Izvor: tehnoklik.net.hr

Garry Sidaway je direktor strategije sigurnosti u Integralisu, tvrtki koja savjetuje Vladu Velike Britanije te farmaceutske i financijske multinacionalke.

»Kriminalci točno znaju kakve podatke traže na internetu i gdje se oni nalaze«, rekao je Sidaway koji misli kako su Britanci, a to vrijedi i za ostale narode, prenaivni što se tiče objave i pohranjivanja podataka na internetu.

Danas smo svjedoci velikog broja različitih napada hakera – od pokušaja »izvlačenja« lozinki kroz linkove-zamke postavljene na stranice koje se podrazumijevaju da su sigurne, pa do visoko organiziranih kriminalnih jedinica koje ciljaju na poslovne i Vladine sustave kako bi se domogli intelektualnog vlasništva i vrijednih informacija.

Potaknuti »objavljivačkom kulturom« društvenih mreža i sve sofisticiranijim zlonamjernim softerima znanim i kao »malware«, internetski kriminalci su sve vještiji u svojim napadima na pojedince i organizacije. Prevarantske poruke lažnim predstavljanjem kroz korisnikove interese, najčešće sakupljenih iz društvenih mreža, žele doći do korisnih podataka, kao što su korisničko ime, lozinka, broj kreditne kartice i sl.

Primjerice, »phishing« je metoda kojom se prevaranti služe na način da korisnicima pošalju mail za koji se čini da je službeni mail iz banke s porukom kako iz određenih razloga (često se navode sigurnosni razlozi, blokada računa ili slično) korisnik mora upisati svoje osobne podatke,

broj računa, PIN ili slično na internetsku stranicu banke, te je u mailu priložen link na tu stranicu. Kada korisnici kliknu na link, čini se da je zaista riječ o stranici banke, no to je lažna stranica koju su stvorili prevaranti i kada korisnik upiše svoje podatke, on zapravo kriminalcima predaje sve svoje osobne podatke koje oni poslije mogu iskoristiti za pražnjenje bankovnih računa, krađe identiteta ili ih mogu prodati na internetu.

1. Nikad ne klikajte na linkove koje ne očekujete
Ovo je zlatno pravilo. Glavni način na koji kriminalci zaraze vaše računalo »malwareom« je tako da namae korisnika da kliknu na određeni link ili otvore privitak.

2. Koristite različite lozinke na različitim stranicama
Istraživanje (Ofcom) je pokazalo da čak 55% odraslih koristi iste lozinke za većinu internetskih stranica koje posjećuju. Najčešće se to datumi rođendana, imena omiljenih osoba, ljubimaca ili sportskih ekipa koje se lako »provale«. Umjesto toga koristite neku zapamtljivu frazu kao npr: »Net.hr je vodeći hrvatski portal«.

3. Nikad nemojte ponovno upotrijebiti lozinku glavnog maila
Haker koji je provalio vaš glavni mail ima ključeve vašeg virtualnog kraljevstva.

4. Koristite anti-virusni program
Istraživanja su pokazala da su najuspješniji anti-virusni paketi »Bitdefender«,»Kaspersky« i »F-Secure«, no ni oni vam ne jamče stopostotnu sigurnost od virusa.

5. Ako ste u dvojbama, blokirajte
Samo recite ne pozivima društvenih mreža (prijatelj na Facebooku ili zahtjev na Linkedlnu) koji vam nisu poznati.

6. Razmislite prije nego »tweetate« i kako dijelite informacije
Ako to ne možete glasno reći na utakmici u Maksimiru pred svima, onda ne stavljajte ni na društvene mreže.

7. Ako imate opciju »wipe your phone« podesite ju

Opcije kao »Find my iPhone«, »Android Lost«, ili »BlackBerry Protect« omogućuju vam da izdaleka pobrišete sve osobne podatke ako vam netko ukrade uređaj ili ga izgubite.

8. Kupujte online samo na sigurnim stranicama
Prije nego unesete detalje s vaše kreditne kartice, provjerite je li stranica »http« ili »https«. Ovo »s« na kraju znači da je veza sigurna.

9. Ne očekujte da vam banka vrati novac
Banka najvjerojatnije neće vratiti novac klijentu ako je on ili ona bio žrtva prevare koju je sam na neki način skrivio/la, odnosno ako se nije pridržavao bankinih uputstava o sigurnosti, primjerice sigurnosnih uputstava o plaćanju računa putem mobilnog telefona.

10. Ignorirajte »pop up« prozore
Tzv. »skočni prozori« mogu sadržavati maliciozni softver. Klikom na njih, taj softer se u pozadini može instalirati na vaše računalo.

11. Budite oprezni s javnim Wi-Fi hotspotovima
Većina Wi-Fi *hostpotova* ne šifrira podatake i jednom kada podatak napusti vaš uređaj i krene prema web odredištu, on je »na čistini« i prenosi se kroz zrak na bežičnu mrežu, navodi Symantecov stručnjak Sian John. »To znači da bilo koje 'njuškalo paketa' [program koji može presresti podatke] ili zlonamjerni pojedinac koji je sjedi na javnom mjestu sa softverom spremnim da traži i presreće podatke koji se prenose preko Wi-Fi mreže, može presresti vaše nekodirane poruke.

12. Imajte više od jednog računa za elektroničku poštu
Razmislite o tome da imate jedan e-mail za svoje bankovne račune i druge financijske usluge, drugi za kupovinu, treći za društvene mreže i sl. Ako vam jedan račun hakiraju, nećete sve odjedanput izgubiti.

13. Macovi su ranjivi kao i PC-evi
Da ne bude zabune, vaš sjajni novi MacBook Air također može biti napadnut kao i bilo koji PC. Istina je da su Macovi manje na meti hakera i to jednostavno zato što kriminalci žele zahvatiti što je veći broj korisnika, pa zato više ciljaju na Windowse.

14. Nemojte pohranjivati podatke sa svoje kartice na web stranice

Budite oprezni kada vas netko pita želite li pohraniti podatke o svojoj kreditnoj kartici za buduću uporabu. Masovne krađe tih podataka nisu tako česte, ali zašto riskirati? Dodatna minuta koja vam je potrebna da prepišete podatke s kartice u neku formu na web stranici je mala cijena koju možete platiti za sigurnost.

15. Dodaj DNS servis za zaštitu i drugih uređaja

DNS sustav pretvara web adresu (niz slova) u strojno čitljivu IP adresu (niz brojeva). Vi vjerojatno koristite DNS servis vašeg ISP-a po *defaultu*, ali možete odlučiti da se pretplatite na uslugu kao što je OpenDNS ili Norton ConnectSafe, koji vas preusmjeravaju ako pokušate pristupiti zlonamjernim stranicama.

16. Omogućite potvrdu u dva koraka

Ako vaš e-mail ili *cloud* servis to nudi, a Gmail, Dropbox, Apple, Facebook te odnedavno i Twitter to imaju, iskoristite potvrdu u dva koraka (*two-step verification*). Uz unos lozinke, također će se od vas tražiti da unestete kontrolni kôd koji će vam biti poslan SMS-om na telefon. Haker može provaliti vašu lozinku, ali bez tog jedinstvenog i privremenog kontrolnog koda ne može zadržati kontrolu nad vašim računom.

17. Zaključavajte svoj mobitel i tablet

Držite ga zaključanima baš kao i vaša ulazna vrata u stan ili kuću. Utipkavanje lozinke ili koda 40-ak puta dnevno može se činiti kao gnjavaža, ali stručnjaci za sigurnsot tvrde da je to »prva linija obrane«. Sljedeća generacija uređaja imat će identifikaciju preko otiska prsta kao dodatnu razinu sigurnosti.

18. Budite oprezni na stranicama za aukcije

Na ovim stranicama posebno vrijedi oprez. Provjerite prodavatelja i držite online plaćanje računa sigurnim te redovito mijenjajte svoje lozinke. Također provjeravajte bankovne račune na koje ste povezani i razmislite o otvaranju posebnog bankovnog računa ili kreditne kartice koje ćete koristiti isključivo za aukcijske web stranice kako bi ograničili potencijalne prevare.

19. Provjerite postavke privatnosti na Facebooku

Facebook redovito ažurira svoje postavke privatnosti, pa je u tom smislu pametno pratiti svoj profil, osobito ako se i dizajn Facebooka promijenio. Jedna od najvažnijih stvari je da provjerite

postavke privatnosti i uvjerite se »tko može vidjeti vaše stvari«. Jesu li to »prijatelji« ili »prijatelji prijatelja«? Obratite pažnju na to. Također, onemogućite tražilicama da mogu pristupiti vašem *ti melineu*
. Možda da razmislite i o kreiranju »popisa«, odnosno podskupina prijatelja, kao što su bliski prijatelji i obitelji, poznanici i sl. kako bi imali bolju kontrolu nad time što s kime dijelite na Facebooku.

20. Sjeti se da si nakon svega običan čovjek

Premda su ovo sve tehnička rješenja kako bi se spriječili hakerski napadi i prevare, imajte na umu da je hakiranje neka vrst vještine prevare. Krajnji cilj prevare nisu računala, već ljudska bića jer se iskorištava njihva lakovjernost, povjerenje, pohlepa ili altruizam. Ljudska pogreška je i dalje najčešći uzrok zašto hakeri imaju tako puno uspjeha.