DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Butlletí protecció de dades

Butlletí del Departament de Protecció de Dades i Seguretat de la Informació de la Diputació Provincial de València

Butlletí Núm. 7 | Gener 2021

PHISHING

Í N D E X

Vos invitem a traslladar-nos aquelles temàtiques que resulten del vostre interès per als pròxims butlletins informatius. Estes peticions hauran de dirigir-se a:

Diputació de València

Dpt. de Protecció de Dades i Seguretat de la Informació

Pl. de Manises, 4 46003 València

Correu electrònic: dpdssi@dival.es

SUBSCRIPCIONS

Si desitges subscriure's al nostre Butlletí informatiu accedix al següent enllaç

QUÈ ÉS EL *PHISHING*?

Entre els riscos amb els quals ens podem trobar quan fem ús d'Internet està el phishing, una de les tècniques d'enginyeria social més usades pels ciberdelinqüents per a obtindre informació personal dels usuaris suplantant a una persona o entitat.

La tècnica consisteix en l'enviament d'un missatge o la realització d'una crida per part d'un ciberdelinqüent a un usuari simulant ser una personal o una entitat de confiança (banc, institució pública, etc.) amb l'objectiu enganyar-li i manipular-li a fi que acabe realitzant alguna acció que pose en perill les seues dades o els de l'organització a la qual pertany.

COM ACTÚEN ELS CIBERDELINQÜENTS?

T'envien un correu electrònic, SMS, MMS, un missatge mitjançant alguna eina de missatgeria instantània o fins i tot realitzen una crida, on es fan passar per una persona o entitat legítima.

Et demanen que accedisques a un enllaç d'aparença legítima, que descarregues un document o que verifiques una sèrie de dades.

Acabes accedint a pàgines web falsificades on, creient estar en un lloc de tota confiança, introdueixes la informació sol·licitada..

La informació (per exemple, contrasenyes o dades bancàries) pararà a les mans de l'estafador, que habitualment utilitza per a causar-te pèrdues econòmiques, a tu o a l'organització a la qual pertanys.

"LA TÈCNICA DEL PHISHING CONSISTEIX EN L'ENVIAMENT D'UN MISSATGE PER PART D'UN CIBERDELINQÜENT A UN USUARI SIMULANT SER UNA PERSONA O ENTITAT DE CONFIANÇA (BANC, INSTITUCIÓ PÚBLICA, ETC.), AMB L'OBJECTIU ENGANYAR-LI I MANIPULAR-LI, A FI QUE ACABE REALITZANT ALGUNA ACCIÓ QUE POSE EN PERILL LES SEUES DADES O ELS DE L'ORGANITZACIÓ A LA QUAL PERTANY."

QUINES SÓN LES TÈCNIQUES MÈS HABITUALS?

SPEAR PHISHING

Mètode d'atac personalitzat en una persona o organització

PHISHING REDIRECTOR

Mètode d'atac basat en campanyes massives

SMISHING (SMS)

Mètode d'atac per mitjà de missatges de text

VISHING

Mètode d'atac per mitjà d'una trucada telefònica.

PHISHING EN TEMPS DE PANDÈMIA

En el context de pandèmia en el qual ens trobem, els ciberdelinqüents estan aprofitant per a llançar atacs de phishing.

El *modus operandi* sempre molt similar: els ciberdelinqüents tracten de suplantar organitzacions legítimes amb informació rellevant sobre el COVID-19 com el Ministeri de Sanitat, una Conselleria de Sanitat d'una Comunitat Autònoma, Forces de l'Ordre, Organitzacions Internacionals, simulant prestar ajuda i consell, o fins i tot fingint ser l'organització en la qual treballes.

Ho fan a través de missatgeria instantània y també a través de correus electrònics. En la majoria dels casos et demanaran que òbrigues un arxiu amb urgència o seguisques un enllaç d'Internet per a obtindre la informació. Si se segueix l'enllaç i es descarrega i executa un arxiu adjunt, es tractarà d'alguna mena de *malware* que permeta als ciberdelinqüents prendre el control del teu dispositiu, accedir a la teua informació i dades personals i fins i tot xifrar aqueixes dades.

Els enllaços d'Internet inclosos en aquests missatges o correus electrònics també et poden portar a pàgines web que suplanten la identitat d'altres organitzacions per a robar les teues credencials d'accés a un servei o una altra informació personal.

Per exemple, el mes d'octubre passat de 2020, va ser detectada una campanya d'enviament massiu de correus electrònics maliciosos que intentaven suplantar la identitat del Ministeri de Sanitat mitjançant la duplicació de la imatge corporativa i l'ús de dominis de correu inexistents, com @mscbs.gob.es. Aquests correus contenien informació relacionada amb termes com el coronavirus, la COVID-19, Estat d'Alarma i uns altres.

"EN EL CONTEXT DE PANDÈMIA EN EL QUAL ENS TROBEM, ELS CIBERDELINQÜENTS ESTAN APROFITANT PER A LLANÇAR ATACS DE PHISHING".

COM PROTEGIR-NOS CONTRA EL PHISHING?

Aquestes són algunes de les mesures que l'Agència Espanyola de Protecció de Dades (AEPD), el Centre Criptològic Nacional (CCN) i l'Institut Nacional de Seguretat (INCIBE) ens recomanen seguir per a evitar ser víctimes del *phishing:*

Si el missatge et demana fer alguna acció estranya: ignora-ho i esborra-ho.

Si el missatge t'obliga a prendre una decisió en unes poques hores, és mal senyal. Contrasta directament si la urgència és real o no amb el servei a través d'altres canals.

Comprova el domini del correu remitent i que el seu nom coincidisca amb el seu compte de correu.

Evita obrir arxius adjunts si desconeixes el remitent o no s'espera el document.

Verifica l'enllaç web al qual remet el missatge. A vegades, els ciberdelinqüents són capaços de crear enllaços que s'assemblen molt a les direccions legítimes.

Para atenció a la sintaxi dels enllaços a les pàgines web que arriben per correu.

Comprova que la pàgina web en la qual has entrat és una adreça segura. Per a això, ha de començar amb https:// i un xicotet cadenat tancat ha d'aparèixer en la barra d'estat del nostre navegador.

Sospita de missatges amb faltes d'ortografia, errors gramaticals i salutacions genèriques.

Ves amb compte amb les sol·licituds de dades a través de webs a les quals has arribat seguint l'enllaç. Millor accedeix directament a la web de l'organització.

Comunica l'incident al teu responsable (DPD, CISO...)

Mantingues actualitzat el navegador, el sistema operatiu i altre programari.

Evita l'ús de mitjans extraïbles.

Instal·la un programa antivirus i mantén-lo actualitzat.

Evita usar xarxes públiques.

Protegeix la teua contrasenya. No magatzems les contrasenyes en els navegadors.

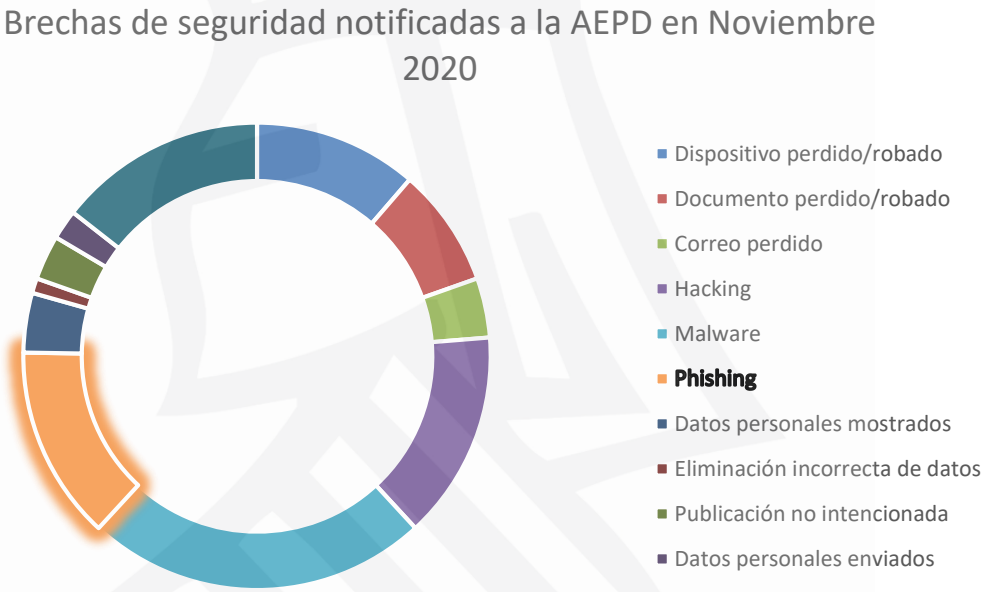
SEGUEIX AQUESTES RECOMANACIONS

PODRIA SUPOSAR UNA BRETXA DE SEGURETAT EN LA MEUA ORGANITZACIÓ?

El fet que un usuari de la teua organització fora víctima d'un atac de phishing, podria suposar una bretxa de seguretat dins de l'organització i generar una sèrie d'efectes adversos considerables, susceptibles d'ocasionar danys i perjudicis físics, materials o immaterials; pel que hem d'intentar evitar-lo i, en cas que succeïsca, saber gestionar-ho adequadament.

Per això, hem d'atendre les mesures assenyalades en l'apartat anterior, sent de vital importància que, si detectem qualsevol missatge sospitós en el nostre correu, telèfon o altres eines corporatives, el posem en coneixement de la persona responsable en la nostra organització, de manera que analitze si es tracta d'un atac phishing i advertisca a la resta de les persones treballadores i, en el seu cas, informe a l'Agència Espanyola de Protecció de Dades (AEPD).

Si acudim als informes mensuals sobre bretxes de seguretat de dades personals notificades a l'AEPD, es pot apreciar com el phishing és un dels mitjans pel qual les bretxes de seguretat es materialitzen més habitualment, molt prop d'altres tècniques similars com el malware o el hacking:



"SI DETECTEM QUALSEVOL MISSATGE SOSPITÓS, HEM DE POSAR-LO EN CONEIXEMENT DE LA PERSONA RESPONSABLE EN LA NOSTRA ORGANITZACIÓ."

MATERIAL COMPLEMENTARI

- "Protecció de dades i prevenció de delictes", de l'AEPD. Consulta el document en aquest enllaç.
- "Guia de Privacitat i Seguretat en Internet", de l'AEPD, INCIBE y OSI. Consulta aquest enllaç.
- "Com evitar ser víctima del phishing", del CCN. Consulta aquest enllaç.
- "Phishing", de INCIBE. Consulta aquest enllaç.
- "Campanyes de phishing sobre el Covid-19" de l'AEPD. Consulta aquest enllaç.
- "Notificacions de Bretxes de seguretat" de la AEPD. Consulta aquest enllaç.

NOTÍCIES

- **L'Agència Espanyola de Protecció de Dades (AEPD) adverteix a l'Alcalde d'un Ajuntament per exposar en la seua pàgina de Facebook la Sentència íntegra d'un procediment en el qual actuava com a part codemandada al costat de l'Ajuntament.** El post exposat pel reclamat en aquesta xarxa social dona a conèixer uns fets i unes dades que permeten identificar al reclamant a través de l'íntegra sentència exposada, juntament amb les diverses circumstàncies que en les seues pàgines es relaten, entre altres el desenvolupament del seu ús, o l'al·lusió a terceres persones a les quals s'identifica que se succeeixen en el relat d'aquesta. Consulta la Resolució en aquest enllaç.

- **L'Autoritat Catalana de Protecció de Dades (APDCAT) emet un informe jurídic en relació amb l'accés d'un pare a les qualificacions acadèmiques universitàries del seu fill major d'edat.** Conclou la APDCAT que la denegació de l'accés a la informació sol·licitada podria obstaculitzar el dret a la tutela efectiva del progenitor, regulat en l'article 24.1 de la Constitució espanyola, en la mesura que el progenitor no pot conèixer si el fill manté el rendiment regular acadèmic, ni disposar de l'element probatori que requereix la normativa processal per a l'admissió d'una demanda de modificació de mesures. Consulta l'informe en aquest enllaç.

- **INCIBE ens facilita una sèrie de consells per a evitar els riscos de ciberseguretat des del lloc de treball.** Fugida de dades, pèrdua d'informació confidencial, infeccions per malware o relliscades en l'ús del correu electrònic o les xarxes socials són alguns dels riscos als quals ens enfrontem en el lloc de treball. És important conèixer les situacions més comunes relacionades amb la seguretat de l'entorn de treball dels empleats per a poder així minimitzar el risc de fugida o pèrdua de dades. Consulta les recomanacions en aquest enllaç.