SANS SECURITY AWARENESS

OUCH!

Mesečni bilten za podizanje svesti o bezbednosti informacija

Ne dajte se upecati

Uvod

Servisi za razmenu elektronske pošte i drugih elektronskih poruka (poput Skype, Twitter ili Snapchat poruka) su jedan od osnovnih vidova komunikacije u današnje vreme. Koristimo ih ne samo za svakodnevne poslovne potrebe nego i da ostanemo u kontaktu sa prijateljima i članovima porodice. Kako veliki broj ljudi širom sveta zavisi od ovih tehnologija, one su postale i jedan od glavnih načina za napad koje koriste sajber kriminalci, i to u vidu metode poznate pod nazivom pecanje. U ovom tekstu saznaćete šta je pecanje i kako da uočite i zaustavite ove napade, bilo da ste na poslu ili kod kuće.

Šta je pecanje

Pecanje je vrsta napada u kojem se koristi elektronska pošta ili poruke koje treba da vas navedu da uradite nešto što ne bi trebalo, na primer da kliknete na maliciozni link, odate vašu lozinku ili otvorite maliciozan prilog iz mejla. Sajber kriminalci vredno rade na kreiranju uverljivih poruka koje će uticati na vaše emocije, stvoriti osećaj hitnosti ili pobuditi vašu radoznalost. Poruke mogu izgledati kao da su stigle od nekoga koga poznajete, kao što je prijatelj ili kompanija čije usluge često koristite. Može im biti dodat i logo vaše banke ili se adresa pošiljaoca može izmeniti tako da poruka deluje još uverljivije. Sajber kriminalci ovakve poruke šalju milionima ljudi. Oni ne znaju ko će zagristi mamac, ali znaju da će što više poruka pošalju, imati više uspeha.

Kako da se zaštitite

U većini slučajeva bezbedno je da otvorite i pročitate telo mejla ili poruke. Da bi napad pecanjem bio uspešan, loši momci će pokušati da vas prevare da uradite još nešto. Sreća je što postoje načini da prepoznate da je poruka zapravo napad, a ovde navodimo najuspešnije:

- Poruka stvara osećaj velike hitnosti i zahteva se da što pre preduzmete akciju da se ne bi desilo nešto loše, poput zatvaranja naloga ili odlaska u zatvor. Napadač vas požuruje kako biste nepromišljeno napravili grešku.
- Poruka vas ubeđuje da zaobiđete ili zanemarite pravila ili procedure koje imate na poslu.
- Pobuđuje se radoznalost ili saopštava nešto što je suviše dobro da bi bilo istinito (ne, niste dobitnik na lutriji).
- Koristi se generičko obraćanje poput “Poštovani korisniče”. Većina kompanija ili prijatelja će vam se obratiti po imenu.

- Zahteva se dostavljanje osetljivih informacija, poput broja vaše platne kartice, lozinke ili neke druge informacije koja bi trebalo da je već poznata pošiljaocu.
- U poruci stoji da je šalje zvanična organizacija, ali poruka sadrži gramatičke ili slovne greške ili je poslata sa neke privatne mejl adrese i domena poput @gmail.com.
- Poruka izgleda kao da dolazi sa adrese kojoj se može verovati (poput mejl adrese vašeg šefa) ali se uočava da Reply-To adresa vodi na privatni nalog elektronske pošte nekoga drugog.
- Poruka je stigla od nekoga koga poznajete, ali način obraćanja i upotrebljene reči uopšte ne zvuče kao da ih je pisala ta osoba. Ako imate ovakve sumnje, pozovite pošiljaoca telefonom da biste proverili da li je zaista poslao tu poruku. Sajber kriminalci veoma lako mogu kreirati poruku koja izgleda kao da ju je poslao vaš prijatelj ili kolega.

Na kraju, zdrav razum je vaša najbolja odbrana. Ako mejl ili poruka deluju čudno, sumnjivo ili previše dobro da bi bili istiniti, moguće je da se radi o pecanju.

Verzija na srpskom

Telekom Srbija kao društveno odgovorna telekomunikaciona kompanija pomaže prevođenje i distribuciju ovog biltena kako bi se unapredila svest korisnika informaciono-komunikacionih tehnologija o bezbednosti informacija.

Gost urednik

Tonia Dadli se od 2011. godine bavi razvojem i implementacijom programa za unapređenje svesti o bezbednosti informacija, a njen program za unapređenje svesti o sajber pecanju je i nagrađen. Možete je pronaći na www.linkedin.com/in/toniadudley.

Dodatne informacije

Socijalni inženjering:	https://www.sans.org/u/Cb1
Pomozite drugima da budu bezbedni:	https://www.sans.org/u/Cb6
E-mail – šta treba, a šta ne treba raditi:	https://www.sans.org/u/Cbg
CEO Fraud:	https://www.sans.org/u/Cbl
OUCH! prevodi i arhive:	https://www.sans.org/u/Cbq

Licenca

Redakcija: Walt Scrivens, Phil Hoffman, Кэти Клик, Cheryl Conley | Preveli: Dragan Ristić i Gordana Živanović