



A „*Futok a pénzem után*” podcast a Marketing Commando és
a K&H Bank Üzletet ide együttműködésében jött létre
a bajbajutott kisvállalkozók megsegítésére



A támadók jobban ismerik az érzelmeidet, mint te magad – így manipulálnak pillanatok alatt a „social engineering” eszközeivel

Gärtner Dávid, a K&H Bank üzleti információbiztonsági vezetője segít
felvértezni magunkat ellenük

I. Egy morzsányi info is lehet veszélyes

Bárki lehet célpont, igen, még te is! Nemcsak cégek, felsővezetők, IT-val foglalkozó személyek a jó célpontok, hanem a „kishalak” is értékesek lehetnek. Nincs olyan, hogy „*engem úgyse támadnak meg, mert nincs miért*”: Sosem tudhatod, hogy éppen mire van szüksége a csalónak! Egészen apró információkkal (például adatmorzsákkal, belső részinformációkkal, vagy akár csak hozzáférési szokások megismerésével) is tudnak dolgozni egy későbbi támadásuk során: ezekre hivatkozva hamis biztonságérzetet kelthetnek egy gyanútlan emberben. Fontos, hogy egy beszélgetés, egy óvatlan megosztás is kockázatot jelenthet egy komolyabb támadás előtt. Ezért a megelőzés első lépése a tudatosság: minden információ lehet értékes – vigyázz rá!

II. Inkább bizalmatlan légy, mint áldozat!

A bizalmas értékes, ne add oda bárkinek: a social engineeringnek pont az a lényege, hogy a bizalomra épít. Ismeretlenekkel, ha kedvesnek, segítőkésznek, udvariasnak is tűnnek, mindig légy szkeptikus, különösen, ha szokatlan kéréssel fordulnak hozzád. Ne ossz meg bizalmas adatokat, céges részleteket, szokásokat idegenekkel, különösen e-mail-ben, chat-en, telefonon. Ha valaki kérdez, mindig tedd fel magadnak a kérdést: „Miért kérdezi; valóban szüksége van rá; van joga megismerni?”.

III. Ellenőrizd a forrást, kérj te is “kettős hitelesítést”!

E-mail-ben, SMS-ben, telefonon bárki könnyen kiadja magát valaki másnak, ezért soha ne higgy vakon egy bemutatkozásnak! Ne dőlj be jól hangzó titulusoknak, fölényesen szakmai szöveghasználatnak, magabiztos hanghordozásnak vagy lendületes, tempós beszédnek. Helyette bármilyen egyeztetés során szerezz kétséget kizáróan bizonyosságot arról, hogy valóban azzal a valakivel állsz kapcsolatban, akinek az illető mondja magát. Ezért mindig kérj egy visszahívási telefonszámot és egy hivatalos e-mail címet, amin vissza tudsz jelezni. Ezeket ellenőrizd le az adott szervezetnél, és csak ha rendben találd, akkor bocsájtkozz érdemi egyeztetésbe.

Gyakran közeli hozzátartozónak, munkatársnak vagy hivatalos személynek adják ki magukat a csalók, például „banki ügyintéző; rendőr; informatikus; főnök” vagy “az ön bankjából vagyok a

...”. Mindig legyen ott a fejedben a kulcs kérdés: „*Vajon ő biztosan az, akinek mondja magát???*”

IV. Kérj időt!

Ha érzékeny vagy (és ki nem az?), akkor fajsúlyos témákban ne dönts hirtelen, időnyomás hatására. A sürgetés, stresszelés és nyomásgyakorlás az egyik legnagyobb fegyvere a csalóknak. Tipikus, és sajnos hatásos kényszerítő mondataik:

*„Azonnal cselekednie kell, különben baj lesz”
“Ha most nem lép, zárolják a számláját!”
“Erre csak most van lehetőség, különben kár éri!”*

Ha ilyet hallasz, azonnal kezdj el gyanakodni – és ha gyanakszol, lassítsd le a folyamatot:

- Tarts szünetet, vegyél pár mély levegőt – egy fontos dologban sosem szabad kapkodni! És ez ugye, egy fontos dolognak hangzik?
- Ha tudsz a beszélgetés közben koncentrálni, akkor vizsgálj meg a helyzetet és gondold át: reális ez a téma?
- Ha továbbra is bizonytalan vagy, kérj gondolkodási időt, ami után majd a megszokott csatornákon keresztül keresed meg újra a bankot. Ha tényleg a banktól hívtak, ez ellen nem lesz kifogásuk – ha mégis, akkor már le is buktattad a csalókat.
- De az se baj, ha egyszerűen csak bontod a kapcsolatot!

V. Aki ezt kéri, az tuti nem a bank...

Amit biztosra vehetsz: egyetlen bank sem fogja soha elkérni a banki belépési azonosítóidat, sem a jelszavaid, sem a PIN-kódjaid, SMS-ben kapott azonosító kódokat, sem egyéb bankkártya adataidat. Ha valaki ilyet kér, okkal feltételezheted, hogy csalóval van dolgod. Ezért ilyen esetben szakítsd meg a kapcsolatot (nyomd ki a telefonodat) és rögtön jelentsd a bankodnak az esetet!

Ugyanígy: egy banki dolgozó soha nem fog téged siettetni, sürgetni, következményekkel ijesztgetni. Aki ezt teszi, az nem a te érdekeidre vigyáz.

VI. Ami túl jó, az nem jó!

Ha valami csodás jutalommal, befektetési vagy nyerési lehetőséggel keresnek meg, ami csak neked, és főleg csak most elérhető, azonnal kezdj el gyanakodni: ilyen értékről telefonban döntést kérni tőled nem reális! Sőt: ez nem professzionális, és ezért egy bank részéről nem is lenne tisztességes. Ha pedig valamilyen rendkívül elfoglalt, magasrangú tisztségviselőnek adja ki magát a hívó, aki azt állítja, hogy azért ő keres most meg téged, mert fontos kiemelt ügyfél vagy, az még inkább gyanús...

Óvatosnak lenni menő: vigyázz magadra, vigyázz az információidra, vigyázz a pénzedre!

Az adásban szakértő vendégeink **Oroszi Eszter**, a Silent Signal Kft információbiztonsági tanácsadója és üzletág vezetője, valamint **Gärtner Dávid**, a K&H Bank üzleti információbiztonsági vezetője voltak. Tapasztalataik megosztását, a tőlük kapott hasznos információkat, tanácsaikat ezúton is köszönjük!