
OKTOBAR
mjesec
CYBER
SIGURNOSTI
MUPZDK

Mjesečni bilten za podizanje svijesti o bezbjednosti informacija

Zaštitite se od malvera

Uvod

Sigurno ste već u pričama o sajber bezbjednosti čuli za termine kao što su virus, trojanac, ransomver ili rutkit. Sve su to različiti tipovi malicioznih programa poznatih kao malver, koje sajber kriminalci koriste da bi zarazili računare i uređaje. Kada se instaliraju na vašem uređaju, ovi programi mogu da urade sve što želi onaj ko ih je kreirao. U ovom tekstu saznaćete šta je malver, do kakvih opasnosti dovodi, kao i ono najvažnije, šta možete da uradite da biste se od njega zaštitili.

Šta je malver?

Jednostavno rečeno, malver je softver, računarski program, koji se koristi za izvršavanje malicioznih aktivnosti. Riječ malver je složenica riječi maliciozan i softver. Sajber kriminalci instaliraju malver na vašim računarima i uređajima sa ciljem da uspostave kontrolu nad njima. Po uspešnoj instalaciji, malver može da omogući kriminalcima nadgledanje vaših aktivnosti na internetu, krađu vaših lozinki ili fajlova, ili da korištenjem vašeg sistema napadnu druge. Malver čak može da uskrati pristup vašim podacima, tražeći da platite otkupninu da biste ga vratili. Mnogi ljudi vjeruju da malver predstavlja prijetnju samo za Windows računare. Nažalost, malver može zaraziti bilo koji uređaj, od Mac računara i pametnih telefona do digitalnih video i bezbjednosnih kamera. Što više računara i uređaja sajber kriminalci zaraze, njihova zarada će biti veća. Zato smo svi, pa i vi sami, potencijalna meta.

Zaštitite se – zaustavite malver

Možda vam se čini da je dovoljno da instalirate bezbjednosni program poput antivirusnog softvera da biste bili zaštićeni od malvera. Nažalost, antivirus ne može da zaustavi sav malver. Sajber kriminalci neprestano razvijaju novi i sve napredniji malver koji ima osobinu da ostane neprimjećen. S druge strane, proizvođači antivirusnog softvera stalno ažuriraju svoje proizvode novim funkcionalnostima za otkrivanje malvera. Na mnogo načina to sve više liči na nekakvu trku u naoružavanju, u kojoj su loši momci obično za korak ispred. Pošto se ne možete osloniti samo na antivirus, evo dodatnih koraka koje treba da preduzmete da biste se zaštitili:

Sajber kriminalci često iskorištavaju ranjivosti u vašem softveru da zaraze računare ili uređaje. Što je vaš softver ažurniji, to su vaši sistemi manje ranjivi i sajber kriminalcima je teže da ih zaraze. Potrudite se da vaši operativni sistemi, aplikacije, veb pregledači (eng. Web browser) i dodaci za pregledače budu uvek ažurirani i aktuelni. Najlakši način da to postignete je da, kad god je to moguće, uključite njihovo automatsko ažuriranje.

Uobičajen način koji sajber kriminalci koriste da zaraze računare ili mobilne uređaje je kreiranje lažnih računarskih ili mobilnih aplikacija i njihovo objavljivanje na internetu, nakon čega ostaje samo da vas prevare da ih preuzmete i instalirate. Zato je najbolje da softver ili aplikacije preuzimate i instalirate samo iz pouzdanih onlajn prodavnica. Takođe, izbjegavajte mobilne aplikacije koje su potpuno nove, imaju malo pozitivnih ocjena, rijetko se ažuriraju ili ih je preuzeo mali broj ljudi. Ukoliko ste prestali da koristite neki softver ili mobilnu aplikaciju, deinstalirajte ga.

Dešava se često i da sajber kriminalci, služeći se prevarom, instaliraju malver u ime drugih. Na primjer, oni vam mogu poslati mejl poruku koja izgleda legitimno i sadrži neki prilog ili link. Može se čak desiti i da poruka izgleda kao da je šalje vaša banka ili prijatelj. Međutim, ako biste otvorili priloženi fajl ili kliknuli na link, aktivirali biste maliciozni kod koji instalira malver na vašem sistemu. Ako poruka stvara snažan osjećaj hitnosti ili izgleda previše dobro da bi bila istinita, to ukazuje na potencijalni napad. Budite sumnjičavi, zdrav razum je često vaša najbolja odbrana.

Redovno kreirajte rezervne kopije vašeg sistema i podataka korišćenjem Cloud rešenja za bekap ili eksternih diskova koje ćete čuvati oflajn, odnosno fizički odvojene. Time ćete zaštititi vaše bekape u slučaju da malver pokuša da ih šifruje ili obriše. Rezervne kopije su veoma važne jer su često jedini način da se oporavite od štete koju vam je malver nanjeo.

Ponovimo na kraju, najbolji način da se odbranite od malvera je da redovno ažurirate sav softver i uređaje, instalirate pouzdan antivirusni softver kad god je to moguće i uvek budete na oprezu kako vas neko ne bi prevario da zarazite sopstveni sistem. Kada sve ostalo padne u vodu, bekap je često jedini način za oporavak vaših podataka.

Uprava policije Ministarstva unutrašnjih poslova Zeničko dobojskog kantona kao društveno odgovorna institucija pomaže distribuciju ovog biltena kako bi se unaprijedila svijest korisnika informaciono-komunikacionih tehnologija o bezbjednosti informacija.

Gost urednik

Leni Zelcer ima veliko iskustvo u borbi protiv malvera. Bavi se kreiranjem endpoint bezbjednosnih rješenja u kompaniji Minerva Labs i predaje na SANS Institutu. Leni je aktivan na Tviteru kao @lennyzeltser i autor je bloga o sajber bezbjednosti zeltser.com.

Dodatni materijal

Ransomver:	https://www.sans.org/u/EdI
Rezervne kopije i oporavak:	https://www.sans.org/u/EdN
Ne dajte se upecati:	https://www.sans.org/u/EdS

 Redakcija: Walt Scrivens, Phil Hoffman, Кэти Клик, Cheryl Conley | Prilagodili: Edin Beriša i Adis Bajramović

SANS SECURITY AWARENESS
MUPZDK
OUCH! | Januar 2018
Mjesečni bilten za podizanje svijesti o bezbjednosti informacija

OUCH!

U OVOM BROJU...

Napravite digitalno bezbjedan dom

Uvod

Pravljenje bezbjednog digitalnog doma prije nekoliko godina bilo je jednostavno jer je većina kuća imala samo bežičnu mrežu i nekoliko računara. Danas je tehnologija postala mnogo složenija i integrisana u svaki dio naših života, od mobilnih uređaja i konzola za igru do kućnog termostata, pa čak i vašeg frižidera. U nastavku su opisana četiri jednostavna koraka kako da vaš dom učinite digitalno bezbjednim.

Gost urednik

Met Bromili (Matt Bromiley) se bavi rješavanjem incidenata pomažući kompanijama svih veličina da se izbore sa ugrožavanjem bezbjednosti svojih podataka. On je takođe SANS instruktor i drži kurs Napredna digitalna forenzika i rješavanje incidenata (FOR508, Advanced Digital Forensics and Incident Response). Pratite Meta na tviteru **@mbromileyDFIR**.

Vaša bežična mreža

Osnova gotovo svake kućne mreže je bežična (Wi-Fi) mreža. Ova mreža omogućuje svim vašim uređajima da se povežu na internet. Većinom kućnih bežičnih mreža se upravlja pomoću vašeg internet rutera ili bežične pristupne tačke (eng. wireless access point). Oba ova uređaja rade na isti način, tako što emituju bežične signale putem kojih se povezuju uređaji u vašoj kući. Ovo praktično znači da je zaštita vaše bežične mreže ključni dio u zaštiti vašeg doma. Zaštitite je primjenom sljedećih savjeta:

- Promjenite podrazumjevanu administratorsku lozinku na vašem ruteru ili bežičnoj pristupnoj tački, u zavisnosti od toga koji od ovih uređaja kontroliše vašu bežičnu mrežu. Administratorski nalog vam omogućava da mijenjate podešavanja vaše bežične mreže.
- Osigurajte da samo osobe kojima vjerujete mogu da se povežu na vašu bežičnu mrežu tako što ćete postaviti jake mjere zaštite. Trenutno najbolja opcija je da koristite bezbjednosni mehanizam pod nazivom WPA2. Kada omogućite ovu opciju biće neophodna lozinka kako bi se drugi povezali na vašu kućnu mrežu, a dok su povezani njihove aktivnosti na mreži će biti šifrovane.
- Osigurajte da lozinka koja se koristi za povezivanje na vašu bežičnu mrežu bude kompleksna i da se razlikuje od administratorske lozinke. Takvu lozinku je samo jednom potrebno unijeti na svaki vaš uređaj, budući da je oni čuvaju i pamte.
- Mnoge bežične mreže podržavaju kreiranje takozvane „Gost mreže“. Ova mreža omogućava posjetiocima da se povežu na Internet, ali štiti vašu kućnu mrežu pošto se oni ne mogu povezati ni sa jednim drugim uređajem u

vašoj kućnoj mreži. Ako dodate mrežu za goste, obavezno i za nju uključite WPA2 i postavite jedinstvenu lozinku za povezivanje na ovu mrežu.

Niste sigurni kako da primjenite ove savjete? Pitajte vašeg internet provajdera ili potražite pomoć na njihovom veb sajtu, provjerite dokumentaciju koju ste dobili uz vaš internet ruter ili bežičnu pristupnu tačku ili pogledajte njihove veb sajtove.

Slijedite ova četiri jednostavna koraka za kreiranje bezbjednog digitalnog doma: obezbjedite svoju bežičnu mrežu, omogućite automatsko ažuriranje, koristite jedinstvene lozinke i izrađujte bekap.

Vaši uređaji

Sljedeći korak je da znate koji su sve uređaji povezani na vašu kućnu bežičnu mrežu i da se postarate da su svi ti uređaji zaštićeni. Ovo je bilo jednostavno kada ste imali samo jedan ili dva računara. Međutim, danas se gotovo sve može povezati sa vašom kućnom mrežom, uključujući vaše pametne telefone, televizore, konzole za igrice, bebi alarme, zvučnike ili možda čak i vaš automobil. Kada ste identifikovali sve uređaje na vašoj kućnoj mreži, osigurajte da je svaki od njih zaštićen. Najbolji način da ovo sprovedete je da osigurate da automatsko ažuriranje na njima bude uključeno kad god je to moguće. Sajber napadači stalno pronalaze nove ranjivosti na različitim uređajima i operativnim sistemima. Omogućavanjem automatskog ažuriranja, vaš računar i uređaji će uvijek koristiti najnoviji softver, što bilo koji pokušaj njihovog hakovanja čini mnogo težim.

Lozinke

Sljedeći korak je da koristite jaku, jedinstvenu lozinku za svaki vaš uređaj i nalog na internetu. Ključne riječi za lozinku su: jaka i jedinstvena. Umorni ste od kompleksnih lozinki koje se teško pamte i komplikovano unose? Niste jedini. Koristite frazu za pristup umesto lozinke. Ovo je vrsta lozinke koja koristi niz riječi koje je lako zapamtiti, kao što su “Gdje je moja kafa?” Ili “ Snežana i sedam patuljaka”. Što je vaša fraza duža, jača je. Jedinstvena lozinka podrazumjeva korištenje različite lozinke za svaki uređaj i nalog na internetu. Na ovaj način, ukoliko je jedna lozinka kompromitovana, ostali vaši nalozi i uređaji će i dalje biti bezbjedni. Ne možete da zapamtite sve te jake, jedinstvene lozinke? Ne brinite, malo ko to i može. Zbog toga se preporučuje da koristite menadžer lozinke, posebnu aplikaciju koja za vas na bezbjedan način čuva sve vaše lozinke u šifrovanom, virtuelnom sefu.

Konačno, omogućite verifikaciju u dva koraka kad god je to moguće, naročito za vaše naloge na internetu. Verifikacija u dva koraka pruža bolju zaštitu. Ona koristi vašu lozinku, ali takođe dodaje drugi korak, kao što je šifra poslata na vaš pametni

telefon ili aplikacija na pametnom telefonu koja generiše šifru za vas. Verifikacija u dva koraka je vjerovatno najvažniji korak koji možete preduzeti da biste se zaštitili na mreži i koristi se mnogo lakše nego što mislite.

Rezervne kopije

Ponekad, bez obzira koliko ste pažljivi, možete da budete hakovani. U tom slučaju je često jedini način na koji možete povratiti vaše lične informacije taj da ih oporavite iz bekapa. Postarajte se da redovno izrađujete rezervne kopije svih važnih informacija i provjeravajte da li možete da ih oporavite. Većina mobilnih uređaja podržava automatsku izradu rezervnih kopija u Cloud-u. Za većinu računara možda ćete morati da kupite neku vrstu softvera ili servisa za bekap, koji su relativno jeftini i jednostavni za korištenje.

Saznajte više

Prijavite se na OUCH! mjesečni bilten za podizanje svijesti o bezbjednosti informacija namjenjen svima, pročitajte prethodne brojeve OUCH!-a i saznajte više o SANS-ovim rješenjima za unapređenje svijesti o bezbjednosti informacija na našoj internet prezentaciji securingthehuman.sans.org/ouch/archives.

Uprava policije Ministarstva unutrašnjih poslova Zeničko dobojskog kantona kao društveno odgovorna institucija pomaže distribuciju ovog biltena kako bi se unaprijedila svijest korisnika informaciono-komunikacionih tehnologija o bezbjednosti informacija.

Dodatne informacije

Pristupne fraze:	https://securingthehuman.sans.org/ouch/2017#april2017
Menadžeri lozinki:	https://securingthehuman.sans.org/ouch/2017#september2017
Dvofaktorska autentifikacija:	https://securingthehuman.sans.org/ouch/2017#december2017
Rezervne kopije:	https://securingthehuman.sans.org/ouch/2017#august2017

Redakcija: Walt Scrivens, Phil Hoffman, Кэти Клик, Cheryl Conley
Prilagodili: Edin Beriša i Adis Bajramović

Mjesečni bilten za podizanje svijesti o bezbjednosti informacija

Kako da zaštitite vaše mobilne uređaje

Uvod

Vaši mobilni uređaji omogućavaju veoma jednostavnu komunikaciju sa prijateljima, kupovinu putem interneta, pristup mobilnom bankarstvu, gledanje filmova, igranje igrica i obavljanje brojnih drugih aktivnosti. Pošto su mobilni uređaji toliko važan dio naših života, u nastavku predstavljamo nekoliko jednostavnih koraka koji će omogućiti da i vi i vaši uređaji ostanete bezbjedni.

Zaštitite vaše uređaje

Možda će vas iznenaditi činjenica da najveći rizik po vaše mobilne uređaje ne predstavljaju hakeri, već najvjerovatnije vi sami. Mnogo je veća vjerovatnoća da ćete izgubiti ili zaboraviti svoj mobilni uređaj nego da će ga neko hakovati. Prvo što u cilju zaštite uređaja treba da preduzmete je da uključite automatsko zaključavanje ekrana (eng. screenlock). To znači da ćete svaki put kada budete željeli da koristite vaš uređaj prvo morati da otključate ekran, najbolje korištenjem jake lozinke ili otiska prsta. Ovim se spriječava da neko drugi pristupi vašem uređaju ako ga izgubite ili bude ukraden. Dodatni koraci koji će vam pomoći da obezbjedite vaš uređaj su sljedeći:

Ažuriranje

Na vašim uređajima uključite automatsko ažuriranje jer time obezbjeđujete da uređaj uvijek koristi najnovije verzije operativnog sistema i aplikacija. Potencijalni napadači neprestano traže nove ranjivosti u softveru, a proizvođači stalno objavljuju nove verzije i zakrpe kako bi ispravili otkrivene ranjivosti. Korištenjem najnovijih verzija operativnog sistema i mobilnih aplikacija u velikoj mjeri ćete otežati hakovanje vaših uređaja.

Praćenje

Instalirajte i/ili omogućite da softver udaljeno prati vaše uređaje preko interneta. Tako ćete, u slučaju da je vaš uređaj izgubljen ili ukraden, imati mogućnost da se preko interneta povežete sa uređajem i saznate njegovu lokaciju, a u najgorem slučaju i udaljeno obrišete sve vaše informacije na njemu.

Bezbjednost aplikacija

Instalirajte samo aplikacije koje su vam neophodne i preuzimajte ih samo iz pouzdanih izvora. Za iPhone i iPad uređaje to znači da aplikacije treba da preuzimate sa Apple App Store-a. Za Android uređaje preuzimajte aplikacije sa Google Play-a, a za Amazon tablete sa Amazon App Store-a. Iako možda aplikacije možete da preuzmete i

sa drugih sajtova, znajte da one nisu provjerene i veća je vjerovatnoća da aplikacija bude zaražena. Takođe, prije nego što preuzmete aplikaciju uvjerite se da ima veliki broj pozitivnih komentara i da se često ažurira. Izbjegavajte potpuno nove aplikacije, aplikacije sa svega nekoliko komentara ili one koje se rijetko ažuriraju. Na kraju, bez obzira na koji način da ste do aplikacije došli, preporuka je da je obrišete sa svog uređaja kada vam više nije potrebna ili je aktivno ne koristite.

Privatnost

Kada instalirate novu aplikaciju, obavezno pregledajte dozvole u vezi sa privatnošću vaših podataka. Na primjer, razmislite da li aplikacija koju ste upravo preuzeli zaista treba da ima pristup informacijama o svim vašim prijateljima i kontaktima? Takođe vam preporučujemo da prvo potpuno isključite praćenje vaše lokacije, a potom ga omogućite samo za one aplikacije za koje smatrate da su im potrebne informacije o lokaciji. Ako sumnjate da aplikacija zahtijeva dozvole koje su veće od neophodnih za njeno funkcionisanje, pronađite drugu koja zadovoljava vaše potrebe. Ne zaboravite da povremeno provjerite dozvole date aplikaciji kako biste se uvjerili da se nisu promjenile.

Bekap

Uvek kreirajte rezervne kopije vaših podataka. Za mobilne uređaje bekap se kreira automatski za veliki dio vaših informacija, poput fotografija i poruka. Međutim, kompletni bekapi takođe čuvaju i vašu konfiguraciju, aplikacije i druge informacije o uređaju, i pojednostavljuju oporavak u slučaju kada izgubite uređaj ili prelazite na novi.

Poslovno okruženje

Kada ste na poslu, budite posebno pažljivi i nikada ne fotografišite i ne snimajte bilo šta što uključuje osjetljive i povjerljive informacije, poput tabli sa skicama ili prikaza na ekranu.

Mobilni uređaji su moćni alati koje želimo da koristimo i u tome uživamo. Primjenom ovih jednostavnih koraka možete učiniti mnogo u pogledu sopstvene zaštite i zaštite vaših uređaja.

Uprava policije Ministarstva unutrašnjih poslova Zeničko dobojskog kantona kao društveno odgovorna institucija pomaže distribuciju ovog biltena kako bi se unaprijedila svijest korisnika informaciono-komunikacionih tehnologija o bezbjednosti informacija.

Dodatne informacije

Pristupne fraze:	https://www.sans.org/u/A3E
Rezervne kopije i oporavak:	https://www.sans.org/u/A3z
Kako da se otarasite mobilnog uređaja na bezbjedan način:	https://www.sans.org/u/A3u
Bezbjedno korištenje mobilnih aplikacija:	https://www.sans.org/u/A3p
SANS savjet dana:	https://www.sans.org/tip_of_the_day.php

Licenca

Redakcija: Walt Scrivens, Phil Hoffman, Кэти Клик, Cheryl Conley | Prilagodili: Edin Beriša i Adis Bajramović

SANS SECURITY AWARENESS
MUPZDK
OUCH! | Decembar 2017
Mjesečni bilten za podizanje svijesti o bezbjednosti informacija

OUCH!

U OVOM BROJU...

Obezbjedite svoj nalog

Uvod

Proces autentifikacije ili utvrđivanja identiteta ključan je za zaštitu vaših informacija poput elektronske pošte, informacija na društvenim mrežama ili onlajn bankovnim računima. Možda niste svjesni ali postoje tri različita načina da dokažete ko ste: pomoću nečega što znate - kao što je lozinka, nečega što imate - kao što je vozačka dozvola i nečega što je dio vas samih - poput otiska prsta. Svaka od ovih metoda ima prednosti i mane. Najčešće se kao metod autentifikacije koriste lozinke, dakle nešto što znate. Nažalost, sve se više pokazuje da korištenje samo lozinki nije dovoljno bezbjedno. U ovom tekstu možete saznati kako da zaštitite sebe i svoje naloge nečim što je bolje od samih lozinki, a zove se dvofaktorska autentifikacija.

Gost urednik

Tifani Šonike je direktorka za kampanje i inicijative pri Nacionalnoj alijansi za sajber bezbjednost (**@staysafeonline**). Tokom 2016. godine, u saradnji sa Bijelom kućom, vladom SAD i različitim industrijama, radila je na kampanji pod imenom STOP. THINK. CONNECT.™ koja se bavila i povećavanjem bezbjednosti naloga i dvofaktorskom autentifikacijom.

Lozinke više nisu dovoljne

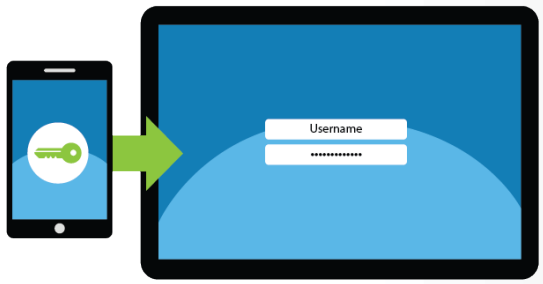
Lozinke dokazuju ko ste na osnovu nečega što vi znate. Međutim, ako neko uspije da pogodi ili pristupi vašoj lozinki, on može da se predstavi kao vi i pristupi svim vašim informacijama. Kompromitovane lozinke postale su jedan od glavnih uzročnika hakovanja naloga. Otud i savjeti da kad kreirate lozinke koristite fraze koje će drugi teško moći da pogode, da koristite različite lozinke za svaki vaš nalog i da nikada ne dijelite svoje lozinke sa drugima. Iako svi ovi savjeti ostaju na snazi, činjenica je da lozinke više nisu uspješan metod zaštite. Srećom, postoji lak i brz način da opet uspostavite kontrolu i učinite svoje lične informacije bezbjednijim, a to je dvofaktorska autentifikacija.

Šta je dvofaktorska autentifikacija?

Dvofaktorska autentifikacija (dvostepena verifikacija, verifikacija iz dva koraka, multifaktorska autentifikacija, 2FA) je daleko bezbjednija nego autentifikacija prilikom koje se koriste samo lozinke. Funkcioniše tako što zahtjeva ne jednu već dvije

Obezbjedite svoj nalog

različite metode za dokazivanje da ste vi osoba za koju se predstavljate. Dobar primjer je vaša platna kartica. Kada podižete novac na bankomatu, vi zapravo koristite dvofaktorsku autentifikaciju. Da biste podigli svoj novac potrebe su vam dve stvari, vaša platna kartica (nešto što imate) i vaš PIN (nešto što znate). Ako izgubite ili vam neko ukrade platnu karticu niko drugi ne može da podigne vaš novac bez poznavanja PIN-a. Kradljivac mora da ima i vašu platnu karticu i PIN da bi na bankomatu obavio transakciju. Dvofaktorska autentifikacija koristi isti koncept.



Obezbjedite svoj nalog korištenjem dvofaktorske autentifikacije kad god je to moguće, jer je to jedan od najvažnijih koraka za zaštitu na internetu koji možete da preduzmete.

Kako funkcioniše

Dvofaktorska autentifikacija je široko rasprostranjena na većini sajtova poznatih banaka, usluga e-pošte, društvenih mreža i drugih. Osim toga većina ovih sajtova nudi i jednostavna uputstva korak-po-korak za omogućavanje dvofaktorske autentifikacija (više informacija naći ćete na kraju u odeljku Dodatne informacije). Jednom kada omogućite dvofaktorsku autentifikaciju možete da očekujete da funkcioniše na sljedeći način. Prvo, svom nalogu pristupate korišćenjem korisničkog imena i lozinke kao što ste to i ranije činili. Time ste upotrebili prvi od dva faktora – nešto što znate. Zatim će vam, najčešće putem tekstualne poruke na mobilni telefon, biti poslat jedinstveni kod (da biste primili kod morate da imate svoj telefon). Jedinstveni kod unosite u polje na stranici za prijavljivanje i time ste upotrijebili i drugi od dva faktora. Tako je vaš nalog dodatno obezbjeđen. Čak i ako sajber kriminalac ukrade vašu lozinku, neće moći da pristupi vašem nalogu osim ako nema i vaš telefon.

Umjesto korištenja jedinstvenog koda dobijenog putem tekstualne poruke, možete na vašem pametnom telefonu da instalirate posebnu mobilnu aplikaciju za autentifikaciju. Aplikacija neprestano generiše novi jedinstveni kod koji možete da upotrijebite kad god poželite da se prijavite. Prednost mobilne aplikacije je u još većoj bezbjednosti jer se jedinstveni kod generiše u aplikaciji umjesto da se prenosi mobilnom mrežom kao tekstualna poruka. Pored toga, zgodnija je za upotrebu jer nije neophodno da budete povezani na mobilnu mrežu kako biste dobili vaš jedinstveni kod.

Obezbjedite svoj nalog

Iako na prvi pogled možda djeluje da dvofaktorska autentifikacija zahtjeva mnogo posla, njenim korištenjem će vaše lične informacije biti znatno bezbjednije. Ne čekajte da vaši nalozi budu kompromitovani, već za vaše važne naloge poput naloga za e-poštu, bankovnih ili naloga na društvenim mrežama omogućite upotrebu dvofaktorske autentifikacije i budite spokojni znajući da su mnogo bezbjedniji.

Saznajte više

Prijavite se na OUCH! mjesečni bilten za podizanje svijesti o bezbjednosti informacija namjenjen svima, pročitajte prethodne brojeve OUCH!-a i saznajte više o SANS-ovim rješenjima za unapređenje svijesti o bezbjednosti informacija na našoj internet prezentaciji securingthehuman.sans.org/ouch/archives.

Uprava policije Ministarstva unutrašnjih poslova Zeničko dobojskog kantona kao društveno odgovorna institucija pomaže distribuciju ovog biltena kako bi se unaprijedila svijest korisnika informaciono-komunikacionih tehnologija o bezbjednosti informacija.

Dodatne informacije

Pristupne fraze:	https://securingthehuman.sans.org/ouch/2017#april2017
Sajtovi koji podržavaju dvofaktorsku autentifikaciju:	https://twofactorauth.org
Stop|Think|Connect:	https://www.lockdownyourlogin.org
Google dvostepena verifikacija:	http://www.google.com/landing/2step/

Redakcija: Walt Scrivens, Phil Hoffman, Кэти Клик, Cheryl Conley
Prilagodili: Edin Beriša i Adis Bajramović

Mjesečni bilten za podizanje svijesti o bezbjednosti informacija

OUCH!

U OVOM BROJU...

- Šta je socijalni inžinjering
- Detekcija i sprečavanje napada socijalnim inžinjeringom

Socijalni inžinjering

Uvod

Uobičajena zabluda koju većina ljudi ima o sajber napadačima je da oni koriste samo veoma napredne alate i tehnike da bi hakovali nečiji računar ili korisnički nalog. Ovo jednostavno nije tačno. Sajber napadači su naučili da je često najlakši način da ukradu vaše informacije, hakuju vaš nalog ili zaraze vaše sisteme taj da vas jednostavno zavaraju (obmanu) da napravite grešku. U ovom tekstu naučićete kako ovi napadi, poznati kao socijalni inžinjering, funkcionišu i šta možete da uradite da biste se zaštitili.

Gost urednik

James Lyne (@jameslyne) je sertifikovani SANS instruktor i globalni rukovodilac istraživanja u kompaniji Sophos. On dekomponuje i obrnutim inženjeringom analizira najnovije i najveće prevare sajber kriminalaca. On je takođe i autor SANS-ovih obuka Metasploit (SEC580) i Social Engineering (SEC567).

Šta je socijalni inžinjering

Socijalni inžinjering je psihološki napad u kojem vas napadač obmane da uradite nešto što ne bi trebalo da uradite. Koncept socijalnog inžinjeringa uopšte nije nov, on postoji hiljadama godina unazad. Pomislite na razne prevarante ili varalice, to je u osnovi ista ideja. Ono što današnju tehnologiju čini mnogo efikasnijom za sajber napadače je da ne možete fizički da ih vidite, oni mogu lako da se pretvaraju da su bilo ko ili bilo šta i da ciljaju milione ljudi širom sveta, uključujući i vas. Dodatno, napadi socijalnim inžinjeringom mogu da zaobiđu mnoge tehnološke mjere zaštite. Najjednostavniji način da razumijete kako ovi napadi funkcionišu i da se zaštitite od njih je da se upoznate sa dva primjera iz stvarnog svijeta.

Primili ste telefonski poziv od nekoga ko tvrdi da je iz kompanije za računarsku podršku, vašeg provajdera internet usluga ili Mikrosoftove tehničke podrške. Osoba koja vas je pozvala objašnjava vam da vaš računar aktivno skenira Internet, oni vjeruju da je računar zaražen i dobili su zadatak da vam pomognu da zaštitite vaš računar. Oni zatim koriste razne tehničke termine i niz zbunjujućih koraka kako bi vas ubijedili da vam je računar zaražen. Na primjer, mogu da vas pitaju da provjerite da li imate određene fajlove na vašem računaru i da vas upute kako da ih pronađete. Kad locirate ove fajlove, pozivalac vas uvjerava da su ovi fajlovi dokaz da je vaš računar zaražen, dok u realnosti ovi fajlovi predstavljaju uobičajene sistemske fajlove koji se nalaze na skoro svakom računaru u svijetu. Nakon što vas ubijede da je vaš računar zaražen, oni vas onda pritiskaju da kupite njihov bezbjednosni softver ili da im dozvolite udaljeni pristup vašem računaru kako bi mogli da ga poprave. Međutim, softver koji oni prodaju je u stvari maliciozni program. Ako kupite i instalirate ovaj softver ne samo da su

Socijalni inžinjering

vas prevarili da zarazite vaš računar, već ste im i platili da to urade. U slučaju da im dozvolite da udaljeno pristupaju vašem računaru, oni će preuzeti kontrolu nad njim, ukrasti vaše podatke ili ih prodati

Zdrav razum je vaša najmoćnija odbrana za otkrivanje i zaustavljanje većine napada socijalnim inžinjeringom.

Drugi primjer je napad putem elektronske pošte poznat kao „CEO prevara“, koji se najčešće događa na poslu. Ovo je situacija kada sajber napadač istraživanjem vaše organizacije na Internetu sazna imena vaših pretpostavljenih ili kolega. Napadač zatim pripremi mejl koji izgleda kao da je od te osobe i pošalje vam ga. U mejlu se traži da hitno preduzmete neku akciju, kao što je prenos novca na neki račun ili slanje osjetljivih informacija o zaposlenima. Veoma često ovi mejlovi koriste navodnu hitnost situacije kao razlog za zaobilaženje standardnih bezbjednosnih procedura, npr. može da se zahtijeva da pošaljete vrlo osjetljive informacije na privatni nalog na @gmail.com. Ono što ciljane napade poput ovog čini tako opasnim je činjenica da sajber napadači unaprijed obave istraživanje. Pored toga, tehnološke mjere zaštite kao što su antivirus programi ili fajervoli ne mogu da detektuju ili spriječe ove napade jer oni ne koriste maliciozne programe ili linkove.

Imajte na umu, napadi socijalnim inžinjeringom poput ovih nisu ograničeni samo na telefonske pozive ili elektronsku poštu; oni mogu da se pojave u bilo kojoj formi uključujući i tekstualne poruke na vašem telefonu, putem društvenih mreža ili čak uživo. Ključno je da znate na šta da obratite pažnju, sami ste sebi najbolja zaštita.

Detekcija i sprečavanje napada socijalnim inžinjeringom

Na sreću sprečavanje ovakvih napada je jednostavnije nego što mislite – zdrav razum je vaša najbolja odbrana. Ako vam nešto izgleda sumnjivo ili vam ne djeluje u redu, to može biti napad. Najčešći znakovi koji ukazuju da je u pitanju napad socijalnim inžinjeringom su:

- Neko stvara izuzetan osjećaj hitnosti pokušavajući da vas prevari da napravite grešku.
- Neko vam traži informaciju kojoj ne bi trebalo da ima pristup ili bi već trebalo da je zna.
- Neko vam traži vašu lozinku, nijedna legitimna organizacija vam to nikad neće tražiti.
- Neko vrši pritisak na vas da zaobiđete ili ignorišete bezbjednosne procedure kojih bi trebalo da se pridržavate na poslu.

Socijalni inžinjering

- Nešto je previše dobro da bi bilo istinito. Na primjer, obavješteni ste da ste dobili novac ili iPad u nagradnoj igri, iako nikad niste učestvovali u toj nagradnoj igri.
- Primili ste neobičan mejl od prijatelja ili kolege koji sadrže formulacije koje uopšte nisu uobičajene za njih. Sajber napadač je možda hakovao njihov nalog i pokušava da vas prevari. Da biste se zaštitili provjerite ove zahtjeve, tako što ćete stupiti u kontakt sa vašim prijateljima korištenjem drugih metoda za komunikaciju, uživo ili preko telefona.

Ukoliko sumnjate da neko pokušava da vas prevari ili obmane, nemojte komunicirati više sa tom osobom. Ako je napad povezan sa poslom, obavezno ga odmah prijavite vašoj IT podršci (help desk) ili timu koji se bavi informacionom bezbjednošću. Zapamtite, zdrav razum je često vaša najbolja odbrana.

Saznajte više

Prijavite se na OUCH! mjesečni bilten za podizanje svijesti o bezbjednosti informacija namjenjen svima, pročitajte prethodne brojeve OUCH!-a i saznajte više o SANS-ovim rješenjima za unapređenje svijesti o bezbjednosti informacija na našoj internet prezentaciji securingthehuman.sans.org/ouch/archives.

Uprava policije Ministarstva unutrašnjih poslova Zeničko dobojskog kantona kao društveno odgovorna institucija pomaže distribuciju ovog biltena kako bi se unaprijedila svijest korisnika informaciono-komunikacionih tehnologija o bezbjednosti informacija.

Dodatne informacije

Sajber pecanje:	https://securingthehuman.sans.org/ouch/2015#december2015
CEO prevara:	https://securingthehuman.sans.org/ouch/2016#july2016
Ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016
Arhive OUCH biltena:	https://securingthehuman.sans.org/ouch/archives

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis Cheryl Conley
Prilagodili: Edin Beriša i Adis Bajramović

Mjesečni bilten za podizanje svijesti o bezbjednosti informacija

Ne dajte se upecati

Uvod

Servisi za razmjenu elektronske pošte i drugih elektronskih poruka (poput Skype, Twitter ili Snapchat poruka) su jedan od osnovnih vidova komunikacije u današnje vrijeme. Koristimo ih ne samo za svakodnevne poslovne potrebe nego i da ostanemo u kontaktu sa prijateljima i članovima porodice. Kako veliki broj ljudi širom svijeta 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 primjer da kliknete na maliciozni link, odate vašu lozinku ili otvorite maliciozan prilog iz mejla. Sajber kriminalci vrijedno rade na kreiranju uvjerljivih poruka koje će uticati na vaše emocije, stvoriti osjećaj 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 izmjeniti tako da poruka djeluje još uvjerljivije. Sajber kriminalci ovakve poruke šalju milionima ljudi. Oni ne znaju ko će zagristi mamac, ali znaju da će što više poruka pošalju, imati više uspjeha.

Kako da se zaštitite

U većini slučajeva bezbjedno je da otvorite i pročitate tijelo mejla ili poruke. Da bi napad pecanjem bio uspješan, loši momci će pokušati da vas prevare da uradite još nešto. Sreća je što postoje načini da prepoznate da je poruka zapravo napad, a ovdje navodimo najuspješnije:

- Poruka stvara osjećaj velike hitnosti i zahtjeva se da što prije 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 ubjeđuje 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.

- Zahtjeva se dostavljanje osjetljivih 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 vjerovati (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 riječi uopšte ne zvuče kao da ih je pisala ta osoba. Ako imate ovakve sumnje, pozovite pošiljaoca telefonom da biste provjerili 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 djeluju čudno, sumnjivo ili previše dobro da bi bili istiniti, moguće je da se radi o pecanju.

Uprava policije Ministarstva unutrašnjih poslova Zeničko dobojskog kantona kao društveno odgovorna institucija pomaže distribuciju ovog biltena kako bi se unaprijedila svijest korisnika informaciono-komunikacionih tehnologija o bezbjednosti informacija.

Gost urednik

Tonia Dadli se od 2011. godine bavi razvojem i implementacijom programa za unapređenje svijesti o bezbjednosti informacija, a njen program za unapređenje svijesti 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 bezbjedni:	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 | Prilagodili: Edin Beriša i Adis Bajramović

OUCH!

SANS SECURITY AWARENESS

Mjesečni bilten za podizanje svijesti o bezbjednosti informacija

Telefonski napadi i prevare

Uvod

Kada razmišljate o sajber kriminalcima vjerovatno vam je pred očima slika zlog genijalca koji sjedi za računarom i pokreće sofisticirane napade preko interneta. Iako u današnje vrijeme mnogi sajber kriminalci koriste tehnologije poput elektronske pošte ili čata, oni se i dalje služe i telefonom kako bi prevarili svoje žrtve. Upotreba telefona ima dvije velike prednosti. Prvo, za razliku od elektronske pošte, mnogo je manje tehnoloških rješenja koja nadgledaju telefonske pozive i koja su u stanju da otkriju i zaustave napad. Druga prednost korištenja telefona je u tome što je mnogo lakše prenijeti emocije putem telefonskog razgovora, zbog čega je vjerovatnije da će prevara biti uspješna. U nastavku teksta saznaćete kako da uočite i zaustavite ovakve napade.

Kako funkcionišu telefonske prevare?

Prvo je neophodno da shvatite šta je cilj ovih napadača. Oni obično žele vaš novac, informacije ili pristup vašem računaru (a ponekad i sve tri stvari). Do željenog dolaze tako što vas prvo prevare da uradite nešto nesmotreno što oni žele. Loši momci telefoniraju ljudima širom svijeta i stvaraju privid situacija koje traže hitnu reakciju. Želja im je da vas izbace iz ravnoteže i uplaše kako biste prestali racionalno da razmišljate i požurili da napravite grešku. Neki od najčešćih primjera su:

Pozivalac se pretvara da je iz poreske uprave ili kancelarije javnog izvršitelja i da imate neplaćene poreze. Objašnjava vam da ćete otići u zatvor, ako odmah ne platite svoja dugovanja, a zatim vas ubjeđuje da dugovanja platite korištenjem vaše platne kartice preko telefona. Ovo je prevara jer mnoga poreska odjeljenja nikada ne zovu niti šalju elektronsku poštu poreskim obveznicima, već se sva službena poreska obavještenja šalju redovnom poštom.

Pozivalac se pretvara da je iz Microsoft-ove tehničke podrške i obavještava vas da je vaš računar zaražen. Kada vas u to ubijedi, predlaže vam da kupite njihov softver ili da mu omogućite udaljeni pristup vašem računaru. Microsoft vas nikada neće zvati na kućni broj.

Dobili ste automatsku govornu poruku da je vaš bankovni račun blokiran i da morate da pozovete određeni telefonski broj kako biste ga odblokirali. Kada pozovete taj broj, javlja vam se govorni automat i traži vam da potvrdite svoj identitet tako što vam postavlja različita pitanja u vezi sa vašim privatnim informacijama. Nije vas pozvala vaša banka, već neko ko prikuplja vaše informacije u cilju krađe identiteta.

Kako da se zaštitite

Imajte na umu da ste vi sami najbolja odbrana od telefonskih prevara koja postoji.

Kad god vas neko pozove i stvara veliki osjećaj hitnosti, ubjeđujući vas da učinite nešto, budite izuzetno sumnjičavi. Čak i u slučaju da telefonski poziv isprva djeluje istinito, a kasnije postane sumnjiv, možete se slobodno predomisliti i reći „ne“ u bilo kom trenutku.

Ako smatrate da je telefonski poziv napad, jednostavno ga prekinite. Ako želite da potvrdite da li je telefonski poziv legitiman, posjetite veb sajt organizacije koja vas je pozvala (na primjer vaše banke), pronađite broj telefona za podršku korisnicima i pozovite ih direktno sami. Na taj način ćete provjeriti da li vas je zvala stvarna organizacija.

Nikada ne vjerujte identifikaciji pozivaoca jer napadači mogu učiniti da telefonski broj pozivaoca izgleda kao da dolazi iz legitimne organizacije ili da ima isti pozivni broj kao vaš broj telefona.

Nikada nemojte dozvoliti da pozivalac preuzme privremenu kontrolu nad vašim računarom ili da vas prevari da instalirate neki softver. Na taj način sajber napadači mogu zaraziti vaš računar.

Ako telefonski poziv dolazi od nekoga koga lično ne poznajete, podesite da poziv ode direktno na vašu govornu poštu. Na taj način ćete moći da pregledate nepoznate pozive u vrijeme koje vama odgovara. Na mnogim telefonima se to omogućava pomoću funkcije “Ne uznemiravaj”.

Prevare i napadi preko telefona su u porastu. Za njihovo prepoznavanje i zaustavljanje najbolja odbrana koju imate ste vi sami.

Uprava policije Ministarstva unutrašnjih poslova Zeničko dobojskog kantona kao društveno odgovorna institucija pomaže distribuciju ovog biltena kako bi se unaprijedila svijest korisnika informaciono-komunikacionih tehnologija o bezbjednosti informacija.

Gost urednik

Džen Foks je senior konsultant u domenu IT bezbjednosti u kompaniji All Covered i bavi se unapređenjem nivoa svijesti o bezbjednosti informacija i socijalnom inženjeringu, kao i procjenama rizika. Možete je pronaći na Tviteru kao @j_fox .

Dodatni materijal

Socijalni inženjering: https://www.sans.org/u/Fi5

Mjesečni bilten za podizanje svijesti o bezbjednosti informacija

Kako izbjeći greške u komunikaciji mejlom

Uvod

Elektronska pošta (mejl) je i dalje jedan od primarnih načina na koji komuniciramo, kako u privatnom tako i u profesionalnom životu. Ipak, vrlo često sami sebi možemo biti najgori neprijatelj kada koristimo ovaj vid komunikacije. U nastavku su opisane četiri najčešće greške koje ljudi prave u komunikaciji mejlom i dati su savjeti kako da ih izbjegnete.

Auto-Complete

Auto-complete (automatsko dovršavanje) je uobičajena funkcionalnost većine mejl klijenata. Auto-complete omogućava da, dok kucate ime osobe kojoj želite da pošaljete mejl, vaš softver za elektronsku poštu automatski dopunjava njenu adresu umjesto vas. Na ovaj način ne morate da pamtite adrese elektronske pošte svih vaših kontakata, već samo njihova imena. Problem nastaje kada imate više kontakata sa sličnim imenima, kada se vrlo lako može desiti da auto-complete izabere pogrešnu adresu elektronske pošte. Na primjer, možda namjeravate da pošaljete mejl sa osjetljivim informacijama vašem kolegi „Petru Petroviću“ iz računovodstva, ali umesto njega, auto-complete odabere mejl adresu vašeg komšije „Petra Pavlovića“. Zbog toga se može dogoditi da osjetljive informacije pošaljete pogrešnoj osobi. Da biste se zaštitili, prije slanja mejlova koji sadrže osjetljive informacije uvijek dva puta provjerite ime i mejl adresu primaoca.

Odgovaranje na mejl

Pored polja „To“, kada pišete mejl, na raspolaganju imate takođe i „Cc:“ opciju. Cc je skraćenica od engleske reči „Carbon copy“ (bukvalan prevod bi bio: indigo kopija) i ova opcija vam omogućava da u mejl prepisku dodate osobe kojima želite da pošaljete kopiju mejla kako bi bile informisane. Kada vam neko pošalje mejl koji sadrži i osobe koje su u polju Cc, na vama je da odlučite da li želite da odgovorite samo pošiljaocu ili svima (Reply-All) koji su uključeni u prepisku. Ako vaš odgovor sadrži osjetljive informacije najvjerovatnije ćete htjeti da odgovorite samo pošiljaocu. U tom slučaju pazite da umjesto opcije „Odgovori“ (Reply) greškom ne upotrijebite opciju „Odgovori svima“ (Reply All) jer biste tako mejl poslali svima koji su u prepisci. Nije na odmet ponoviti još jednom, kad god šaljete ili odgovarate na mejlove koji sadrže osjetljive informacije, prije slanja uvijek dva puta provjerite kome šaljete mejl.

Emocije

Nikada ne šaljite mejl kada ste pod emotivnim nabojem. Takav mejl bi mogao da vam naškodi u budućnosti, a možda čak i da vas košta prijateljstva ili posla. Umjesto toga, izdvojite malo vremena i na miru sredite svoje misli. Ako već morate da izbacite svoje frustracije, započnite novi mejl (provjerite da nema primaoca u polju „To“) i otkucajte upravo ono što ste htjeli da kažete. Onda se udaljite od svog računara, skuhajte sebi kafu, čaj ili prošetajte. Kada se vratite nazad, obrišite mejl i napišite novi ispočetka ili, još bolje, popričajte sa tom osobom telefonom ili licem u lice ako je moguće. Ljudima često može biti teško da razaznaju vaš ton i namjeru samo čitajući mejl, pa vaša poruka izgovorena u telefonskom razgovoru ili uživo može zvučati bolje. Zapamtite da se humor ne prenosi uvek baš najbolje u emotivnim mejlovima, pa ljudi možda neće razumjeti vašu poruku.

Privatnost

Na kraju, imajte na umu da elektronska pošta nema dovoljnu zaštitu privatnosti. Vaš mejl može pročitati svako ko može da mu pristupi, nalik razglednici poslatoj tradicionalnom poštom. Vaš mejl može lako biti proslijeđen drugima, postavljen na javnim forumima, objavljen po sudskoj odluci ili distribuiran dalje ako je server na kome se nalazi hakovan. Ako imate nešto zaista privatno da kažete nekome, pozovite tu osobu telefonom. Takođe, važno je zapamtiti da u mnogim zemljama elektronska pošta može da se koristi kao dokaz na sudu. Najzad, ako za slanje privatnih mejlova koristite vaš računar na poslu zapamtite da vaš poslodavac najvjerovatnije ima pravo da nadzire ili možda čak i da čita vaše mejlove kada koristite kompanijske resurse.

Uprava policije Ministarstva unutrašnjih poslova Zeničko dobojskog kantona kao društveno odgovorna institucija pomaže distribuciju ovog biltena kako bi se unaprijedila svijest korisnika informaciono-komunikacionih tehnologija o bezbjednosti informacija.

Gost urednik

Kit Palmgrin (Keith Palmgren) se bavi bezbjednošću više od 30 godina. On je direktor kompanije NetIP i autor petodnevnog kursa SANS SEC301 – “Introduction to Cyber Security” https://sans.org/sec301.

Dodatni materijal

Ne dajte se upecati: https://www.sans.org/u/IJj

Socijalni inženjering: https://www.sans.org/u/IJo

Upravljajte vašim Auto-complete listama:

Windows Mac

SANS SECURITY AWARENESS
MUPZDK
OUCH! | Novembar 2017
Mjesečni bilten za podizanje svijesti o bezbjednosti informacija

OUCH!

U OVOM BROJU...

- Lažne (onlajn) internet prodavnice
- Vaš računar / mobilni uređaj
- Vaša platna kartica

Bezbjedna kupovina na internetu

Uvod

Sezona praznika se približava i uskoro će milioni ljudi širom svijeta biti u potrazi za savršenim poklonima. Da bi pronašli najpovoljnije ponude i izbjegli gužve i čekanja u dugačkim redovima, mnogi od nas će se odlučiti za kupovinu putem interneta (eng. online shopping). Nažalost, ovo je takođe i doba godine kada mnogi sajber kriminalci prave lažne sajtove za kupovinu u cilju obmane i krađe. U nastavku će biti pojašnjeni rizici kupovine putem interneta i kako da ovu fantastičnu uslugu koristite na bezbjedan način.

Gost urednik
Leni Zelcer radi za kompaniju Minerva Labs koja je specijalizovana za bezbjednosne proizvode i drži predavanja o borbi protiv malvera u SANS Institutu. Leni je aktivan na Tviteru pod nalogom **@lennyzeltser** i autor je bloga o bezbjednosti **zeltser.com**.

Lažne prodavnice na internetu

Iako je većina prodavnica na internetu prava i legitimna, na internetu postoje i lažni veb sajtovi koje su postavili sajber kriminalci. Kriminalci prave ove lažne veb stranice tako što kopiraju izgled pravih sajtova ili koriste imena dobro poznatih prodavnica ili brendova. Oni zatim koriste ove lažne veb stranice da vrebaju ljude koji traže najpovoljnije ponude. Kada na internetu pretražujete apsolutno najniže cene, može se desiti da budete usmjereni na neki od ovih lažnih veb sajtova. Kada birate veb sajtove za kupovinu, budite oprezni kod veb sajtova koji reklamiraju cijene značajno jeftinije od bilo kog drugog sajta ili nude proizvode koji su rasprodati širom zemlje. Razlog zašto su njihovi proizvodi tako jeftini ili dostupni je u tome što prodaju ono što nije legitimno, može biti falsifikovano ili ukradeno, ili u nekim slučajevima nikada i ne bude isporučeno. Zaštitite sebe primjenom sledećih savjeta:

- Kad god je to moguće, kupujte sa veb sajtova koji su vam poznati, kojima vjerujete i već ste kupovali na njima.
- Provjerite da li veb sajt ima ispravnu poštansku adresu i telefonski broj za pitanja u vezi prodaje ili podrške. Ako sajt izgleda sumnjivo, pozovite ih i razgovarajte uživo. Ako ne možete da dobijete nekoga sa kime biste razgovarali, to je prvi veliki znak za vas da imate posla sa lažnim veb sajtom.
- Potražite očigledne znakove upozorenja kao što su ponude koje su očigledno previše dobre da bi bile istinite, gramatičke i pravopisne greške.
- Budite veoma obazrivi ako veb sajt izgleda kao identična kopija dobro poznatog veb sajta kojeg ste ranije koristili, ali je ime domena veb sajta ili ime prodavnice malo drugačije. Na primjer, možda za kupovinu putem interneta koristite

Bezbjedna kupovina na internetu

Amazon, čija je veb stranica na adresi https://www.amazon.com. Stoga budite vrlo sumnjičavi ako se nađete na sajtovima koji se pretvaraju da su Amazon, kao što je http://store-amazoncom.com.

- Ukucajte ime ili URL prodavnice u pretraživač i pogledajte šta su drugi ljudi rekli o tom veb sajtu. Potražite pojmove kao što su “prevara”, “nikad više” ili “lažni” (eng. „fraud”, „scam”, „never again“, „fake“). Nedostatak komentara o sajtu takođe može biti znak koji ukazuje da je njegova veb lokacija nova i možda nije pouzdana.
- Prije nego što bilo šta kupite putem interneta provjerite da li je vaša veza sa veb sajtom šifrovana (enkriptovana). Većina pregledača šifrovanu vezu ilustruje katancem i/ili slovima HTTPS u zelenoj boji neposredno prije naziva veb sajta.

Zaštitite se prilikom kupovine na internetu tako što ćete kupovati samo na pouzdanim veb sajtovima sa dokazanom reputacijom.

Zapamtite, samo zato što sajt izgleda profesionalno ne znači da je pravi. Ako niste sigurni u bezbjednost veb sajta, nemojte ga koristiti. Umjesto toga, pronađite poznati veb sajt kome vjerujete ili ste ga već koristili bezbjedno u prošlosti. Možda tu nećete pronaći najpovoljniju moguću ponudu, ali je mnogo veća vjerovatnoća da ćete dobiti očekivani proizvod i izbjeći da vam lični i finansijski podaci budu ukradeni.

Vaš računar / mobilni uređaj

Pored izbjegavanja kupovine na lažnim veb sajtovima, postarajte se i da vaš računar ili mobilni uređaj bude bezbjedan. Sajber kriminalci će pokušati da zaraze vaše uređaje kako bi mogli da prikupe informacije o vašim bankovnim računima, platnim karticama i lozinkama. Preduzmite sljedeće korake kako biste obezbjedili vaše uređaje:

- Ako u kući imate djecu, razmislite o tome da imate dva uređaja, jedan za vašu djecu i jedan za odrasle. Djeca su radoznala i interaktivna s tehnologijom, pa je veća vjerovatnoća da će zaraziti svoj uređaj. Korištenjem zasebnog računara ili tableta samo za onlajn transakcije, poput elektronskog bankarstva i kupovine na internetu, smanjujete šansu da budete zaraženi.
- Uvijek instalirajte najnovije ispravke i koristite ažuran antivirusni softver. Na taj način značajno otežavate sajber kriminalcu da zarazi vaš uređaj.

Vaša platna kartica

Redovno provjeravajte izvode sa platne kartice kako biste identifikovali sumnjive troškove, naročito nakon što ste učestalo

Bezbjedna kupovina na internetu

koristili svoje kartice za kupovinu na internetu ili ste koristili novi sajt za kupovinu. Neki provajderi platnih kartica vam pružaju mogućnost obavještavanja putem elektronske pošte ili sms poruka svaki put kada se sa vaše kartice skinu određena sredstva ili kada troškovi prelaze određeni iznos. Druga mogućnost je da imate jednu platnu karticu samo za kupovinu na internetu, na ovaj način ako vam kartica bude kompromitovana možete je lako zamijeniti, bez ikakvih posljedica na bilo koje vaše druge aktivnosti plaćanja. Ako vjerujete da je izvršena prevara, odmah obavjestite kompaniju koja vam je izdala platnu karticu. Ovo je takođe razlog zašto je bolje da za onlajn kupovinu koristite kreditne kartice i izbjegavate korištenje debitnih kartica kad god je to moguće. Debitne kartice skidaju novac direktno sa vašeg bankovnog računa, pa se u slučaju prevare može desiti da teže povratite svoj novac. Konačno, razmotrite korištenje platnih kartica koje generišu jedinstveni broj kartice za svaku onlajn kupovinu, poklon kartica ili koristite dobro poznate servise za plaćanja, kao što je PayPal, koji ne zahtjevaju da otkrijete broj vaše kreditne kartice prodavcu.

Saznajte više

Prijavite se na OUCH! mjesečni bilten za podizanje svijesti o bezbjednosti informacija namjenjen svima, pročitajte prethodne brojeve OUCH!-a i saznajte više o SANS-ovim rješenjima za unapređenje svijesti o bezbjednosti informacija na našoj internet prezentaciji securingthehuman.sans.org/ouch/archives.

Uprava policije Ministarstva unutrašnjih poslova Zeničko dobojskog kantona kao društveno odgovorna institucija pomaže distribuciju ovog biltena kako bi se unaprijedila svijest korisnika informaciono-komunikacionih tehnologija o bezbjednosti informacija.

Dodatne informacije

Socijalni inženjering:	https://securingthehuman.sans.org/ouch/2017#january2017
Četiri koraka da ostanete bezbjedni:	https://securingthehuman.sans.org/ouch/2016#october2016
Bezbjednost vaše kućne mreže:	https://securingthehuman.sans.org/ouch/2016#february2016
SANS bezbjednosni savjet dana:	https://www.sans.org/tip_of_the_day.php

Redakcija: Walt Scrivens, Phil Hoffman, Кэти Клик, Cheryl Conley
Prilagodili: Edin Beriša i Adis Bajramović

Mjesečni bilten za podizanje svijesti o bezbjednosti informacija

Savjeti za bezbjedno korištenje društvenih mreža

Uvod

Društvene mreže (socijalni mediji) kao što su Snapchat, Facebook, Tvitter, Instagram i LinkedIn su moćni resursi koji vam omogućavaju da se upoznate, komunicirate i dijelite informacije sa ljudima širom svijeta. Međutim, uz svu ovu moć dolaze i rizici, ne samo za vas već i za vašu porodicu, prijatelje i poslodavce. U ovom tekstu predstavljeni su ključni koraci za bezbjedno korištenje društvenih mreža.

Objavljivanje

Budite oprezni i razmislite prije nego što nešto objavite na društvenoj mreži. Sve što objavite (postujete na društvenim mrežama) će u nekom trenutku najvjerovatnije postati javno, utičući na vašu reputaciju i budućnost, uključujući i to gdje možete da nastavite školovanje ili koji posao možete da dobijete. Ukoliko ne želite da vaša porodica ili vaš šef nešto vide, to najvjerovatnije ne bi trebalo ni da objavite. Takođe, trudite se da budete svjesni onoga što drugi objavljuju o vama. Možda će biti potrebno da od njih zahtjevate da uklone nešto što su objavili o vama.

Privatnost

Skoro sve društvene mreže imaju mnoštvo opcija u vezi sa privatnošću, uključite ih kad god je to moguće. Provjerite, npr. da li je zaista neophodno da društvenoj mreži bude omogućeno da prati vašu lokaciju? Dodatno, opcije u vezi sa privatnošću se često mijenjaju i mogu biti zbunjujuće. Steknite naviku da ih provjeravate i potvrđujete da one funkcionišu onako kako to vi očekujete.

Pristupne fraze

Obezbjedite vaš nalog na društvenim mrežama dugačkom, jedinstvenom pristupnom frazom. Pristupna fraza je lozinka sačinjena od više riječi što je čini lakšom za unos i pamćenje, ali teškom za pogađanje od strane sajber napadača.

Obezbjedite svoj nalog

Štaviše, omogućite dvo-faktorsku autentifikaciju na svim vašim nalozima. Ovakav vid autentifikacije dodaje jednokratni kod (eng. one time code) vašoj lozinci kada hoćete da se prijavite na vaš nalog. Ovo je veoma jednostavna mjera i jedan od najboljih načina da obezbjedite vaš nalog.

Prevare

Kao i kod elektronske pošte sajber kriminalci mogu pokušati da vas prevare korištenjem poruka koje se razmjenjuju putem društvenih mreža. Na primjer, mogu da vas prevare da im otkrijete lozinku ili podatke sa platne kartice. Budite obazrivi na šta klikate: ako vam prijatelj pošalje poruku koja izgleda neobično ili ne liči na nešto što bi on poslao, možda je u pitanju sajber napadač koji se predstavlja kao vaš prijatelj.

Uslovi korištenja

Upoznajte se sa uslovima korištenja društvenih mreža. Bilo šta što postavite ili objavite na društvenoj mreži može postati vlasništvo društvene mreže.

Poslovno okruženje

Ako hoćete da objavite bilo šta što ima veze sa poslom provjerite prvo sa vašim nadređenim da li je prihvatljivo da javno podijelite te informacije.

Pratite ove savjete kako biste uživali u društvenim mrežama na bezbjedan način. Da biste saznali više o tome kako da bezbjedno koristite sajtove pojedinih društvenih mreža ili kako da im prijavite neovlaštene aktivnosti, posjetite stranicu posvećenu bezbjednosti na tim društvenim mrežama.

Uprava policije Ministarstva unutrašnjih poslova Zeničko dobojskog kantona kao društveno odgovorna institucija pomaže distribuciju ovog biltena kako bi se unaprijedila svijest korisnika informaciono-komunikacionih tehnologija o bezbjednosti informacija.

Gost urednik

Džesika Barker je ekspert za ljudsku stranu sajber bezbjednosti. Ona je suosnivač kompanije Redacted Firm u kojoj pruža konsultantske usluge klijentima širom svijeta, Džesika je takođe i dobro poznati govornik. Pratite je na tviteru @drjessicabarker

Dodatne informacije

Pristupne fraze:	https://www.sans.org/u/B6E
Dvo-faktorska autentifikacija:	https://www.sans.org/u/B6J
Zaštite djece na internetu:	https://www.sans.org/u/B6O
Obezbjedite svoj nalog:	https://www.lockdownyourlogin.org/

Licenca

Redakcija: Walt Scrivens, Phil Hoffman, Кэти Клик, Cheryl Conley | Prilagodili: Edin Beriša i Adis Bajramović

OUCH! | Maj 2017

Mjesečni bilten za podizanje svijesti o bezbjednosti informacija

OUCH!

U OVOM BROJU...

- Edukacija i komunikacija
- Tehnološka zaštita
- Budite dobar primjer djeci

Zaštita djece na Internetu

Uvod

Načini na koji današnja djeca mogu da pristupe Internetu i budu u interakciji sa drugima su zapanjujući. Društveni život i budućnost djece zavise od njihove sposobnosti da koriste novu tehnologiju i sve njene prednosti, bilo da su to nove aplikacije za društvene medije, kompjuterske igrice ili školski računari. Kao roditelji želimo da budemo sigurni da tehnologiju koriste na bezbjedan način. Međutim, ovo može da bude veliki izazov, pošto mnogi od nas nisu odrastali u tehnološkom okruženju nalik sadašnjem. Da bismo vam pomogli, u ovom tekstu su obrađeni ključni koraci koji omogućavaju da današnja djeca koriste tehnologiju na siguran i bezbjedan način.

Gost urednik

Adrien de Beaupre je sertifikovani SANS instruktor i autor SANS kursa koji radi kao nezavisni penetracioni tester u Otavi, glavnom gradu Kanade. Kada se ne bavi tehnološkim novotarijama, vrijeme provodi sa svojom porodicom ili trenirajući. Tviter nalog: **@adriendb**

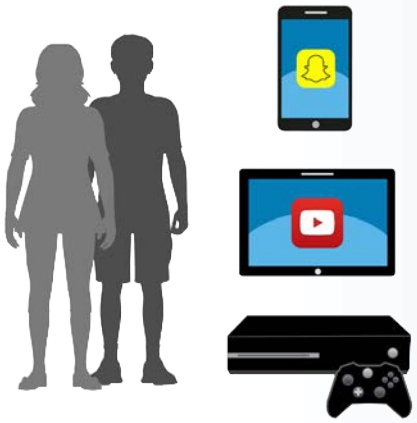
Edukacija i komunikacija

Prva i najvažnija stvar koju možete preduzeti je komunikacija. Potrudite se da uvijek pričate sa vašom djecom i da ona razgovaraju sa vama. Prečesto roditelji budu zaneseni modernom tehnologijom, pa ih interesuje samo koje aplikacije su dobre ili loše ili koji je najbolji softver za zaštitu djece. Zaboravlja se da ovde nije riječ samo o tehnološkom izazovu, već je prije svega riječ o vrijednosnom sistemu i načinu ponašanja. Svi mi želimo da se djeca na Internetu ponašaju isto kao i u stvarnom svijetu. Dobar način za početak je da zajedno sa svojom djecom napravite listu pravila ili očekivanja za korištenje moderne tehnologije. U nastavku su neke stavke koje treba da razmotrite (ne zaboravite da pravila treba da se mijenjaju kako djeca odrastaju):

- Vrijeme kada mogu ili ne mogu da budu na Internetu, i koliko dugo.
- Pitajte vašu djecu ko su njihovi prijatelji ili pratioci na Internetu i kako su postali prijatelji. Da li ona zaista poznaju ljude s kojima su povezani putem Interneta?
- Razgovarajte o vrstama veb sajtova koje bi trebalo da posjećuju, a koje ne kao i o kompjuterskim igricama koje su prikladne, a koje ne i zašto.
- Koje informacije mogu da dijele i sa kim. Djeca često ne shvataju da je ono što objavljuju javno i da ostaje trajno na Internetu. Pored toga, djeca mogu da misle da neku tajnu dijele samo sa jednom osobom, a ta tajna može vrlo lako da postane dostupna svima.

Zaštita djece na Internetu

- Kome da se obrate u slučajevima kada ih neko zastrašuje ili se ponaša nasilnički na Internetu.
- Neka se na Internetu prema drugima ponašaju onako kako žele da se drugi ophode prema njima.
- Anonimnost na Internetu ne postoji, ljudi mogu da saznaju ko si.
- Ljudi na Internetu ne moraju biti oni za koje se predstavljaju.



Ključ za zaštitu djece na Internetu je da ih edukujete o opasnostima sa kojima se suočavaju i da postignete ne samo da vi pričate njima, već da se i ona obraćaju vama.

Kada su u pitanju starija djeca, jedna od mogućnosti je da ova pravila vežete za njihove ocjene u školi, završetak kućnih poslova ili način na koji se ophode prema drugima. Što je njihovo ponašanje u stvarnom svijetu bolje, biće im dopušteno više stvari na Internetu. Kada uvedete pravila, postavite ih na vidno mjesto, na primjer pored porodičnog računara ili na vrata dječije sobe. Još bolja opcija je da djeca pregledaju i potpišu dokument jer na taj način potvrđuju svoju saglasnost sa dogovorenim. Što ranije sa djecom počnete da pričate o vašim očekivanjima, to će rezultati biti bolji. Niste sigurni kako da započnete razgovor, naročito sa starijom djecom? Pitajte ih koje aplikacije koriste i kako one rade. Stavite vaše dijete u ulogu učitelja i dopustite mu da vam pokaže šta radi na Internetu.

Tehnologija

Pored edukacije možete koristiti i tehnološka rješenja za nadzor i zaštitu vaše djece. Ovakva tehnološka rješenja najbolje funkcionišu kada su mlađa djeca u pitanju, posebno rješenja za zaštitu od slučajnog pristupa neprikladnom ili štetnom sadržaju. Međutim, tehničke mjere ne funkcionišu najbolje kako djeca odrastaju. Starija djeca ne samo da zahtjevaju veći pristup Internetu, već često koriste uređaje koji vi ne kontrolišete ili ne možete da nadzirete, poput školskih računara, konzola za igrice ili računara kod rođaka ili prijatelja. Zato je edukacija toliko važna.

Još jedna stvar koju možete preduzeti je da imate poseban računar samo za vašu djecu. Na ovaj način spriječavate da ona slučajno zaraze vaš računar koji koristite za osjetljivije aktivnosti, kao što je online bankarstvo. Kao dodatnu mjeru, njihov računar postavite na prometnom, vidnom mjestu tako da možete da nadzirete njihove aktivnosti. To što oni kažu da rade domaći, ne mora da znači da se stvarno time bave. Na kraju, osigurajte da računar bude zaštićen, da se redovno radi bekap i da djeca nemaju administratorska prava na njemu. Za mobilne uređaje, predvidite jedno mjesto u kući za punjenje baterija uređaja. Prije nego što uveče djeca krenu na spavanje, neka sve mobilne uređaje priključe na ovo mjesto i tako neće doći u iskušenje da ih koriste u doba kad bi trebalo da spavaju.

Zaštita djece na Internetu

Budite dobar primjer djeci

Imajte na umu da, kao roditelji, treba da budemo dobar primjer svojoj djeci. To znači da, kada dijete razgovara sa vama, treba da odložite svoj uređaj i sa djecom razgovarate dok ih gledate u oči. Razmotrite da uvedete pravilo da dok večerate zajedno ne koristite digitalne uređaje i da nikada ne kuckate poruke dok vozite. Na kraju, kada djeca načine grešku, iskoristite je kao iskustvo na kome se uči, umjesto da odmah posegnete za kaznom. Svaki put objasnite „zašto“ i podsjetite ih da samo pokušavate da ih zaštitite od opasnosti kojih ona još nisu svjesna. Dajte im do znanja da mogu da vam se obrate ako i kada dožive neku neprijatnost na Internetu, možda čak i da vam naprave snimak ekrana (screenshot) koji bi mogli da vam pokažu. Potrudite se da djeci ne bude neprijatno da vam se obrate kad shvate da su uradila nešto što nije trebalo. Održavanje otvorene i žive komunikacije je najbolji način da pomognete djeci da budu bezbjedna u današnjem digitalnom svijetu.

Saznajte više

Prijavite se na OUCH! mjesečni bilten za podizanje svijesti o bezbjednosti informacija namjenjen svima, pročitajte prethodne brojeve OUCH!-a i saznajte više o SANS-ovim rješenjima za unapređenje svijesti o bezbjednosti informacija na našoj internet prezentaciji securingthehuman.sans.org/ouch/archives.

Uprava policije Ministarstva unutrašnjih poslova Zeničko dobojskog kantona kao društveno odgovorna institucija pomaže distribuciju ovog biltena kako bi se unaprijedila svijest korisnika informaciono-komunikacionih tehnologija o bezbjednosti informacija.

Dodatne informacije

RSAC CyberSafety: Kids:	https://www.rsaconference.com/safety
NCSA:	https://staysafeonline.org/stay-safe-online/for-parents
FOSI:	https://www.fosi.org/good-digital-parenting
UK’s National Crime Agency:	https://www.thinkuknow.co.uk

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Кэти Клик, Cheryl Conley
Prilagodilii: Edin Beriša i Adis Bajramović

OUCH! | Avgust 2018

OUCH!

SANS SECURITY AWARENESS

Mjesečni bilten za podizanje svijesti o bezbjednosti informacija

Pametni kućni uređaji

Šta su pametni kućni uređaji?

Do skora je bilo uobičajeno da su samo pojedini uređaji koje imate kod kuće (laptop, pametni telefon ili konzola za igru) mogli da se povežu na internet. Međutim, danas se sve više i više vaših uređaja, počev od sijalica i zvučnika na televizoru do brave na ulaznim vratima pa čak i automobila, povezuje na internet. Uskoro će skoro svaki uređaj u vašoj kući imati mogućnost povezivanja na internet. Ovi povezani uređaji često se nazivaju Internet stvari (eng. Internet of Things, IoT) ili pametni kućni uređaji. Iako ovi povezani uređaji unose velike pogodnosti u svakodnevni život, oni donose i sebi svojstvene opasnosti.

U čemu je problem?

Što je više uređaja koji su povezani na vašu kućnu mrežu, to su veće šanse da nešto krene po zlu. Hakeri mogu programirati vaše uređaje da napadaju druge, proizvođači mogu prikupljati detaljne informacije o vašim aktivnostima ili se vaši uređaji mogu zaraziti i zaključati vas. Mnoge kompanije koje proizvode ove uređaje nemaju iskustva sa sajber bezbjednošću i vide bezbjednost kao dodatni trošak. Kao posljedica toga, brojni uređaji koje kupujete imaju malo ili nimalo ugrađenih bezbjednosnih komponenti. Na primjer, neki uređaji imaju predefinisane (unaprijed postavljene) lozinke koje su dobro poznate i ne mogu se promijeniti.

Kako da se zaštitite

Šta možete da učinite kako biste povezane uređaje koristili na bezbjedan i siguran način? Ovi uređaji mogu da pruže izvanredne funkcije koje olakšavaju svakodnevni život. Pored toga, kako tehnologija brzo napreduje, možda jednostavno nećete imati izbora osim da koristite pametne uređaje. U nastavku navodimo ključne korake koje možete preduzeti da biste se zaštitili.

Povežite samo ono što je potrebno: Najjednostavniji način obezbjeđivanja uređaja jeste da ga ne povežete sa internetom. Ako nije neophodno da vaš uređaj bude dostupan sa interneta, nemojte ga ni povezivati na vašu Wi-Fi mrežu. Da li je zaista neophodno da vam toster šalje obavještenja na telefon?

Znajte šta ste povezali: Koji uređaji su vam povezani sa kućnom mrežom? Niste sigurni ili ne možete da se sjetite? Isključite vašu bežičnu mrežu i provjerite šta više ne radi. Možda na ovaj način nećete otkriti sve uređaje, ali ćete se iznenaditi za koliko ste uređaja zaboravili da su uopšte povezani.

Ažurirajte uređaje: Važi isto što i za vaš računar i mobilne uređaje, od ključnog je značaja da ažurirate sve vaše uređaje. Ako uređaj posjeduje mogućnost automatskog ažuriranja, uključite je.

Lozinke: Zamijenite lozinke na vašim uređajima sa jedinstvenim i jakim pristupnim frazama koje samo vi znate. Nove lozinke ćete najvjerovatnije morati da unesete samo jednom. Ne možete da se sjetite svih vaših lozinki ili fraza za pristup? Ne brinite, ne možemo ni mi. Razmislite o korištenju menadžera lozinki da biste ih čuvali na bezbjedan način.

Postavke privatnosti: Ako vaš uređaj dozvoljava da konfigurišete opcije vezane za privatnost, iskoristite ih da ograničite količinu informacija koje uređaj prikuplja ili dijeli. Jedna od opcija je i da onemogućite bilo kakvo dijeljenje informacija.

Proizvođač: Kupujte uređaje od kompanije koju poznajete i kojoj vjerujete. Potražite proizvode koji imaju opcije vezane za bezbjednost, kao što su mogućnost automatskog ažuriranja, izmjena podrazumjevane lozinke i promjena postavki privatnosti.

Stalno slušanje: Ako uređaj može da prima vaše glasovne komande, on neprestano sluša. Zato budite svjesni da vaši Aleksa i Google Home uređaji mogu snimati osjetljive razgovore, uzmite to u obzir kada odlučujete gdje ćete u vašem domu postaviti uređaje i obavezno preispitajte njihove postavke privatnosti.

Gost mreža: Razmislite o tome da svoje pametne kućne uređaje smjestite u zasebnu „Gost“ Wi-Fi mrežu umjesto na osnovnu Wi-Fi mrežu koju koristite za računare i mobilne uređaje. Na ovaj način, u slučaju da neki pametni uređaj bude zaražen malverom, računari ili mobilni uređaji na vašoj glavnoj mreži će ostati zaštićeni.

Nema razloga za strah od novih tehnologija, ali budite svjesni rizika koji njihovo korištenje nosi sa sobom. Primjena ovih nekoliko jednostavnih savjeta može vam pomoći da napravite daleko bezbjedniji digitalni dom.

Uprava policije Ministarstva unutrašnjih poslova Zeničko dobojskog kantona kao društveno odgovorna institucija pomaže distribuciju ovog biltena kako bi se unaprijedila svijest korisnika informaciono-komunikacionih tehnologija o bezbjednosti informacija.

Gost urednik

Robert M. Li (@RobertMLee) je SANS-ov sertifikovani predavač i autor kurseva o sajber prijetnjama i odgovoru na incidente, „FOR578 - Cyber Threat Intelligence“ i „ICS515 - ICS Active Defense and Incident Response“. Robert je, takođe, direktor i osnivač kompanije Dragos koja se bavi sajber bezbjednošću u industrijskim sistemima.

Dodatni materijal

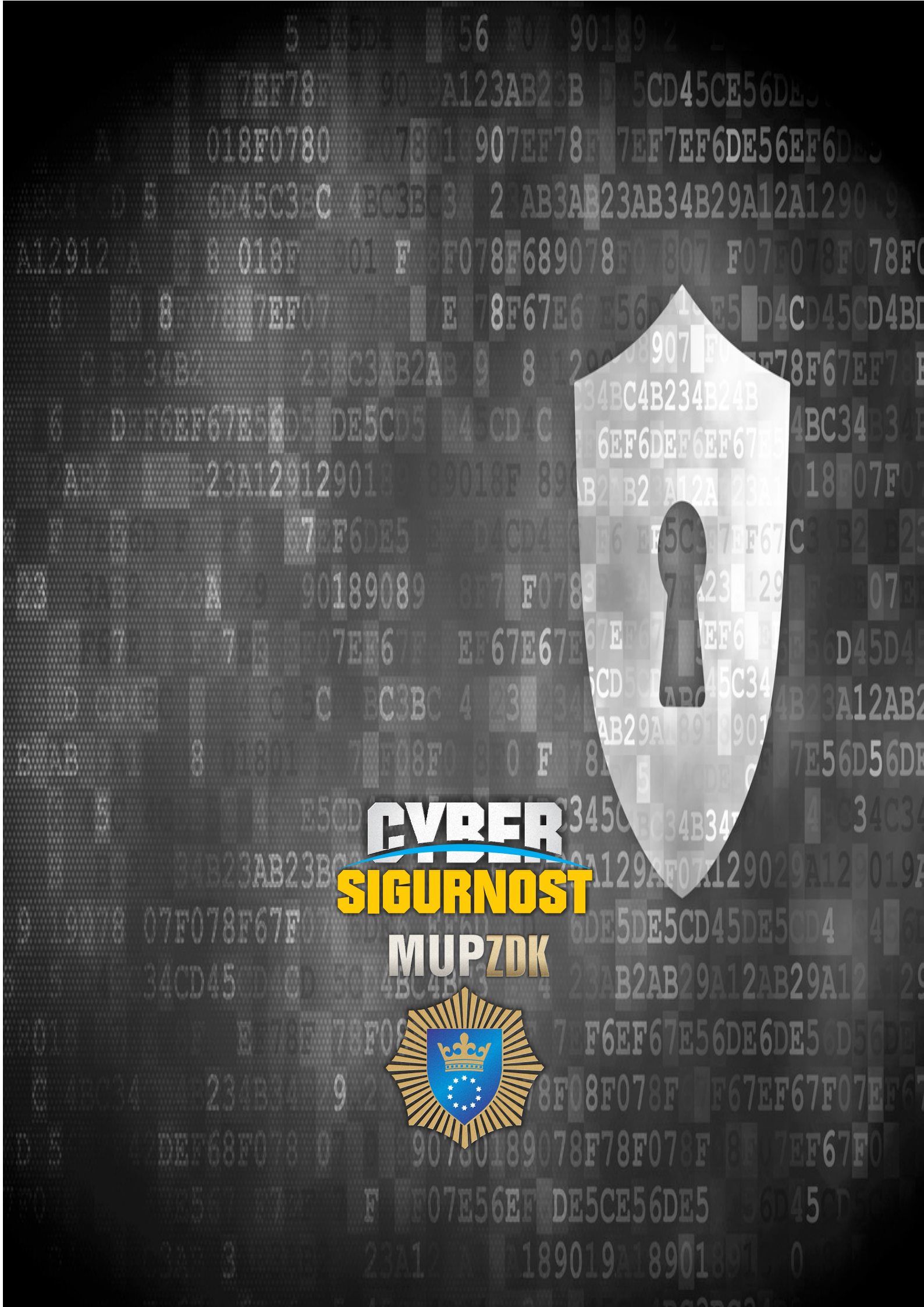
Pristupne fraze:	https://www.sans.org/u/GEB
Menadžeri lozinki:	https://www.sans.org/u/GEG
Bezbjednost vaše kućne mreže:	https://www.sans.org/u/GEL

MUPZDK

SAVJETI ZA KREIRANJE DOBRE LOZINKE

- Nemojte koristiti jednostavne, lake za pogoditi lozinke kao što su imena prijatelja, porodice i kućnih ljubimaca. Nemojte koristiti riječi iz riječnika ili često korištene lozinke kao što su 12345 ili QWERTY.
- Nemojte dijeliti lozinke sa drugim ljudima. Ako im je potreban pristup podacima, treba im se kreirati vlastiti korisnički račun.
- Nemojte ostavljati lozinke na vidnim mjestima u sveskama, na ljepljivim podsjetnicima pored vašeg računara ili u lako dostupnim i nezaštićenim fajlovima na vašem računaru.
- Prije nego što unesete lozinku na veb lokaciju, uvjerite se da koristi zaštićenu vezu koja počinje sa https: // (takođe može prikazati i mali katanac blizu adrese) to znači da sajt koristi zaštićenu vezu koju ne mogu presresti napadači.
- Kada se registrujete sa nekim onlajn uslugama, oni će vam poslati lozinku tako da se možete prijaviti. Mnoge stranice vas prisiljavaju da promijenite lozinku kada se prvi put prijavite, a ako ne, promijenite lozinku kada prvi put posjetite stranicu.
- Ako je moguće, promijenite podrazumijevanu lozinku na uređajima kao što je vaš Internet ruter. On je programiran u fabrici, a neke kompanije imaju jednu lozinku za sve svoje uređaje. Napadač mora samo da zna model rutera kako bi imao pristup.
- Ako imate problema da zapamtite lozinke koristite program za upravljanje lozinkama koji ne samo da čuva lozinke, već može generisati i nove, veoma složene lozinke za vas.
- Dvostruka autentikacija vam pruža dodatnu zaštitu jer zahtijeva dvije informacije (poput lozinke i slučajnog broja poslatog putem SMS-a ili pametnog telefona) kako biste omogućili pristup svojim podacima. **Ako kompanija nudi dvostruku autentikaciju, trebate je koristiti.**

CYBER SIGURNOST


CYBER
SIGURNOST
MUPZDK