ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

AGÈNCIA NACIONAL DE CIBERSEGURETAT D'ANDORRA

CONSCIENCIACIÓ EN CIBERSEGURETAT

PRÀCTIQUES D'ENGINYERIA SOCIAL I ESTAFES MÉS HABITUALS

Març 2024
Document d'ús públic

1. INTRODUCCIÓ BREU I CONTEXT

1. A què anomenem «enginyeria social»?

L'enginyeria social és un tipus d'**ATAC DE SEGURETAT** mitjançant el qual els estafadors **ENGANYEN** les persones perquè els donin **ACCÉS A LA SEVA INFORMACIÓ CONFIDENCIAL** (informació personal, econòmica, financera, professional…). Els estafadors i els pirates informàtics fan servir la **PSICOLOGIA HUMANA** per dur a terme els atacs d'enginyeria social.

Els enginyers socials tenen el mateix objectiu que els pirates informàtics, però generalment se centren a **ENGANYAR** la gent, en comptes d'atacar la xarxa.

A vegades, la manera més fàcil que tenen els estafadors d'aconseguir la informació que volen és demanar-la directament a l'usuari.

2. Per què funciona i té èxit l'enginyeria social?

Per regla general, les persones solen **CONFIAR** en els altres. De fet, la clau de l'èxit de l'enginyeria social és que actua aprofitant la **CONFIANÇA** que les persones tenen en els altres. Per exemple, a la feina, pot fer que els treballadors donin informació que permeti als estafadors accedir a les seves dades i a sistemes d'informació confidencials; a casa, per exemple, que revelis dades personals i/o economicofinanceres que puguin fer servir els estafadors per robar-te la identitat.

3. Per què cal que vagis amb compte amb aquest tipus de pràctiques socials?

Els atacs d'enginyeria social suposen una **AMENAÇA** significativa per a les dades i els sistemes d'informació. Els enginyers socials poden utilitzar pràcticament tot tipus d'informació que obtinguin dels usuaris per treure'n **PROFIT**.

Compte amb els correus electrònics falsificats o que semblen legítims!

Els correus electrònics de pesca (*phishing*) que envien els ciberdelinqüents són **MALICIOSOS** i **ENGANYOSOS**, i provoquen **DANYS IRREPARABLES**, tant als usuaris individuals com a les organitzacions.

Les tàctiques que fan servir els ciberdelinqüents per crear aquests correus electrònics evolucionen constantment, cosa que fa que cada vegada sigui més difícil detectar-los.

Per evitar que els atacs de pesca per correu electrònic tinguin èxit i que les nostres dades quedin compromeses, **et recomanem que prestis molta atenció al contingut de les diapositives següents.**

2. USUARIS A QUI VAN DIRIGITS AQUESTS TIPUS D'ATACS

Les comunicacions fraudulentes, com els correus electrònics de pesca i els missatges de text o SMS falsos (*smishing*), confonen, enganyen i espanten els usuaris per tal que facin clic a l'enllaç adjunt que conté el missatge que reben. El cert és que **tothom pot ser un objectiu d'aquests atacs d'enginyeria social.** Per exemple, qualsevol treballador d'una organització disposa d'informació molt valuosa (secrets comercials, informació de clients, registres financers, dades personals dels treballadors, informació interna de l'organització...).

Un exemple de pesca per correu electrònic podria ser aquest:

De: Serveis de comptabilitat

«El teu compte s'ha bloquejat a causa d'una activitat inusual. Fes clic aquí per restablir la teva contrasenya i desbloquejar el teu compte.»

Aquests missatges semblen legítims, però contenen **PERILLS AMAGATS**: enllaços maliciosos, arxius adjunts infectats, sol·licituds de credencials d'inici de sessió, dades personals, etc.

3. ALTRES EXEMPLES D'ENGINYERIA SOCIAL

Als enginyers socials també els agrada fer ús de les **XARXES SOCIALS** per conèixer detalls personals dels usuaris en qüestió. Utilitzen la informació per accedir als seus comptes professionals i obtenir informació confidencial.

Altres **PRÀCTIQUES** habituals d'enginyeria social són les següents:

- ***Enllaços estranys en publicacions.***
- ***Finestres emergents inesperades.***
- ***Mitjans piratejats amb programes maliciosos.***
- ***Missatges oferint premis de concursos en els quals no has participat.***
- ***Perfils, pàgines o grups falsos.***
- ***Aplicacions o jocs que demanen accedir a la informació del teu perfil.***

Exemple

Un enginyer social fa una trucada amb una identitat falsa intentant establir cert nivell de credibilitat. Al final, l'estafador sol·licita informació confidencial a l'usuari.

«Hola, soc la Cristina del Departament de Tecnologia de la Informació de l'organització. Els nostres sistemes indiquen que hi ha un problema amb el teu compte de correu electrònic de l'empresa. Ens hauries de confirmar, si us plau, el teu nom d'usuari i la contrasenya perquè puguem modificar el teu compte.»

«La confiança és la base d'un atac d'enginyeria social»

- Un enginyer social es guanya la confiança portant una capsa de dolços o fent servir l'humor.
- Es presenten a la recepció i diuen que s'han oblidat la targeta d'identificació de treballador a la seva taula. Els treballadors poden deixar passar la persona a les instal·lacions.
- No tots els atacs dels enginyers socials impliquen ser sociables o utilitzar tècniques sofisticades. Els enginyers socials poden aprendre molt simplement examinant les papereres que hi ha en els centres de treball, atès que s'hi pot trobar informació com factures, directoris de telèfons, documents confidencials, missatges de correu electrònic impresos i molta més informació confidencial.
- Els enginyers socials poden trobar ordinadors o dispositius mòbils en desús a les organitzacions i utilitzar-los per recuperar informació confidencial.
- *Alguna vegada has tingut la sensació que algú mira quan introdueixes el teu pin al caixer automàtic?* Els enginyers socials usen aquesta tècnica, anomenada «mirar per sobre de l'espatlla», per veure com un usuari legítim inicia la sessió en un sistema. Memoritzen els noms d'usuari, contrasenyes i qualsevol altra informació necessària per poder-hi accedir més tard. Això es pot fer personalment o servint-se de càmeres o programes.

4. CONCLUSIONS FINALS I RECOMANACIONS

CONCLUSIONS

1. Quina diferència hi ha entre els correus electrònics de pesca i la pesca dirigida?

- Els correus electrònics de pesca general van dirigits a un **gran nombre d'usuaris**. En canvi, els correus electrònics de pesca dirigida van adreçats a un **usuari concret**.

2. Qui són les persones que creen aquest tipus de correus electrònics?

- Els usuaris que els creen tenen molts de noms: **estafadors, atacants, pirates informàtics i defraudadors.**

- Els correus de pesca estan dissenyats per enganyar les víctimes amb l'objectiu que els donin alguna cosa a canvi o els permetin accedir a algun lloc. Normalment, tot això està relacionat amb **diners, l'accés a determinades dades personals/confidencials, l'accés a xarxes/sistemes d'informació, les credencials dels usuaris**, així com amb altres tipus d'informació confidencial.

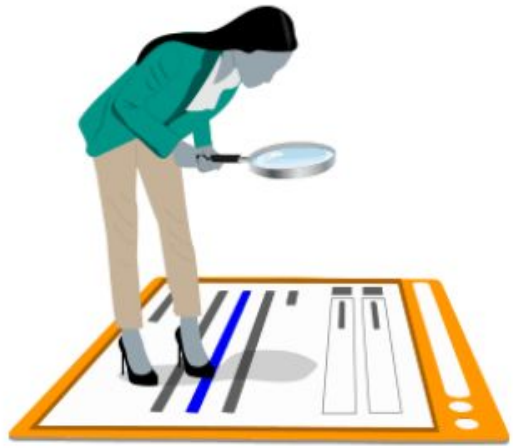
3. De qui sembla que provenen els correus electrònics?

- Un correu electrònic de pesca pot semblar que prové d'**algú que coneixes o d'una organització reconeguda i legítima**. Malgrat que siguis capaç de reconèixer un tipus de correu de pesca, és possible que NO sàpigues detectar-ne d'altres o que siguis vulnerable a aquests.

RECOMANACIONS

4. A qui van dirigits aquests correus electrònics?

- *Tothom pot ser **víctima** d'un correu electrònic de pesca. Els atacs de pesca es poden executar **en qualsevol moment** i qualsevol correu electrònic pot ser **maliciós**.*
- ***Revisa** cada correu electrònic detingudament.*
- *Presta especial atenció a l'**adreça des de la qual s'envia el correu electrònic** i comprova de qui prové abans de respondre'l.*
- *Busca **senyals d'advertiment**, com, per exemple, logotips borrosos.*
- *Ves amb compte amb les **sol·licituds de pagament inusuals**, especialment les que provenen d'altres persones de la teva organització.*
- *Si un correu electrònic sembla **sospitós**, **NO facis clic a cap enllaç**, **ni a cap arxiu adjunt.***
- *No responguis directament cap correu electrònic sospitós, ni utilitzis la informació de contacte que inclogui. Empra altres **mètodes de comunicació alternatius**, com, per exemple, fer una trucada de telèfon, enviar un missatge de text o un correu electrònic independent.*
- *Fes servir sempre **fonts oficials i llocs web de confiança** per confirmar qualsevol correu electrònic que sembli sospitós.*



Avís Legal

Aquest document conté informació pública.

El seu objectiu és la conscienciació en ciberseguretat pels ciutadans, empreses i entitats d'Andorra.