Buletini mujor për vetëdijësimin mbi sigurinë e përdoruesve të kompjuterëve

OUCH!

NË KËTË NUMËR..

Phishing

Përmbledhje

Emaili është një nga rrugët kryesore të komunikimit tonë. Ne e përdorim emailin jo vetëm në punë, por edhe për të kontaktuar me miqtë dhe familjarët tanë. Për më tepër, shumë kompani përdorin emailin për të ofruar shërbimet e tyre, si për shembull konfirmimi I blerjes që bëni në internet apo shërbimet bankare përmes internetit. Meqë ka kaq shumë njerëz në botë që përdorin emailin si mjet kryesor komunikimi dhe pune, ai është shndërruar edhe në një nga metodat kryesore të sulmeve kibernetike. Në këtë buletin ne shpjegojmë phishing, një metodë e zakonshme e sulmimit të emailit, dhe hapat që mund të merrni për ta përdorur emailin në mënyrë të sigurtë.

Botuesi i ftuar

Dr. Lance Hayden është Drejtor Menaxherial i Berkeley Research Group. Ekspert në fushën e kulturës dhe sjelljes së sigurisë, ai është autori i People-Centric Security: Transforming Your Enterprise Security Culture from McGraw-Hill (Siguria e përqëndruar te njerëzit: Të transformoni kulturën e sigurisë në sipërmjarrjen tuaj nga McGraw-Hill) Mund ta gjeni në: **www.linkedin.com/in/drhayden**.

Phishing

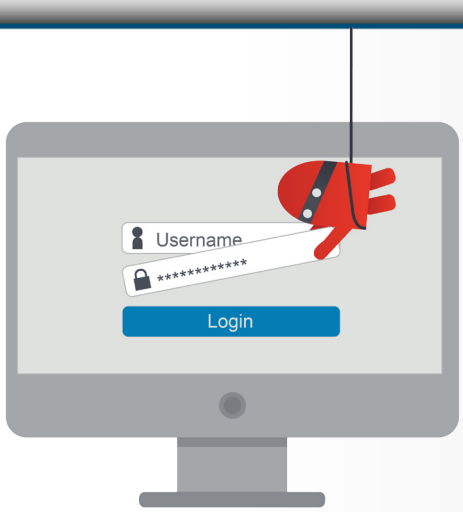
Phishing i referohet një sulmi që përdor emailin ose një shërbim për dërgimin e mesazheve, si për shembull në mediat sociale, dhe që ju mashtron duke ju bindur të kryeni një veprim si të klikoni një link ose të hapni një dokument të bashkëlidhur. Kur bëheni viktimë e një sulmi të tillë, juve mund t'ju vidhen të dhëna shumë sensitive dhe/ose mund t'ju infektohet kompjuteri. Sulmuesit përpiqen që t'i bëjnë emailet e tyre phishing bindëse. Për shembull, ata bëjnë që emaili të duket sikur është dërguar nga një miku juaj ose kompani e besuar që ju e përdorni shpesh. Ata madje përdorin logon e bankës ose falsifikojnë adresën e emailit që mesazhi të duket sa më i besuar. Sulmuesit ua dërgojnë këto emaile phishin miliona njerëzve. Ata nuk e dinë se kush do jetë viktimë, kështu që sa më shumë emaile të dërgojnë aq më shumë mundësi kanë për sukses. Phishing është i ngjashëm me përdorimin e një rrjete peshkimi. Ju hidhni rrjetën pa e ditur cfarë peshku do kapni, por sa më e madhe rrjeta aq më shumë peshq do kapni. Sulmuesit përdorin phishing në disa mënyra për të arritur qëllimin e tyre.

- **Marrin informacion**: Qëllimi i sulmuesit është të vihet në dijeni të informacioneve tuaja personale, si fjalëkalimet, numrin e kartës së kreditit, apo të dhënat bankare. Për këtë qëllim ata dërgojnë një email që ju drejton tek një faqe interneti e cila duket e ligjshme. Kjo faqe kërkon që ju të jepni të dhënat e llogarisë suaj apo të dhënat personale. Por, kjo faqe interneti nuk është e vërtetë, kështu që cdo informacion që jepni i shkon sulmuesit.
- **Linqe infektuese**: Qëllimi i sulmuesit është të marrë kontrollin e pajisjes suaj. Për këtë dërgon një email me një

Phishing

link. Nëse ju klikoni linkun, ai ju drejton te një faqe interneti që sulmon pajisjen tuaj dhe që mund të infektojë sistemin e saj.

- **Bashkëlidhje infektuese**: Sulmuesi ka për qëllim të infektojë dhe të marrë kontrollin e pajisjes suaj. Por në vend të një linku, sulmuesi ju dërgon me email një dokument të infektuar, si për shembull një dokument ëord. Kur ju hapni dokumentin e bashkëlidhur, ai sulmon pajisjen dhe mund t'i japë sulmuesit kontroll mbi sistemin e pajisjess.
- **Mashtrimet**: Disa emaile phishing nuk janë asgjë tjetër veçse artistë të fshehur që janë digjitalizuar. Ata mundohen t'ju mashtrojnë duke ju thënë që keni fituar llotari, duke u hequr sikur janë organizatë humanitare në kërkim të donacioneve, apo duke ju kërkuar t'u ndihmoni të lëvizin miliona dollarë. Nëse i përgjigjeni këtyre mashtruesve, ata do t'ju thonë që në fillimi ju duhet t'u dërgoni të holla për shërbime ose t'ju qasen juve në llogari, duke provuar kështu t'u marrin edhe më shumë të holla nga ju.



Logjika e shëndoshë është vetëmbrojtja më e mirë. Nëse një email apo mesazh ju duket i çuditshëm, ose i pabesueshëm, mund të jetë sulm phishing.

Të mbrosh veten

Gati në shumicën e rasteve është në rregull të hapësh një email dhe ta lexosh atë. Që të funksionojë një sulm phishing mashtruesit duhet t'ju detyrojnë të bëni diçka. Për fat të mirë ka disa shenja dalluese në që tregojnë që një mesazh mund të jetë mashtrues dhe dashakeq, ketu janë shenjat më të zakonta:

- Emaili të krijon një sens urgjence, duke kërkuar një përgjigjje të shpejtë para se diçka e keqe të ndodhe, si p.sh. t'ju mbyllin llogarinë bankare. Sulmuesi dëshiron t'ju shtyjë duke u ngutur që të bëni një gabim pa menduar mirë.
- Ju pranoni një email me përmbajtje apo dokument të bashkangjitur por që nuk keni qenë duke e pritur ose emaili ju tërheq që ta hapni dokumentin e bashkangjitur. Për shembull ju mund të merrni një email që ka një listë të personave të pushuar nga puna, informata mbi rrogat e punëtorëve ose një letër nga administrata tatimore që ju thotë se kanë filluar një lëndë gjyqësore ndaj jush.
- Në vend se t'ju drejtohen në emrin tuaj, emaili përdor një titull të përgjithshëm si "I nderuar klient". Shumica e kompanive ose shokëve që ju drejtohen juve e dinë emrin tënd.
- Emaili ju kërkon informata të ndieshme si numri i kartës së kreditit ose fjalëkalimin/passwordin tuaj.
- Emaili thotë që vjen nga një organizatë e njohur, por përdor përmbajtje me gabime gramatikore ose përdor email personal që mbaron me adresa si @gmail.com, @yahoo.com, or @hotmail.com.

Phishing

- Linqet apo vegëzat duken të pazakonta apo jozyrtare. Një këshillë është të mbani shigjetën e mousit mbi link (pa e klikuar) derisa shfaqet një njoftim që ju tregon se ku realisht ju dërgon ai link. Nëse linku në email nuk ju dërgon në destinacionin që duket atëherë mos klikoni në atë link. Në pajisje mobile mbani shtypur me gisht në link dhe pastaj shfaqet adresa ku të dërgon atë link. Një hap më i sigurt është të kopjoni linkun apo edhe ta shkruani vetë.
- Ju pranoni një email nga dikush që e njihni, por me një ton apo fjalë që nuk tingëllojnë normale për atë person. Nëse keni dyshime, telefononi dërguesin dhe verifikoni që vërtet e ka derguar ai/ajo. Është e lehtë për një kriminel kibernetik që të krijojë një email që duket sikur është nga një shok apo koleg pune.

Nëse besoni se një email apo mesazh është sulm phishing, thjesht fshijeni. Në fund, logjika e shëndoshë është vetëmbrojtja më e mirë.

Mëso më shumë

Regjistrohuni në buletinin tonë mujor për vetëdijësimin mbi sigurinë OUCH!, qasuni në arkivat e OUCH!, dhe mësoni më shumë mbi zgjidhjet për ngritjen e vetëdijes mbi sigurinë të ofruara nga SANS duke na vizituar në faqen http://www.securingthehuman.org.

Edicioni në shqip

Edicioni në shqip i OUCH! është përkthyer nga gjuha angleze nga Ilir Bytyçi dhe Jorida Nano. Iliri është magjistër i shkencave në administrimin e rrjetave dhe sistemeve kompjuterike, është ligjërues në universitet për lëndë të ndryshme nga fusha e TI, dhe është përgjegjës për sigurinë e teknologjise informative në bankë. Jorida është përkthyese profesioniste e gjuhës angleze në OSBE.

Burimet

Inxhinjeria Sociale:	https://www.securingthehuman.org/ouch/2014#november2014
Pesë hapa që të rrini të sigurt:	https://www.securingthehuman.org/ouch/2014#october2014
Jam hakuar, ç'të bëj?:	https://www.securingthehuman.org/ouch/2014#may2014
OnGuard Online:	https://www.onguardonline.gov/phishing
SANS Këshilla e ditës:	https://www.sans.org/tip_of_the_day.php

Bordi editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Përkthyer nga: Ilir Bytyçi dhe Jorida Nano