de crear enlaces que se parecen mucho a las direcciones legítimas.

Presta atención a la sintaxis de los enlaces a las páginas web que lleguen por correo.

Comprueba que la página web en la que has entrado es una dirección segura. Para ello, ha de empezar con https:// y un pequeño candado cerrado debe aparecer en la barra de estado de nuestro navegador.

Sospecha de mensajes con faltas de ortografía, errores gramaticales y saludos genéricos.

Ten cuidado con las solicitudes de datos a través de webs a las que has llegado siguiendo el enlace. Mejor accede directamente a la web de la organización.

Comunica el incidente a tu responsable (DPD, CISO…)

Mantén actualizado el navegador, el sistema operativo y demás software.

Evita el uso de medios extraíbles.

Instala un programa antivirus y mantenlo actualizado.

Evita usar redes públicas.

Protege tu contraseña. No almacenes las contraseñas en los navegadores.

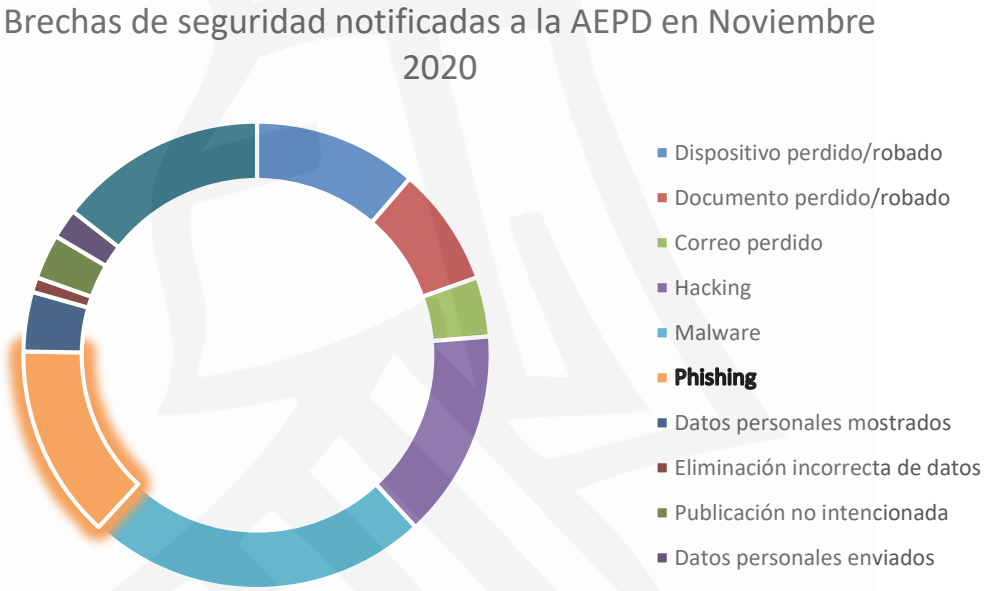
SIGUE ESTAS RECOMENDACIONES

¿PODRÍA SUPONER UNA BRECHA DE SEGURIDAD EN MI ORGANIZACIÓN?

El hecho de que un usuario de tu organización fuese víctima de un ataque de pshishing, podría suponer una brecha de seguridad dentro de la organización y generar una serie de efectos adversos considerables, susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales; por lo que debemos intentar evitarlo y, en caso de que suceda, saber gestionarlo adecuadamente.

Por eso, debemos atender a las medidas señaladas en el apartado anterior, siendo de vital importancia que, si detectamos cualquier mensaje sospechoso en nuestro correo, teléfono u otras herramientas corporativas, lo pongamos en conocimiento de la persona responsable en nuestra organización, de modo que analice si se trata de un ataque phishing y advierta al resto de las personas trabajadoras y, en su caso, informe a la Agencia Española de Protección de Datos (AEPD).

Si acudimos a los informes mensuales sobre brechas de seguridad de datos personales notificadas a la AEPD, se puede apreciar cómo el phishing es uno de los medios por el que las brechas de seguridad se materializan más habitualmente, muy cerca de otras técnicas similares como el malware o el hacking:



"SI DETECTAMOS CUALQUIER MENSAJE SOSPECHOSO, DEBEMOS PONERLO EN CONOCIMIENTO DE LA PERSONA RESPONSABLE EN NUESTRA ORGANIZACIÓN."

MATERIAL COMPLEMENTARIO

- "Protección de datos y prevención de delitos", de la AEPD. Consulta el documento en este enlace.
- "Guía de Privacidad y Seguridad en Internet", de la AEPD, INCIBE y OSI. Consulta este enlace.
- "Cómo evitar ser víctima del phishing", del CCN. Consulta este enlace.
- "Phishing", de INCIBE. Consulta este enlace.
- "Campañas de phishing sobre el Covid-19" de la AEPD. Consulta este enlace.
- "Notificación de Brechas de seguridad" de la AEPD. Consulta este enlace.

NOTICIAS

- **La Agencia Española de Protección de Datos (AEPD) apercibe al Alcalde de un Ayuntamiento por exponer en su página de Facebook la Sentencia íntegra de un procedimiento en el que actuaba como parte codemandada junto al Ayuntamiento.** El post expuesto por el reclamado en dicha red social da a conocer unos hechos y unos datos que permiten identificar al reclamante a través de la íntegra sentencia expuesta, junto con las diversas circunstancias que en sus páginas se relatan, entre otras el desarrollo de su empleo, o la alusión a terceras personas a las que se identifica que se suceden en el relato de la misma. Consulta la Resolución en este enlace.

- **La Autoridad Catalana de Protección de Datos (APDCAT) emite un informe jurídico en relación con el acceso de un padre a las calificaciones académicas universitarias de su hijo mayor de edad.** Concluye la APDCAT que la denegación del acceso a la información solicitada podría obstaculizar el derecho a la tutela efectiva del progenitor, regulado en el artículo 24.1 de la Constitución española, en la medida que el progenitor no puede conocer si el hijo mantiene el rendimiento regular académico, ni disponer del elemento probatorio que requiere la normativa procesal para la admisión de una demanda de modificación de medidas. Consulta el informe en este enlace.

- **INCIBE nos facilita una serie de consejos para evitar los riesgos de ciberseguridad desde el puesto de trabajo.** Fuga de datos, pérdida de información confidencial, infecciones por *malware* o deslices en el uso del correo electrónico o las redes sociales son algunos de los riesgos a los que nos enfrentamos en el puesto de trabajo. Es importante conocer las situaciones más comunes relacionadas con la seguridad del entorno de trabajo de los empleados para poder así minimizar el riesgo de fuga o pérdida de datos. Consulta las recomendaciones en este enlace.