Descobreix com els ciberdelinqüents es poden fer passar pel teu banc

- ***Els ciberdelinqüents utilitzen tècniques com el vishing (crides fraudulentes) per enganyar els clients i sol·licitar informació confidencial***

- ***En situacions de seguretat, l'entitat pot comunicar-se amb el client per verificar transaccions i protegir el compte contra fraus***

31 de maig de 2024

És crucial **ser cautelós a l'hora de rebre crides de números desconeguts, ja que poden ser intents de frau.** No obstant això, és cert que a vegades les entitats contacten amb els seus clients per diferents raons, com avisar al client que té una targeta sol·licitada, pendent de recollir en l'oficina, entre altres.

Una altra raó, podria ser per verificar si es realitzen gestions des de la banca *online*, confirmar per seguretat les operacions. O bé, citar al client en una entrevista presencial en l'oficina *retail*.

Aquestes **són algunes de les situacions més comunes**, en les quals **l'entitat pot contactar amb els seus clients, per proporcionar-los informació rellevant o verificar l'autenticitat de les transaccions,** per motius de seguretat. Malgrat això, sempre s'ha de mantenir precaució i verificar la legitimitat de les crides que es reben.

És possible que algú es faci passar per un empleat del banc i et cridi?

Les crides fraudulentes (conegudes com a *vishing*), són una realitat cada vegada més comuna en l'era digital. Els ciberdelinqüents estan contínuament millorant les seves tècniques per enganyar les seves víctimes.

Els ciberdelinqüents estan constantment perfeccionant les seves tècniques per enganyar els clients. Entre les més utilitzades estan, un ampli i profund **coneixement de la banca *online***, permetent-los guiar al client a través dels processos de gestió per obtenir informació personal. La **suplantació d'identitat** és una altra tècnica que utilitzen per manipular l'identificador de crides per fer creure a la víctima que la crida prové del número oficial de l'entitat. I **l'ús d'arguments convincents** per guanyar-se la confiança dels clients i oferir ajuda per resoldre problemes falsos dels seus comptes.

És fonamental recordar que, encara que la crida sembli legítima, **mai s'han de proporcionar dades personals per telèfon,** tret que el client estigui segur a qui li està proporcionant la informació.

Les estafes més recurrents entre els ciberdelinqüents són les següents:

Sol·licitar **dades confidencials** com el número de targeta o claus d'accés a la banca online, o bé instar a realitzar un pagament sota la premissa d'una suposada devolució de diners.

És habitual que **utilitzin sistemes de pagament immediats** com BIZUM o sol·licitin la **retirada de diners en efectiu d'un caixer automàtic** mitjançant un codi personal. CaixaBank permet retirar diners a través d'un caixer automàtic, mitjançant un codi personal, que ofereix grans avantatges de seguretat, però pot arribar a suposar un pretext comú per als ciberdelinqüents a l'hora de realitzar aquest tipus d'estafes.

Un pretext comú sol ser és que algú està realitzant un reintegrament en un caixer automàtic i que, per cancel·lar-lo, ha de seguir els passos indicats pels estafadors, els qui guiaran al client per completar la retirada de diners en efectiu.

CaixaBank mai sol·licitarà per telèfon, SMS o correu electrònic informació sobre contrasenyes, dades personals o claus. L'entitat treballa contínuament a proporcionar informació de seguretat als seus clients, mantenint actualitzada la secció de seguretat de la pàgina web. Davant qualsevol sol·licitud sospitosa, es recomana als clients contactar immediatament amb el número d'Atenció al Client de CaixaBank (900 40 40 90).