OUCH! | 2015.gada decembris

Ikmēneša biļetens par informācijas tehnoloģiju drošību datoru lietotājiem

OUCH!

ŠAJĀ NUMMURĀ …

Pikšķerēšana

Ievads

E-pasts ir viens no komunikācijas pamata veidiem. Mēs to izmantojam katru dienu darba vajadzībām, kā arī lai sazinātos ar draugiem un ģimeni. Papildus, e-pasts šobrīd ir veids, kā vairums uzņēmumu nodrošina tiešsaistes pakalpojumus, piemēram, tiešsaistes pirkuma apstiprinājums vai bankas konta pārskats. Ņemot vērā to, ka daudzi cilvēki visā pasaulē paļaujas uz e-pastu, tas ir kļuvis par vienu no galvenajām kiber noziedznieku uzbrukuma metodēm. Šajā izdevumā mēs izskaidrojam pikšķerēšanu - bieži sastopamu e-pasta uzbrukumu metodi un pasākumus, ko varat veikt, lai e-pastu izmantotu droši.

Viesredaktors

Dr. Lance Hayden ir Berkeley Research Group izpilddirektors. Eksperts drošības kultūrā un uzvedībā, viņš ir arī McGraw-Hill izdotās grāmatas People-Centric Security: Transforming Your Enterprise Security Culture. Jūs varat viņu atrast **www.linkedin.com/in/drhayden**.

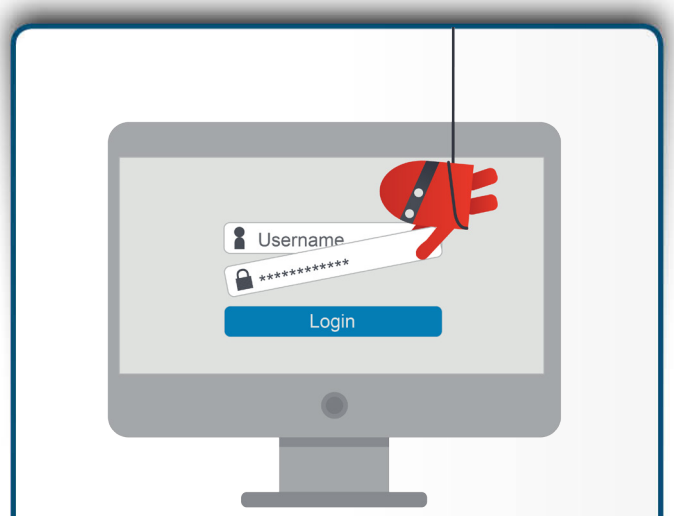
Pikšķerēšana

Pikšķerēšana nozīmē uzbrukumu, kas izmanto e-pastu vai ziņojumu pakalpojumu, piemēram, sociālo tīklu vietnē, kas ievilina vai apmāna Jūs, lai Jūs veiktu kādu darbību, piemēram, uzklikšķinātu uz saites vai atvērtu e-pasta pielikumu. Kļūstot par šāda uzbrukuma upuri, Jūs riskējat ar datora infekciju un Jūsu sensitīvās informācijas zādzību. Uzbrucēji ļoti cenšas, lai padarītu pikšķerēšanas uzbrukumus pārliecinošus. Piemēram, viņi padarīs e-pastu līdzīgu tādam, ko varētu sūtīt Jums pazīstams cilvēks vai uzņēmums, kam Jūs uzticaties un bieži izmantojat. Viņi pat pievienos Jūsu bankas logo, vai viltos e-pasta sūtītāja adresi, lai padarītu ziņojumu ticamāku. Uzbrucēji izsūta šādus pikšķerēšanas e-pastus miljoniem cilvēku. Viņi nezin, kurš kritīs par upuri šiem e-pastiem, viss ko viņi saprot ir jo vairāk e-pasti tiks izsūtīti, jo lielāka veiksmes iespēja. Pikšķerēšanu var pielīdzināt zvejošanai ar tīklu - Jūs nezināt, ko Jūs noķersiet, bet jo lielāks tīkls, jo vairāk zivju ir iespējams noķert. Ir vairāki veidi, kādos uzbrucēji izmanto pikšķerēšanu, lai iegūtu to, ko vēlas.

- **Informācijas ievākšana**: Uzbrucēja mērķis ir iegūt Jūsu personīgo informāciju, piemēram, paroles, kredītkaršu numurus vai bankas informāciju. Lai to izdarītu, viņi nosūta Jums e-pastu ar saiti, kas izskatās pareiza. Attiecīgā mājas lapa Jums prasa ievadīt konta informāciju vai personas datus. Taču mājas lapa ir viltota, un jebkāda informācija, ko Jūs ievadiet nokļūst tieši pie uzbrucēja.

Pikšķerēšana

- **Kaitīgas saites**: Uzbrucēja mērķis ir pārņemt kontroli par Jūsu iekārtu. Lai to izdarītu, viņi nosūta Jums e-pastu ar saiti. Ja Jūs nospiežat šo saiti, tā aizved Jūsu uz mājas lapu, kas īsteno tādu uzbrukumu Jūsu ierīcei, kurš sekmīga iznākuma gadījumā inficē Jūsu iekārtu.
- **Kaitīgi e-pasta pielikumi**: Uzbrucēja mērķis ir tāds pats kā iepriekš - inficēt un pārņemt kontroli pār Jūsu iekārtu. Taču e-pastā tiek nosūtīta nevis saite, bet pievienots inficēts fails, piemēram, Word dokuments. Atverot šo pielikumu, notiek uzbrukums, kas potenciāli var pārņemt kontroli pār Jūsu sistēmu.
- **Krāpniecība**: Daži pikšķerēšnas e-pasti ir nekas vairāk kā krāpniecības mēģinājumi, kas pārvērsti digitālā formā. Viņi mēģina Jūs apmānīt sakot, ka esat laimējis loterijā, izliekoties par labdarības organizāciju, kas aicina ziedot vai lūdz palīdzību pārvietot miljonus dolāru. Ja Jūs atbildiet uz kādu no šiem e-pastiem, viņi parasti lūdz maksājumu par pakalpojumu vai piekļuvi Jūsu bankas kontam, tā mēģinot izkrāpt Jūsu naudu.



Jūsu labākā aizsardzība ir veselais saprāts. Ja e-pasta adrese ir dīvaina, aizdomīga vai par labu, lai būtu patiesība, tā var izrādīties pikšķerēšanas uzbrukums.

Kā aizsargāt sevi

Vairumā gadījumu e-pasta atvēršana un izlasīšana nav nedroša. Lai pikšķerēšanas uzbrukums izdotos, ļaundariem jāmēģina Jūs apmānīt, lai veiktu kādu darbību. Par laimi, uzbrukumiem ir zināmas pazīmes, visbiežāk sastopamās ir šādas:

- E-pasts rada steidzamības sajūtu, aicinot rīkoties nekavējoties pirms noticis kaut kas slikts, piemēram, Jūsu konts tiek slēgts. Uzbrucējs vēlas Jūs pamudināt rīkoties bez domāšanas.
- Jūs saņemiet e-pastu ar pielikumu kas ir negaidīts vai e-pasts iekārdina Jūs atvērt pielikumu. Piemēri varētu būt informācija par nepaziņotām atlaišanām uzņēmumā, kolēģu algas informācija, vai valsts iestāžu informācija par pārkāpumiem.
- E-pasta uzruna noformēta vispārīgi - “Dārgais Klient”. Vairums draugu, paziņu vai uzņēmumu, kas ar Jums sazinās, zina Jūsu vārdu un uzvārdu.
- E-pasts prasa sensitīvu informāciju, piemēram, paroles vai kredītkaršu datus.
- E-pasts it kā nāk no oficiālas iestādes, bet tajā ir daudz gramatikas kļūdu, vai netiek izmantota oficiālā e-pasta

Pikšķerēšana

adrese, bet publiski pieejamie e-pasta pakalpojumu sniedzēji kā @gmail.com, @yahoo.com vai @hotmail.com.

- Saite izskatās neparasta vai neoficiāla. Viens padoms ir novietot peles kursoru, līdz parādās uzlecošais logs, kas parāda, kur patiesībā ved saite. Ja e-pastā rakstītā saite nesakrīt ar to, kas norādīta uzlecošajā logā, neklikšķiniet uz tās. Mobilajās iekārtās piespiežot un turot pirkstu uz saites var redzēt tādu pašu uzlecošo logu. Vēl drošāk ir nokopēt saites adresi un tad ielīmēt to pārlūkā vai pārrakstīt pareizo adresi.
- Jūs saņemat ziņu no kāda, ko Jūs pazīstat, bet tās stils neatbilst šim cilvēkam. Ja neesat pārliecināts, piezvaniet sūtītājam, lai apstiprinātu vai viņš ir sūtījis šo ziņu. Kiber noziedzniekam ir vienkārši izveidot e-pastu, kas izskatās it kā būtu nācis no drauga vai kolēģa.

Ja uzskatāt, ka e-pasts ir pikšķerēšanas uzbrukums, vienkārši izdzēsiet to. Parasti veselais saprāts ir Jūsu labākā aizsardzība.

UZZINIET VAIRĀK

Parakstieties uz OUCH! - ikmēneša biļetenu par informācijas tehnoloģiju drošību datoru lietotājiem, apmeklējiet OUCH! arhīvu, uzziniet vairāk par SANS informācijas tehnoloģiju drošības risinājumiem, apmeklējot tīmekļa vietni http://www.securingthehuman.org.

CERT.LV ir Latvijas Republikas Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. CERT.LV misija ir veicināt informācijas tehnoloģiju drošību Latvijā. Uzziniet vairāk https://www.cert.lv vai sekojiet mums Twiterī @certlv.

Resursi

Sociālā inženierija:	https://www.securingthehuman.org/ouch/2014#november2014
Pieci soļi drošībai:	https://www.securingthehuman.org/ouch/2014#october2014
Mani uzlauza, ko tagad?:	https://www.securingthehuman.org/ouch/2014#may2014
OnGuard tiešsaistē:	https://www.onguardonline.gov/phishing
SANS dienas drošības ieteikums:	https://www.sans.org/tip_of_the_day.php

License

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Tulkojums: Edgars Tauriņš