Buletini mujor për vetëdijësimin mbi sigurinë e përdoruesve të kompjuterëve

OUCH!

NË KËTË EDICION..

- **Pasfrazat**
- **Përdorimi i sigurt i pasfrazave**
- **Burimet**

Pasfrazat

Hyrje

Fjalëkalimet (ang. Passwords) janë diçka që ju përdorni gati përditë, duke filluar nga qasja në emailin tuaj apo llogarinë tuaj bankare online deri te blerja online apo qasja në telefonin tuaj të zgjuar – smartphone. Por, fjalëkalimet tuaja janë njëkohësisht edhe pikat më të dobëta, nëse dikush e mëson fjalëkalimin tuaj ata mund të ju vjedhin identitetin tuaj, të transferojnë paratë tuaja apo t'i qasen informatave tuaja personale. Fjalëkalimet e forta janë pjesa kyçe e mbrotjes suaj. Në këtë botim ju do të mësoni si të krijoni fjalëkalime të forta që janë lehtë për t'u mbajtur mend duke përdorur fjalëkalime të quajtura pasfraza (ang. passphrase).

Botuesi i ftuar

Guy Bruneau është konsulent me eksperiencë në IPSS Inc., instruktor i SANS si dhe drejtues i ISC. Guy e udhëheq SANS GSE dhe e ka përfunduar programin e SANS Cyber Guardian. Ju mund ta ndiqni Guy-in në Twitter si **@GuyBruneau** dhe në **handlers.sans.org/gbruneau**.

Pasfrazat

Sfida që ne ballafaqohemi është se sulmuesit kibernetikë kanë zhvilluar mënyra të sofistikuara që të qëllojnë apo godasin (ang. Brute force) fjalëkalimet, dhe çdo herë e më shumë po bëhen edhe më efikasë. Kjo do të thotë që për ta është e lehtë t'i thyejnë apo qëllojnë fjalëkalime tuaja nëse janë të dobët apo të lehtë për t'u qëlluar. Një hap i rëndësishëm është të përdoren fjalëkalime të forta. Sa më shumë karaktere (shkronja, numra e shenja) që ka fjalëkalimi juaj, aq më i fortë është dhe është më i vështirë për t'u qëlluar nga sulmuesit. Por fjalëkalimet e gjata dhe komplekse është vështirë të mbahen mend. Në vend të tyre ne ju rekomandojmë të përdorni pasfraza, këto janë fraza të thjeshta apo fjali që janë të lehta të mbahen mend, por të vështira të thyhen. Ja një shembull:

Ku eshte mbreti Julian?

Ajo që e bën këtë pasfrazë kaq të fortë është jo vetëm gjatësia që është 21 karakteresh, por edhe përdorimi i shkronjave të mëdha dhe simboleve (mos harroni, hapësirat dhe shenjat e pikësimit janë simbole). Ju mund ta bëni pasfrazën tuaj edhe më të fortë duke zëvendësuar shkronjat me numra apo simbole, si p.sh. shkronjën 'a' me simbolin '@' ose shkronjën 'o' me numrin zero. Nëse një uebfaqe apo program ju limiton në numrin e karaktereve që mund të përdorni, atëherë përdorni numrin maksimal të lejuar.

Pasfrazat

Përdorimi i sigurt i pasfrazës

Ju duhet të keni kujdes se si i përdorni pasfrazat. Përdorimi i pasfrazave nuk na ndihmon nëse njerëzit dashakeqë mund t'a vjedhe apo kopjojë atë.

Përdorimi i pasfrazave është një nga mënyrat dhe hapat më efektive që ju mund të ndërmerrni të mbroni identitetin dhe infromatat tuaja.

1. Sigurohuni që keni pasfraza të ndryshme për çdo llogari apo pajisje që keni. Për shembull kurrë mos përdorni të njejtën pasfraz për llogarinë tuaj të punës ose llogarinë bankare me llogarinë personale si për shembull ajo në Facebook, Youtube apo Twitter. Në këtë mënyrë, nëse njëra nga llogaritë tuaja manipulohet atëherë llogaritë tjera i keni të sigurta. Nëse keni shumë pasfraza që duhet t'i mbani mend (gjë që ndodh), atëherë provoni të përdorni menaxhues të fjalëkalimeve (ang. Password manager). Ky është një program special që ruan në mënyrë të sigurt të gjitha pasfrazat tuaja. Në këtë mënyre ju duhet të mbani mend vetëm pasfrazën për qasje në kompjuter dhe atë të menaxhuesit të fjalëkalimeve.

2. Kurrë mos ia tregoni dikujt pasfrazën tuaj, apo mënyrën si i krijoni pasfrazat. Mos harroni, pasfraza është një sekret; nëse dikush e di pasfrazën tuaj atëherë nuk është më e sigurt. Nëse aksidentalisht ia jepni dikujt pasfrazën tuaj, ose mendoni që dikush mund ta ketë vjedhur apo kompromet uar pasfrazën tuaj, sigurohuni që ta ndërroni menjëherë.

3. Sikurse fjalëkalimet, kini kujdes në përzgjedhjen e pasfrazave të përdorura shpesh apo që janë të lehta për t'u qëlluar.

4. Mos përdorni kompjutera publikë si ato në hotele e librari, për të hyrë në llogarinë tuaj të punës apo llogarinë tuaj bankare. Pasi që këta kompjuterë mund të përdoren nga çdokush, ato mund të infektohen me kode apo softuerë të dëmshëm dhe që mund të kopjojë çdo shtypje të tastierës. Gjithmonë qasuni në llogarinë tuaj të punës apo llogarinë bankare vetëm nga kompjuterët apo pajisjet mobile të besueshme.

5. Kujdes nga uebfaqet që ju kërkojnë t'i përgjigjeni pyetjeve personale. Këto pyetje përdoren në raste kur ju harroni pasfrazën tuaj dhe ju duhet ta resetoni atë. Problemi me këto pyetje është se përgjigjjet e tyre nganjeherë mund të gjenden në Internet apo edhe në faqen tuaj të Facebook-ut. Sigurohuni që ju i përgjigjeni pyetjeve personale dhe ato informata nuk gjenden lehtësisht në internet. Menaxhuesit e fjalëkalimeve mund t'ju ndihmojnë në këto raste, sepse mund të ruajnë edhe këto informata aty.

Pasfrazat

6. Shumë llogari online ofrojnë një shërbim që quhet “autentifikimi me dy faktorë” apo verifikimi në dy hapa. Në këtë rast do të duhet më shume se vetëm pasfrazën për t’u kyçur, d.m.th. një kod shtesë i dërguar në telefonin tuaj. Ky opsion është më i sigurt se përdorimi vetëm i pasfrazës. Atëherë kur është e mundur gjithmonë përdorni mënyrën më të sigurt të autentifikimit.

7. Pajisjet mobile shpesh kërkojnë kod PIN për të mbrojtur qasjen në to. Kini parasysh që një kod PIN është thjesht një fjalëkalim më shumë. Sa më i gjatë të jetë kodi PIN, aq më i sigurt është. Shumica e pajisjeve mobile ofrojnë që në vend të kodit PIN të përdorni një pasfrazë.

8. Në fund, nëse nuk jeni duke e përdorur një llogari, sigurohuni ta mbyllni, fshini ose ta çaktivizoni atë.

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

Verifikimi në dy hapa:	http://www.securingthehuman.org/ouch/2013#august2013
Menaxhuesit e fjalëkalimeve:	http://www.securingthehuman.org/ouch/2013#october2013
Inxhinjeria sociale:	http://www.securingthehuman.org/ouch/2014#november2014
Shprehje të shpeshta të TI-ve:	http://www.securingthehuman.org/resources/security-terms

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