Buletini mujor për vetëdijësimin mbi sigurinë e përdoruesve të kompjuterëve

OUCH!

NË KËTË NUMËR..

- **Dyqanet mashtruese online**
- **Kompjuteri juaj / Pajisja juaj mobile**
- **Karta juaj e kreditit**

Blerja e sigurt online

Është koha të kemi kujdes

Periudha e festave po afron dhe së shpejti miliona njerëz nga e gjithë bota do të kërkojnë të blejnë dhuratat perfekte. Shumica nga ne do të zgjedhim të bëjmë blerje online në kërkim të ofertave më të mira dhe evitimit të radhëve të gjata dhe turmave të padurueshme. Për fat të keq, kjo është edhe periudha më e parapëlqyer e kriminelëve për të bërë mashtrime financiare dhe të atyre online. Në këtë muaj ne do të japim disa sqarime mbi rreziqet e blerjeve online dhe mënyrave se si mund të mbroheni.

Botuesi i ftuar

Jonathan Homer (**@JonathanLHomer**) është udheheqës i njohur në industrinë e vetëdijësimit mbi sigurinë kibernetike dhe është aktiv edhe në sektorin privat poashtu dhe atë publik. Joni specializon në përfshirjen e publikut në diskutime dhe është prin në teknikat trajnuese.

Dyqanet mashtruese online

Edhepse shumica e dyqaneve online janë legjitime, disa nuk janë, pra janë faqe mashtruese të vendosura nga kriminelët. Kriminelët i krijojnë këto faqe duke krijuar kopje të pamjes apo emrit të faqeve të njohura. Pastaj i përdorin këto faqe për të peshkuar njerëz që janë në kërkim të ofertave më të mira. Kur kërkoni online të gjeni çmimin më të ulët të mundshëm ndoshta mund të jeni drejtuar te ndonjë nga këto faqe mashtruese.

Kur e zgjidhni një faqe për të blerë një produkt, vëzhgoni me kujdes çmimet e reklamuara nëse janë shumë më lirë se kudo tjetër apo faqe që mund të jenë duke shitur produkte që mund të jenë shitur tashmë kudo tjetër. Arsyeja pse këto produkte mund të jenë aq të lira apo ende në dispozicion është se ajo që do të bleni mund të mos jetë legjitime, është kopje e keqe apo gjë e vjedhur, ose në disa raste ju as që do ta pranoni atë produkt. Mbrohuni duke bërë hapat e mëposhtëm:

- Verifikoni që faqja e internetit ka adrese legjitime dhe numër telefoni të vërtetë të sektorit të shitjes apo përkrahjes teknike. Nëse ju duket faqe e dyshimtë, telefononi dhe flisni me dikë nga kontaktet.
- Mundohuni të vëreni gjëra si gramatikë e dobët apo gabime drejtshkrimore.
- Jini shumë dyshues nëse një faqe duket të jete kopje e tërësishme e një faqeje të njohur që mund ta keni përdorur në të kaluarën, por që emri i faqes apo emri i dyqanit është pak më i ndryshëm. Për shembull, ju mund të jeni mësuar të vizitoni faqen https://amazon.com për të gjitha blerjet në Amazon. Por kini kujdes nëse e gjeni veten duke bërë blerje në një faqe që pretendon të jetë Amazon me nje adresë si http://store-amazon.com.
- Shkruajeni adresën e faqes që vizitoni në një makinë kërkuese dhe vëreni se çfarë komentesh kanë dhënë tjerët për atë faqe në të kaluarën. Vërej termet e përdoruar si “scam”, “never again” ose “fake.” Nëse askush nuk ka

Blerja e sigurt online

dhënë ndonjë vlerësim, edhe kjo është një shenjë dyshuese sepse do të thotë që është faqe e panjohur dhe e re.

Mos harroni, vetëm se në dukje të parë një faqe mund të duket profesionale, kjo nuk do të thotë se është legjitime dhe e besueshme. Nëse çfarëdo detaji ju duket i dyshimtë, merrni kohë dhe bëni një kërkim. Nëse nuk ndiheni mirë ta përdorni një faqe, mos e përdorni. Më mirë gjeni një faqe të njohur të cilës mund t'i besoni dhe e keni përdorur në mënyrë të sigurt në të kaluarën. Kështu ndoshta nuk do ta gjeni ofertën më të mirë apo më të volitshme, por të paktën në fund keni një produkt legjitim dhe një llogari të padëmtuar.

Mbroni veten online duke blerë vetëm nga faqe të besueshme që kanë reputacion të lartë.

Kompjuteri juaj / Pajisja juaj mobile

Përveç blerjes në faqe legjitime, ju duhet të kujdeseni që kompjuteri juaj apo pajisja juaj mobile janë poashtu të sigurta. Kriminelët kibernetikë do të mundohen t'ju infektojnë pajisjet tuaja në mënyrë që t'ju marrin llogarinë tuaj bankare, informatat tuaja të kredit kartës, si dhe fjalëkalimet (ang. Password). Ju duhet të ndermerrni hapat vijues që t'i mbani pajisjet tuaja të sigurta:

- Nëse keni fëmijë në shtëpi, merrni parasysh këshillën t'i mbani dy pajisje, një për fëmijët tuaj dhe një për të rritur. Fëmijët janë kuriozë dhe përdorin lehtësisht teknologjinë, dhe si rezultat ata mund të infektojnë pajisjen që kanë në dorë. Duke patur një kompjuter tjetër apo tablet për të bërë transaksione online, si p.sh. online bankën apo blerje online, ju e ulni mundësinë që të infektoheni edhe ju. Nëse nuk keni mundësi të keni një pajisje ndaras, sigurohuni që fëmijet tuaj të mos kenë qasje administratori pra të pakufizuar në kompjuter.
- Lidhuni vetëm në rrjeta pa tel (ang. Wireless) të cilat i menaxhoni vetë, si p.sh. rrjeti juaj i shtëpisë ose rrjete të cilave ju besoni për të bërë transaksione financiare. Përdorimi i Wi-Fi në publik si në kafene mund të jetë gjë e mirë për të lexuar lajme por jo për të hyrë në llogarinë tuaj bankare.
- Gjithmonë instaloni përditësimet e fundit dhe kini një program anti-virus. Kjo e bën më të vështirë për kriminelët kibernetikë që ta infektojnë pajisjen tuaj.

Karta juaj e kreditit

Duhet të kini kujdes duke e parë llogarinë tuaj të kartës së kreditit për ndonjë pagesë të dyshimtë. Ju duhet t'i shihni faturat dhe raportet e llogarisë rregullisht, ose të paktën një herë në muaj. Disa ofrues të kartave të kreditit ju mundësojnë që të njoftoheni me email ose me mesazh çdoherë kur ka ndonjë blerje me kartën tuaj të kreditit ose kur pagesa e kalon një vlerë të caktuar. Një opsion tjetër është që të keni kartë krediti vetëm për pagesa online, në këtë mënyrë nëse kjo kartë

Blerja e sigurt online

kompromethohet atëherë do të mund ta ndërroni kartën pa ndikuar në aktivitetet tuaja financiare. Nëse besoni se është bërë ndonjë keqpërdorim me kartën tuaj, telefononi menjëherë dhe spjegoni me kujdes situatën. Kjo është arsyeja se pse kartat e kreditit janë më të mira për blerje online se sa kartat e debitit. Karta e debitit ju tërheq paratë drejtpërdrejt nga llogaria juaj bankare, dhe nëse bëhet ndonjë keqpërdorim apo mashtrim, do të jetë shumë më e vështirë t'ju kthehen paratë.

Në fund, ka një teknologji e cila ju mundëson juve të mos e ekspozoni kartën tuaj të kreditit. Merrni parasysh përdorimin e kartave të kreditit që gjenerojnë nj numër unik për çdo blerje ose përdorni shërbime të njohura si PayPal të cilat nuk ju kërkojnë të shpalosni numrin e kartës së kreditit te faqja ku bleni online.

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

Pesë hapa si të rrini të sigurt:	https://www.securingthehuman.org/ouch/2014#october2014
Mbrojtja e rrjetit tuaj të shtëpise:	https://www.securingthehuman.org/ouch/2014#january2014
Mbrojtja e tabletit tuaj:	https://www.securingthehuman.org/ouch/2013#december2013
Këshilla e ditës e sigurisë nga SANS:	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