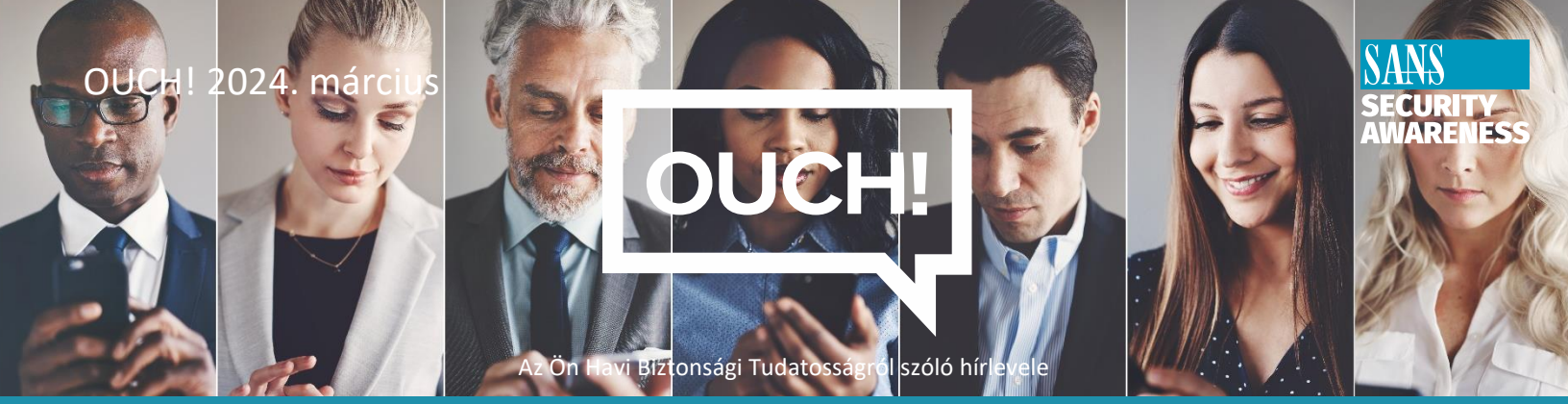

Üzenetküldés: mit tegyünk és mit ne

Áttekintés

Az üzenetküldés elsődleges kommunikációs mód a személyes és szakmai életünkben egyaránt. Azonban ha biztonságos üzenetküldésről van szó, gyakran mi vagyunk saját magunk legnagyobb ellensége. Ismerjük meg a leggyakoribb hibákat, és azt, hogy hogyan kerülhetjük el ezeket a mindennapok során!

Automatikus kitöltés

Az automatikus kitöltés számos üzenetküldő alkalmazás alapvető funkciója. Miközben beírjuk a címzett nevét, az alkalmazás automatikusan kiválaszthatja azt. Ez a funkció hibákhoz vezethet, különösen, ha több ismerősünk hasonló névvel rendelkezik. Előfordulhat, hogy szenzitív információt tartalmazó üzenetet szeretnénk küldeni egy munkatársunknak, de az üzenetet véletlenül másnak, például a lányunk edzőjének címezzük, akinek történetesen nagyon hasonló neve van. Az üzenetek elküldése előtt érdemes többször ellenőrizni a címzett teljes nevét, hogy valóban annak küldjük, akinek szánjuk az üzenetet.

Válasz a csoportos üzenetekre

A csoportos csevegés egy másik gyakran használt funkció, de mielőtt válaszolnánk, mindig nézzük meg, hogy kiknek válaszolunk! Amikor egy teljes csoportnak küldünk választ, bizonyosodjunk meg arról, hogy az üzenetünk mindenki számára elfogadható! Másik gyakori hiba, hogy véletlenül az egész csoportnak válaszolunk egy adott személy helyett. Szánjunk elég időt a válaszra: Ellenőrizzük még egyszer, mielőtt megnyomjuk a küldés gombot!

Indulatok

Sose küldjünk üzenetet haragos, dühös vagy érzelmileg feldúlt állapotban! Egy ilyen üzenet sok kárt okozhat a jövőben, akár egy barátságba vagy a munkánkba is kerülhet. Inkább várjunk pár percet, és nyugodt állapotban rendezzük a gondolatainkat! Ha egyszerűen le *kell* vezetni a frusztrációnkat, nyissunk meg egy új üzenetet, de ne válasszuk ki a címzettet! Írjuk le pontosan, hogy mit érzünk, majd tegyük félre egy kis időre az eszközünket! Esetleg készítsünk egy csésze teát, vagy sétáljunk egyet! Amikor pedig visszatérünk, töröljük az üzenetet, és kezdjük elölről! Valószínűleg sokkal nyugodtabb lelkiállapotban leszünk. A hatékonyabb kommunikáció érdekében fontoljuk meg a telefonos vagy személyes beszélgetést! Néha nehéz lehet megállapítani egy szöveges üzenet alapján a küldő szándékát.

Magánszféra

A hagyományos SMS-üzenetek adatvédelmi szempontból aggályosak; küldés után elveszítjük a kontrollt az üzenet felett. Az üzenetek ugyanis továbbíthatók, nyilvánosan közzétehetők, képernyőképként megoszthatók, vagy bírósági végzés miatt nyilvánosságra hozhatóak. A privát kommunikáció érdekében hívjuk fel az érintettet! Végül, ha munkahelyi eszközünket használjuk üzenetküldésre, ne feledjük, hogy a munkáltatónak felhatalmazása lehet a munkahelyi eszközökön lévő üzenetek figyelésére és esetleges elolvasására!

Rosszindulatú üzenetek

Az e-mailekhez hasonlóan a csalók bármilyen üzenetben megpróbálhatnak bennünket átverni, becsapni vagy megtéveszteni. Az üzenetek rosszindulatú hivatkozásokat is tartalmazhatnak, a csalók ezek megnyitására szeretnének rávenni bennünket, illetve gyakori, hogy személyes információt kérnek tőlünk vagy arra akarnak rávenni, hogy hívjuk fel egy adott telefonszámot. Gondolkozzunk el, hogy kaptunk-e már valaha olyan furcsa szöveges üzenetet, amiben megszólításként annyi szerepelt, hogy: „Szia”, és azon töprengtünk, hogy miről van szó pontosan? Valószínűleg egy csaló keresett minket, aki beszélgetést szeretne kezdeményezni. Gyakran ez a romantikus átverés kezdete. Ha furcsa vagy gyanús üzeneteket kapunk eszközünkre, egyszerűen töröljük azokat!

Ahogy az e-maileknél, a szöveges üzeneteknél is lehetséges a forrás meghamisítása. Győződjünk meg arról, hogy ismerjük annak a személynek a kilétét, aki SMS-t küld nekünk, mielőtt bármilyen személyes adatot megosztanánk, különösen akkor, ha nem mi kezdeményeztük a beszélgetést! Ezenkívül letilthatunk minden kéretlen vagy gyanús telefonszámot vagy fiókot, amely üzenetet próbál küldeni nekünk.

Biztonságos

Győződjünk meg arról, hogy bármilyen üzenetküldő alkalmazást is használunk, az naprakész és a legújabb biztonsági funkciókkal rendelkezik! A fokozott biztonság és adatvédelem érdekében fontoljuk meg a biztonsági fókuszú üzenetküldő alkalmazások használatát, mint például a Signal!

A szerzőről

Michele Tomasic, a Women in Cybersecurity (WiCyS) szervezet helyettes igazgatója, dinamikus vezető, elkötelezett a nők előrejutása mellett a kiberbiztonság területén. Kiemelkedő tapasztalattal rendelkezik a személyzeti- és operatív vezetés területén, szakértelmét az inkluzivitás, a sokszínűség előmozdítására és a nők szerepének megerősítésére használja a kiberbiztonsági szakmában.

Források

Mobileszközök biztonságos használata: https://www.sans.org/newsletters/ouch/securely-using-mobile-apps/
Így szabaduljunk meg a mobilkészülékeinktől: https://www.sans.org/newsletters/ouch/disposing-mobile-devices/
A leggyakoribb e-mailezési hibák elkerülése: https://www.sans.org/newsletters/ouch/avoid-the-most-common-email-mistakes/
Signal: https://signal.org

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