Consells per fer front als ciberatacs

Qualsevol de nosaltres podem ser víctimes d'una estafa digital. Qui no ha rebut alguna vegada un correu fraudulent suplantant la identitat d'una empresa o ha clicat per error en un anunci fals a Internet? Fins el 85% de tots els correus que s'envien al món són *spam.* En els últims anys, i especialment durant la pandèmia de la Covid-19, els *hackers* han intensificat i sofisticat els seus atacs i són moltes les estafes a les quals ens podem enfrontar: fraus telefònics, webs i anuncis falsos, atacs per correu electrònic, fraus a través de missatgeria instantània…

Conèixer les amenaces *online* que circulen per Internet i seguir unes bones pràctiques digitals és clau per no convertir-nos en víctima d'aquests atacs. Per això, CaixaBank desenvolupa accions de conscienciació dirigides tant a empleats com a clients, a través d'InfoProtect i CaixaBank Protect.

Coincidint a l'octubre amb el **mes de la conscienciació en ciberseguretat**, l'entitat ha desenvolupat una campanya per reforçar la cultura de seguretat entre empleats i clients. Durant tot el mes, CaixaBank difondrà diferents continguts relacionats amb aquesta temàtica, organitzarà sessions *online*, conferències per explicar fonaments i conceptes de ciberseguretat per prevenir ser víctima d'un frau… entre altres activitats.

Educar en seguretat digital i mostrar els riscos als quals ens enfrontem com a usuaris són alguns dels objectius de l'entitat, que ofereix consells i guies de bones pràctiques per aprendre a utilitzar els entorns digitals de manera responsable i segura.

1.Navegar per Internet amb seguretat

A l'hora de navegar per Internet hem de seguir algunes recomanacions i tenir en compte alguns consells:

-És fonamental ser previngut amb les webs que visitem i els arxius que descarreguem.

-En cas d'utilitzar connexions WiFi públiques, hem d'evitar navegar per pàgines web que demanin qualsevol tipus de dada personal o financera, usuari i contrasenyes, etc. També hem d'evitar fer compres *online* amb WiFi públiques.

-Comptar amb un antivirus actualitzat i ben configurat ens evitarà molts problemes, encara que hem de ser conscients que l'antivirus no garanteix la nostra seguretat al 100%.

Direcció de Comunicació i
Relacions Institucionals
Tel.: +34 93 404 1398
prensa@caixabank.com
www.caixabank.com/comunicacion

-Tenir correctament actualitzat el sistema operatiu i les aplicacions instal·lades és un requisit tècnic imprescindible per intentar que els ciberdelinqüents no puguin entrar als nostres equips, encara que mai és suficient.

-No accedir a llocs web de dubtosa reputació. Per verificar la legitimitat d'una web, hem de comprovar també la legitimitat del seu certificat digital, revisant que està vigent i que ha estat emès per a la pàgina web per la qual volem navegar. El "famós" cadenat no significa que la web sigui legítima, per a això és imprescindible comprovar el certificat associat.

-Cal vigilar especialment amb la 'identitat digital' que ens creguem i pujar únicament aquella informació sobre nosaltres mateixos que considerem 100% pública.

2.Claus d'accés

Les claus d'accés són personals i intransferibles. Protegeixen tota la informació del nostre entorn digital: dades personals, comptes bancaris, xarxes socials, informació confidencial, imatges i contingut de qualsevol tipus.

-És important crear contrasenyes robustes difícils d'endevinar. Per a això es recomana que tinguin com a mínim 8 caràcters, entre majúscules, minúscules, símbols i números. I sempre serà millor si no conté paraules incloses en el diccionari. Cal intentar ser creatiu i original i no posar dates personals assenyalades, el clàssic 1234 o el nom de la nostra mascota.

-Compartir les contrasenyes és una pràctica molt perillosa. La cessió de contrasenyes té un paper clau en alguns dels fraus més coneguts, com el frau per proximitat. Aquest tipus de frau es produeix quan cedim les nostres claus a un familiar, amic o conegut i aquest les utilitza per cometre un delicte o una operació fraudulenta de forma totalment il·lícita. Davant qualsevol sospita de compromís d'alguna de les nostres contrasenyes, hem de canviar-la a la menor brevetat possible.

-Per emmagatzemar i recordar-nos de totes les claus d'accés que hem generat, l'opció més segura és utilitzar gestors de contrasenyes. Aquestes aplicacions les guarden de manera xifrada i protegides amb una contrasenya única, que dona accés a totes elles.

3.Detectar correus fraudulents

El *phishing* és una de les tècniques més usades pels ciberdelinqüents per robar dades personals i bancàries. Amb l'ajuda de tècniques d'enginyeria social, el ciberdelinqüent

suplanta la identitat d'entitats, persones, marques o serveis coneguts per tractar d'enganyar les seves víctimes. El seu objectiu final sol ser els diners i/o l'obtenció d'informació sensible, generalment sol·licitant les dades a través de pàgines web falses o infectant l'equip mitjançant la descàrrega d'un *malware*. Quan rebem un nou correu, hem de formular-nos algunes preguntes:

-Qui envia el correu? És imprescindible analitzar amb detall l'adreça de correu del remitent i no fiar-nos només del nom que ens mostra. És necessari confirmar que l'adreça de correu té el domini oficial de l'empresa i no deixar-se enganyar per petits canvis a vegades gairebé imperceptibles.

-El missatge és sospitós? El ciberdelinqüent pot crear correus que inspirin confiança o curiositat, suplantant la identitat d'una empresa, d'una plataforma de vídeo en *streaming* o simplement escrivint un missatge atractiu que impulsi a clicar en un enllaç o arxiu. No s'ha de confiar en correus inesperats o en respostes que no hem sol·licitat.

-És una petició urgent? Crear sensació d'urgència és un recurs habitual entre els *hackers*. A més, el concepte de la confidencialitat també és molt usat en aquesta mena d'estafes.

Davant cap mena de dubte, és recomanable contactar amb el remitent per una altra via (telèfon…) per confirmar la legitimitat (encara que mai pel telèfon que pugui aparèixer en el correu).

4.Protegir el mòbil

Els telèfons mòbils són petits ordinadors amb una gran quantitat d'informació molt valuosa. Són dispositius que hem de tractar amb molta cura, ja que estan exposats a riscos de seguretat.

-Activar i fixar el bloqueig automàtic del telèfon. Amb aquesta senzilla mesura, ajudem a mantenir les nostres dades personals segures quant no ho estiguem usant.

-No deixar els dispositius amb el Bluetooth ni la connexió WiFi activades permanentment i evitar l'ús de connexions WiFi desconegudes.

-De manera periòdica, és convenient realitzar còpies de seguretat de la informació que conté el dispositiu mòbil, per poder recuperar-la en cas d'incidències o pèrdua.

-Actualitzar puntualment el sistema operatiu del mòbil, així com les aplicacions.

-És indispensable instal·lar alguna aplicació *antimalware*, ja que els mòbils també poden ser infectats.

5. Instal·lació d'aplicacions

Quan descarreguem aplicacions als nostres dispositius mòbils, ens sol·liciten permisos per accedir a determinades funcionalitats del dispositiu. Algunes requereixen l'estrictament necessari per complir la seva comesa, però altres intenten accedir a la nostra informació personal demanant permisos que no necessiten. Abans d'acceptar la descàrrega d'una *app*, hem de parar atenció als privilegis que sol·licita i valorar si estan justificats o són excessius.

-Revisar els permisos que ens sol·liciten. Els accessos més comuns són les crides i missatges, el calendari, els contactes, la ubicació, la càmera i galeria d'imatges i el micròfon. Són realment necessaris per al funcionament de l'*app*?

-Descarregar *apps* només de fonts oficials.

-Quan eliminem les limitacions de seguretat imposades pel fabricant del mòbil per, per exemple, evitar pagar per unes certes *apps*, estem fent un *jailbreak*, una acció gens recomanada. Amb això, eliminem les barreres de seguretat que venen de fàbrica i pot suposar-nos més problemes que beneficis.

-Tots correm el risc de ser infectats, però per protegir-nos hem d'instal·lar una *app* de seguretat en el mòbil, ja sigui Android o iOS.

-Quan vulguem descarregar-nos una aplicació, és preferible fer-ho des d'una xarxa WiFi segura. Les WiFi públiques no ofereixen cap garantia de seguretat.

6.Compres *online* segures

Cada dia més usuaris decideixen realitzar les seves compres *online*. El comerç electrònic, que ha experimentat un gran creixement en els últims anys, és còmode i pràctic, i aplicant les mesures de protecció adequades, també és segur.

-Compte amb les superofertes i els enllaços. Els preus anormalment baixos poden ser un parany per atreure a compradors incauts; per això és millor indagar altres webs i altres distribuïdors per confirmar el valor real de mercat de l'article.

-No cal utilitzar mai una connexió pública per realitzar les compres *online*, ja que no ofereixen cap garantia de seguretat.

-Prioritzar la compra a botigues que tinguin donat l'alta el servei de Comerç Electrònic Segur (CES), per exemple “Verified by Visa” o “Mastercard Secure Code”.

-Revisar periòdicament l'estat de les nostres targetes i comptes és una bona mesura de seguretat per a compradors *online*.

A més de tot l'esmentat, sempre hi ha noves vies per als ciberdelincuents, com per exemple el **frau del romanç** (tipus de frau que es produeix principalment en les aplicacions de cites o webs de contactes l'objectiu dels quals és atacar als sentiments i la confiança de la víctima com a principal basa per convèncer-la i així aconseguir enganyar-la per aconseguir estafar-li grans quantitats de diners), els **falsos anuncis de lloguer vacacional a Internet** (els ciberdelincuents utilitzen plataformes web legítimes i fiables en les quals publiquen falsos anuncis d'habitatges, a preus molt atractius i amb fotografies que atreuen l'atenció de les víctimes) o el ***vishing*** (estafes a través de crides o missatges de veu).

Amb l'objectiu de convertir-se en una font de referència per clients i usuaris, CaixaBank ha renovat l'espai de seguretat de la web pública de l'entitat. D'altra banda, cada tres mesos, l'equip de Seguretat coordina amb diferents àrees la creació de tres articles sobre temes d'actualitat relacionats amb la seguretat digital. Una altra iniciativa que duu a terme és la *newsletter* d'InfoProtect Security News, que s'envia cada 15 dies als empleats de CaixaBank amb articles i reportatges relacionats amb el món de la ciberseguretat. L'entitat també realitza cursos, sessions *online*, simulacions i altres accions per sensibilitzar als empleats sobre la importància de saber identificar correus *phishing*, entre altres temes sobre ciberseguretat.

A més de tenir en compte tots aquests consells i recomanacions, **la cautela i la màxima atenció per part nostra**, així com **saber quan sospitar** és clau per no ser víctima de ciberatacs.