Mėnesinis informacinio saugumo naujienlaiškis kompiuterių naudotojams

OUCH!

ŠIAME LEIDIME…

- Apžvalga
- Sukčiavimas
- Savisauga

Sukčiavimas

Apžvalga

Elektroninis paštas tai vienas iš pagrindinių mūsų bendravimo būdų. Jį kasdien naudojame ne tik darbo paskirčiai, bet ir norėdami palaikyti ryšį su savo draugais ir šeima. Be to, šiais laikais elektroniniu paštu dauguma įmonių teikia internetines paslaugas, tokias kaip internetu įsigytų pirkinių patvirtinimas ar banko išrašų patikrinimas. Kadangi nuo elektroninio pašto priklauso tiek daug žmonių visame pasaulyje, jis tapo vienu iš pagrindinių kibernetinių nusikaltėlių naudojamų puolimo būdų. Šiame naujienlaiškyje paaiškinsime apie sukčiavimą (angl. phishing) – dažnai elektroniniu paštu naudojamą puolimų būdą bei patarsime, kokių galite imtis veiksmų, norėdami saugiai naudotis elektroniniu paštu.

Kviestinis redaktorius

Dr. Lance Hayden yra įmonės „Berkeley Research Group" vykdomasis direktorius. Taip pat jis dirba specialistu saugumo kultūros ir elgesio srityje bei yra „McGraw-Hill" leidyklos išleistos knygos „Į žmones orientuotas saugumas: jūsų įmonės saugumo kultūros transformavimas" (angl. "People-Centric Security: Transforming Your Enterprise Security Culture") autorius. Daugiau informacijos apie jį rasite apsilankę adresu: **www.linkedin.com/in/drhayden**.

Sukčiavimas

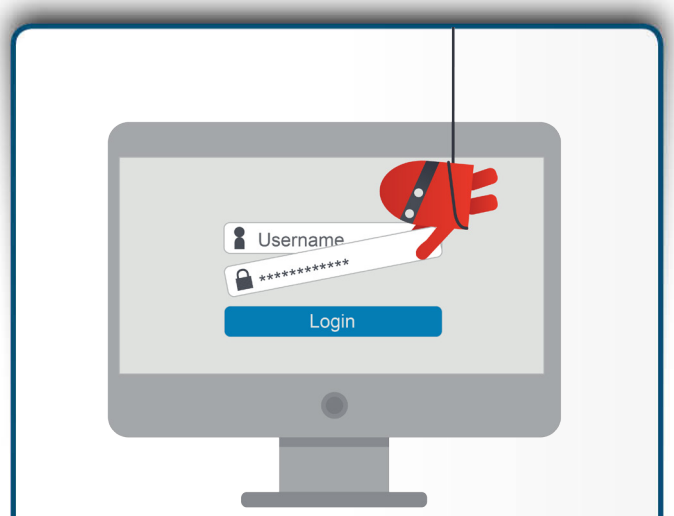
Sukčiavimas (angl. phishing) reiškia elektroniniu paštu arba socialinės žiniasklaidos internetinių svetainių žinutėmis naudojamą puolimą, kuriuo asmuo yra apgaulės arba viliojimo būdu priverčiamas atlikti kokius nors veiksmus, pavyzdžiui, paspausti pateiktą nuorodą arba atsidaryti pridėtą priedą. Tapus tokio puolimo auka, jūs rizikuojate prarasti itin konfidencialią informaciją ir/arba užkrėsti savo kompiuterį. Sukčiai sunkiai dirba, kad jų apgaulingi elektroniniai laiškai atrodytų įtikinamai. Pavyzdžiui, gali atrodyti, kad jų siunčiamas elektroninis laiškas atėjo iš jums žinomo siuntėjo tokio, kaip jūsų draugas ar patikima įmonė, kurios paslaugomis dažnai naudojatės. Jie netgi panaudos jūsų banko logotipus arba nurodys tokį elektroninio pašto adresą, kuris leis jums manyti, kad pranešimas yra teisėtas. Tuomet sukčiai šiuos apgaulingus laiškus išsiuntinės milijonams žmonių. Jie nežino, kas taps auka, tačiau supranta, kad kuo daugiau elektroninių laiškų jie išsiųs, tuo didesnė tikimybė, jog jiems pasiseks. Sukčiavimas yra panašus į tinklo užmetimą žvejojant – jūs nežinote, kas užkibs, tačiau kuo didesnis tinklas, tuo daugiau žuvų sugausite. Štai keletas būdų, kuriuos sukčiai naudoja, siekdami apgaulingais elektroniniais laiškais gauti to, ko nori.

- **Informacijos paieška**: sukčiaus tikslas yra surinkti tokią jūsų asmeninę informaciją, kaip slaptažodžiai, kredito kortelių numeriai ar banko duomenys. Norėdamas tai padaryti, jis jums elektroniniu paštu atsiųs nuorodą, kuri jus nukreips į teisėtai atrodančią internetinę svetainę. Šioje svetainėje jūsų bus paprašyta nurodyti savo sąskaitos informaciją arba asmeninius duomenis. Tačiau iš tiesų, ši internetinė svetainė bus suklastota, todėl

Sukčiavimas

bet kokia jūsų suvesta informacija keliaus tiesiai į sukčiaus rankas.

- **Kenkėjiškos nuorodos**: sukčiaus tikslas yra perimti jūsų įrenginio valdymą. Norėdamas tai padaryti, jis jums elektroniniu paštu atsiųs nuorodą. Paspaudę nuorodą, būsite nukreipti į internetinę svetainę, kuri bandys įsilaužti į jūsų įrenginį ir jeigu tai pavyks, tuomet jūsų sistema bus užkrėsta.
- **Kenkėjiški priedai**: sukčiaus tikslas yra toks pats – užkrėsti jūsų įrenginį ir perimti jo valdymą. Tačiau vietoj nuorodos, sukčius jums elektroniniame laiške prisegs priedą, pavyzdžiui, „Word“ programos dokumentą. Atidarius priedą bus paleista programa, kuri sukčiui perleis jūsų sistemos valdymą.
- **Apgaulingi laiškai (angl. scams)**: už kai kurių apgaulingų laiškų slepiasi ne kas kita, kaip skaitmeniniai sukčiai. Jais stengiamasi jus apkvailinti, pranešant, jog laimėjote loterijoje, apsimetant pinigų prašančia labdaros organizacija arba asmeniu, kuris prašo pagalbos persiųsti milijonus dolerių. Jei į kurį nors iš šių laiškų atrašysite, jie jums atsakys, jog pirmiausiai turite sumokėti už jų paslaugas arba prisijungti prie savo banko sąskaitos, taip iš jūsų išviliodami pinigus.



Geriausia jūsų gynyba yra sveikas protas. Jei el. laiškas ar žinutė yra keista, įtartina arba per gera, kad būtų teisinga – tai panašu į sukčiavimo ataką.

Savisauga

Beveik visais atvejais, perskaičius elektroninį laišką arba žinutę nieko blogo nenutiks. Tam, kad sukčiavimo planas pavyktų, sukčiams reikia jus priversti imtis kokių nors veiksmų. Laimei, yra keletas užuominų, nusakančių, jog žinutė yra apgaulinga. Pateikiame keletą dažniausiai pasitaikančių:

- Elektroniniame laiške jaučiamas skubotumas, reikalaujama „nedelsiant imtis veiksmų“ prieš nutinkant blogam įvykiui, pavyzdžiui, liepiama uždaryti savo sąskaitą. Sukčiai nori jus paskubinti tam, kad negalvodami priimtumėte klaidingą sprendimą.
- Jūs gaunate elektroninį laišką su priedu, kurio nesitikėjote arba elektroniniame laiške jus bandoma įtikinti atidaryti priedą. Pavyzdžiui, laiške nurodoma, kad priede pateikiami duomenys apie nepraneštus atleidimus iš darbo, darbuotojo atlyginimo informacija arba laiškas iš mokesčių inspekcijos, teigiantis, jog esate traukiamas baudžiamojon atsakomybėn.
- Vietoj jūsų vardo, šiuose elektroniniuose laiškuose yra įprastai naudojamas kreipinys „Gerb. kliente“. Dauguma su jumis bendraujančių įmonių arba draugų žino jūsų vardą.

Sukčiavimas

- Elektroniniame laiške prašoma atskleisti itin konfidencialią informaciją, pavyzdžiui, jūsų kredito kortelės numerį ar slaptažodį.
- Elektroniniame laiške teigiama, jog jis yra atsiųstas iš oficialios organizacijos, tačiau tekste yra gramatinių arba rašybos klaidų, naudojamas asmeninis elektroninio pašto adresas, pavyzdžiui, @gmail.com, @yahoo.com arba @hotmail.com.
- Nuoroda atrodo keistai arba neoficialiai. Vienas iš patarimų yra užvesti pele virš nuorodos ir palaukti, kol pasirodys iškylantis langas, rodantis, kur iš tiesų būsite nukreipti. Jei užvedus virš elektroninio laiško nuorodos iškylantis langas nepasirodys, tuomet nuorodos nespauskite. Mobiliuosiuose įrenginiuose iškylantis langas pasirodo ant nuorodos ilgiau palaikius pirštą. Tačiau dar saugiau būtų tiesiog elektroniniu paštu gautą nuorodą nukopijuoti ir įkelti į savo naršyklę arba suvesti teisingą nuorodą.
- Jūs iš kieno nors gaunate žinutę, tačiau kalbėjimo tonas arba žodžių parinkimas neskamba taip, kaip kalba jums pažįstamas asmuo. Jei jaučiatės įtartinai, paskambinkite siuntėjui(-ai) ir įsitikinkite, kad tai siuntė tikrai jis/ji. Kibernetiniams nusikaltėliams lengva susikurti elektroninio pašto adresą, kuris yra panašus į jūsų draugo arba bendradarbio.

Jei manote, kad elektroninis laiškas arba žinutė yra apgaulingi, tiesiog ištrinkite juos. Galiausiai, geriausia jūsų gynyba yra naudotis sveiku protu.

SUŽINOKITE DAUGIAU

Prenumeruokite kas mėnesinį OUCH! naujienlaiškį, gaukite prieigą prie archyvų, sužinokite daugiau apie SANS saugumo sprendimus apsilankę http://www.securingthehuman.org.

Šaltiniai

Socialinė inžinerija:	https://www.securingthehuman.org/ouch/2014#november2014
5 žingsniai išliktu saugiu:	https://www.securingthehuman.org/ouch/2014#october2014
Įsilaužė, ką daryti toliau?:	https://www.securingthehuman.org/ouch/2014#may2014
OnGuard tinkle:	https://www.onguardonline.gov/phishing
SANS dienos saugumo patarimas:	https://www.sans.org/tip_of_the_day.php

Licencija

Redaktoriai: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Lietuvišką vertimą finansavo „Perlo“ įmonių grupė.

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus