Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Egyre trükkösebbek az adathalász támadások

Mára az adathalászat vált a kiberbűnözők leggyakoribb módszerévé a munkahelyi és otthoni felhasználókat célozó támadások során. Az adathalász támadások hagyományosan olyan e-mailek, amelyeket a kibertámadók azért küldenek, hogy valami olyasmire vegyenek rá bennünket, amit nem szabadna megtennünk, mint például egy fertőzött csatolmány megnyitása, egy rosszindulatú hivatkozásra kattintás vagy jelszavunk megosztása. Miközben ezek a hagyományos adathalász támadások manapság is zajlanak, sok kibertámadó fejlettebb adathalász technikát alkalmaz: olyan e-maileket hoznak létre, amelyek testreszabottak, és emiatt nehezebben észlelhetők. Az adathalász átverések során a bűnözők olyan technológiákat is felhasználnak, mint például az SMS, a közösségi média oldalak, vagy akár a telefonhívások. Íme a legújabb trükkök, és hogy ezeket hogyan ismerhetjük fel.

A kiberbűnözők alaposabban felkészülnek

Az adathalász e-maileket korábban könnyebben lehetett észlelni, mivel többnyire nagyon általánosan megfogalmazott üzenetek voltak, amelyeket emberek millióinak küldtek ki, teljesen véletlenszerűen. A kibertámadóknak fogalmuk sem volt arról, hogy ki lesz az áldozat; csupán azt tudták, hogy minél több e-mailt küldenek, annál több embert csaphatnak be. Gyakran találkozhattunk ezekkel az egyszerűbb támadásokkal, amelyek „Kedves Ügyfelünk” megszólítással kezdődnek, elírásokat tartalmaznak, vagy egyszerűen túl szépeket állítanak ahhoz, hogy igazak legyenek, mint például, hogy egy nigériai herceg dollármilliókat kínál nekünk.

A mai számítógépes támadók már sokkal kifinomultabbak. Napjainkban egyre jellemzőbb, hogy előzetes kutatást végeznek az áldozatok kapcsán, ezáltal sokkal személyre szabottabb támadást indíthatnak. Ahelyett, hogy ötmillió embernek küldenének ki egyetlen e-mailt egy vállalat nevében, elküldhetik azt csupán öt embernek, és alakíthatják úgy a támadást, mintha az e-mailt az áldozat ismerőse küldte volna. A számítógépes támadók ezt a következőképpen teszik:

- felkutatják a LinkedIn profilunkat, a közösségi médiában közzétett tartalmainkat, illetve felhasználnak minden nyilvánosan elérhető, vagy a darkweben található információt.
- olyan üzeneteket készítenek, amelyek úgy tűnnek, mintha a munkahelyünk vezetőségétől, ismert munkatársaktól vagy szállítóktól származnának.
- megtudják, hogy mi a hobbink, és üzenetet küldenek, azt tettetve, hogy hasonló az érdeklődési körük.
- kiderítik, ha részt vettünk egy közelmúltbeli konferencián vagy utazáson, majd készítenek egy e-mailt, amelyben erre hivatkoznak.

A kibertámadók párhuzamosan több módszert is alkalmazhatnak egy átverés során, például SMS-t küldenek, emellett akár közvetlenül telefonon is felhívhatják az áldozatot.

Így vegyük észre ezeket a kifinomultabb adathalász támadásokat

Mivel a kibertámadók akár jelentősebb időt is szánhatnak leendő áldozataik megismerésére, jóval nehezebb lehet észrevenni az ilyen támadásokat. A jó hír az, hogy ennek ellenére képesek lehetünk felismerni ezeket, amennyiben tudjuk, hogy mit keresünk. Mielőtt bármit is tennénk egy gyanús üzenettel kapcsolatban, tegyük fel magunkak a következő kérdéseket:

1. Az üzenet fokozott sürgetés érzését kelti? Arra próbál valaki rávenni, hogy megkerüljük a szervezet biztonsági irányelveit? Valaki megpróbál hibába hajszolni? Minél nagyobb a nyomás vagy a sürgetés, annál valószínűbb, hogy egy támadásról van szó.
2. Van értelme az e-mailnek vagy üzenetnek? Reális az, hogy a cégvezető valóban SMS-ben kérne tőlünk sürgős segítséget? Valóban szüksége lehet arra a felettesünknek, hogy sietve ajándékkártyákat vásároljunk számára? Miért kérne tőlünk a bankunk olyan személyes adatokat, amelyekkel már rendelkeznie kell rólunk? Ha az üzenet furcsának vagy oda nem illőnek tűnik, lehet, hogy támadásról van szó.
3. Munkával kapcsolatos e-mailt kaptunk egy megbízható munkatárstól vagy esetleg a felettesünktől, azonban az e-mail személyes e-mail címről érkezett, például @gmail.com?
4. E-mailt vagy üzenetet kaptunk valakitől, akit ismerünk, azonban az üzenet megfogalmazása, hangneme vagy az aláírás hibás és szokatlan?

Ha egy üzenet furcsának vagy gyanúsnak tűnik, az támadás lehet. Ha meg szeretnénk győződni arról, hogy egy e-mail vagy üzenet valódi-e, az egyik lehetőség, hogy felhívjuk az üzenetet küldő személyt vagy szervezetet egy megbízható telefonszámon.

A legjobb védekezés mi magunk vagyunk. Használjuk a józan eszünket!

A szerzőről

Phil Hoffman részben visszavonult informatikai tanácsadó, 40 éves tapasztalattal, aki az infrastruktúrákra és a biztonságra összpontosít. Az OUCH! hosszútávú munkatársa és szerkesztője, szenvedélye a technológia, a kerékpározás és a fotózás.

Források

Pszichológiai manipulációs támadások: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Top három átverés: https://www.sans.org/newsletters/ouch/top-three-social-media-scams/
Üzenetküldéses/SMS csalások: https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks/
Vishing - Telefonos csaló hívások: https://www.sans.org/newsletters/ouch/vishing/
Nyílt forrású információszerzés: https://www.sans.org/security-awareness-training/resources/search-yourself-online/

A fordítást készítette: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)