KAKO PREPOZNATI PRIJEVARE ?

Prema objavi PayPal-a oko 90 % elektroničke pošte spada u pokušaje prijevare, phishing (pokušaj krađe ili krađe bankovnih podataka), neželjenu poštu i općenito poruke u kategoriji smeća. Prijavom sumnjivih poruka pomažete borbi protiv ove suvremene napasti. Što još može pomoći sigurnosti računala ?

Što ste poznatiji ili bolje pozicionirani na web-u, primat ćete veću dnevnu dozu ovog elektronskog smeća. Protiv SPAM-a (neželjenih poruka – uglavnom raznoraznih ponuda) se donekle uspješno možete boriti filtriranjem pošte ugrađenim alatima Internet-preglednika (Browser-a). S izuzetkom ipak rjeđih krajnje agresivnih Spamera, koji su Vam u stanju promijeniti ulaznu stranicu na Internet i uporno sprječavati da napustite njihovu neželjeno učitanu stranicu, što ponekad može ispasti prava gnjavaža, ostali SPAM je samo dosadan i krade Vam dragocjeno vrijeme, ali ipak u načelu nije opasan.
Za razliku od toga, Phishing, pokušaji prijevare, podmetanje virusa i općenito zločudnog softvera može ugroziti Vašu ne samo Internetsku, nego i financijsku sigurnost. Zato je važno prepoznati takve poruke. ***Sumnjive su poruke koje :***

- su dostavljene na neobjavljene primatelje (Undisclosed Recipients) ili na više od jedne adrese
- traže da preuzmete obrazac ili datoteku sa Interneta da bi se obavilo predloženo
- traže da verificirate račun (Account) na mreži ili u banci, PayPal-u i sl. dostavom osobnih podataka poput: imena banke, pin-a, lozinke, vrste i/ili broja bankovne kartice, datuma istjecanja važnosti kartice, troznamenkastog sigurnosnog koda s poleđine kartice (CVV2 code), odgovora na sigurnosna pitanja (security question answers) koje ste deponirali u platno-uslužnom servisu (banka, PayPal i sl.). **Nikako ne šaljite ove podatke e-mailom** i ne uključujte ih u korespondenciju ni sa bankama ili platnim servisima, jer prevaranti mogu presresti Vašu elektronsku poštu i ukrasti ove podatke, a nekoliko od njih dovoljni su za ulazak na Vaš bankovni konto, otvaranje računa na Vaše ime i teret, te za davanje naloga banci da skinu novac s Vašeg bankovnog računa za proizvoljnu svrhu.

  Banke i platni servisi nikada Vas neće tražiti da te podatke šaljete e-mailom ili unosite u obrasce preuzete s Interneta. Jedini način unošenja, mijenjanja ili verifikacije tih podataka je regularni ulazak u Vaš račun uz korištenje lozinke poznate samo Vama, i ažuriranje tih podataka u odjeljku Vašeg računa (Account) na stranicama Banke. Nakon korekcije / izmjene primit ćete od banke, platnog servisa, Google ili drugog web-servisa obavijest o učinjenoj izmjeni. Ako primite takvu obavijest o izmjeni koju niste Vi izvršili, smjesta se **uobičajenim postupkom** logirajte na Vaš Account, pregledajte izmjene i po potrebi alarmirajte – obavijestite o neregularnoj aktivnosti te nastavite po dobivenoj uputi.

- **Ne klikajte na bilokakve, pa ni poznate poveznice (linkove) u elektronskoj pošti** od sumnjivog ili nepoznatog pošiljatelja. Ako želite učitati ili otići na sadržaj na koji poveznica navodno cilja, utipkajte to s poveznice u adresnu ćeliju Internet-preglednika. **Desni** klik na poveznicu trebao bi pokazati stvarnu web ili mail-adresu koja se skriva iza linka. Ako to nije poznato Vam odredište iz ranije korespondencije, vjerojatno je u pitanju prijevara.
- Kod bilokakvih sumnjivih poruka provjerite da li su mailadrese pošiljatelja (From:) i adresa za odgovor (Replay to:) stvarno postojeće adrese. To je vrlo jednostavno: kopirajte tu mail-adresu i ulijepite u jedinu ćelju za upis na stranici http://email-checker.net/ . *Za par sekundi se u email-checker-u prikazuje* ***VALID*** *ako je adresa stvarna, ili* ***NOT VALID*** *ako je lažna. Ako je bilo koja adresa lažna, u pitanju je prijevara ili neki žmukleraj. Obično bude lažna adresa pošiljatelja, a stvarna adresa za odgovor, jer prevarant očekuje dostavu podataka, ako cilj nije bio samo uvaljivanje virusa ili špijuna u Vaše računalo.*
- ***Zločudni softver*** *je obično u prilogu (attach) ili u sadržaju ili na stranici koja se skriva iza linka koji Vam je ponuđen. Zato* ***ne otvarajte priloge u pošti od nepoznatih pošiljatelja****. Ako ste baš znatiželjni, prilog (bez otvaranja) možete ukopirati na desktop ili na USB stik i provjerite ga antivirusnim programom (nadam se da ga imate ažuriranog u funkciji !) Obično će malware biti sadržan u prilogu. No i ako neće, ni to nije garancija da nema opasnosti, jer prilog može inicirati preuzimanje i instaliranje zločudnog softvera kad ga se aktivira (npr. uz pomoć macro-instrukcija u WORD-u EXCEL-u i sl.).*

*Ne zaboravite brisati kopirani prilog kao i čitav sumnjivi mail sa računala. Prije toga sumnjive ili dokazano zlonamjerne poruke, pa i običan SPAM (neželjenu poštu) prijavite jednim klikom na odgovarajuću opciju programa za elektronsku poštu (kod npr. Mozillinog Firefox-a su to dugmeta **REPORT MESSEGE AS SPAM** i **REPORT MESSEGE AS PHISHING**. Sve ostalo obavit će se samo.*

- *Sigurno Vam umirući od raka neće darovati milijune dolara da ih koristite u humanitarne svrhe, niti ste dobili tisuće dolara specijalne nagrade od Google-a ili koga drugoga, to je phishing ili pokušaj da se od Vas iskamči nešto novca. Klonite se kredita koji se nude preko mailova od nepoznatih pošiljatelja, kao i izvrsno plaćenih poslova koji čekaju baš Vas.*

*Ako Vas netko baš pošteno razbijesni, prijavite ga abuse-službi operatera kod kojega ima mail-adresu. To traži malo više angažmana, ali jako bezobrazni seratori to zaslužuju. Kopirajte izvorni kod (Original code) primljene poruke (u hrvatskom Firefox-u to prikazuje menu-opcija: **pogled > izvorni kod poruke**) i dodajte to na kraj proslijeđene (Forward) sumnjive poruke. U izvornom kod-u pronađite barem jednu realnu adresu (to je obično ona za odgovor, tj. Replay to:). Dio adrese iza **@** je tzv. domena. Tako pripremljenu poruku proslijedite na adresu **abuse@domena**. Umjesto "domena" tipkate naravno ono što je iza @ u nađenoj realnoj adresi primljene poruke.*
Ako ste u prilogu našli virus, navedite to u proslijeđenoj poruci.
Ako ne primite poruku da mail nije mogao biti uručen, vjerojatno će naš šaljivđija u najmanju ruku ostati bez svoje mail-adrese, a možda i biti obilježen kao osoba kojoj se barem na toj usluzi više neće davati mail-adrese.

ŠTO JOŠ MOŽETE PODUZETI U CILJU BOLJE ZAŠTITE ?

*Podrazumijeva se da imate instaliran antivirusni program koji se automatski ažurira, tako da može prepoznati nove viruse i zločudne programe koji se kote svakodnevno. Uz to je dobro instalirati dodatak **McAffe Site Advisor** za Internet-preglednik. Site Advisor će Vas upozoriti i spriječiti učitavanje sumnjivih web-stranica, pa onda možete odlučiti da li ćete ipak otići na nju ili odustati.*

*Za sprječavanje gomilanja tisuća kolačića koje web-stranice ostavljaju na Vašem računalu, možete instalirati dodatak **Self Destructng Cookies** . Posljedično će se svi kolačići koje web-stranice ostave na Vašem računalu samoubiti, tj. uništiti, osim onih koje odaberete za preživljavanje (može se dogoditi da neke opcije ili funkcionalnosti neke aplikacije budu narušene ako nema kolačića, iako je to izuzetno rijetko).*
Kolačići inače između ostaloga pamte podatke o Vašem surfanju pa omogućuju prilagodbu tražilica Vašim interesima, ali mogu i sadržavati ili pokretati iskakanje reklamnih okvirića ili dosađivati sa ponudama novih verzija softvera koje imate na računalu i sl, dakle omogućuju stvari koje Vas u načelu neće osobito usrećiti, pa je najčešće bolje biti bez njih.
Oba dodatka instalirat će ikonice u gornji desni ugao Internet-preglednika, pa klikom na njih možete mijenjati opcije i kontrolirati njihovu funkcionalnost.

*Preporučam i instaliranje nekog alatića (widget, gadget i sl.) – pokazivaća operećenja procesora koji će Vam cijelo vrijeme biti pred očima u uglu ekrana. Ako primijetite da Vam je procesor opretećen više od nekoliko postotaka kad računalo "ništa ne radi", vrijeme je da pokrenete **Process Explorer** (bolja verzija Windows Task Menager-a) ili sličan alat za uvid u aktivne programe i procese na računalu i prokljuvite tko je krivac (tj. tko troši resurse procesora) za brbanje po računalu kad niste ništa aktivirali. Često se takvo što događa nakon instalranja raznih "popravljača performansi" računala, koji tobože optimiraju rad računala, a na kraju se pokaže da troše po 30% procesorske snage za tko zna što, kad računalo inače miruje. Takvav softver je najbolje bez milosti deinstlirati i to pomoću programa koji omogućuje čišćenje svih ostataka nakon deinstalacije. Takav je primjerice besplatni **Zsoft Uninstaller 2.5**, koji osim temeljite deinstalacije omogućuje još neke pretrage i funkcionalnosti, no postoje i drugi (Revo Uninstaller i dr.). Ne vjerujte ugrađenim deinstalacijskim programima instaliranih programa, oni često ostavljaju (često i namjerno) desetke, pa i stotine ostataka na računalu iza denstalacije. Koristite spomenute Uninstallere za sve deinstalacije. Iz istog razloga izbjegavajte često instalranje svega i svačega "za probu", ili to nakon "probe" temeljito denstalirajte, da Vam računalo ne skuplja suvišni balast.*

Na kraju, redovno ažurirajte ranjive dodatke (Adobe Acrobat, RealPlayer, Java, QuickTme Plug-in), koje žgadija koristi za provale u računalo ili ako je moguće, koristite umjesto njih manje osjetljive (možda Foxit Reader umjesto Adobe Acrobata i sl.).
Konačno, prije ozbiljnijih intervencija (npr. temeljitog "čišćenja" računala i sl.) snimite backup sistema i povratnu točku za vraćanje računala u prijašnje stanje. U slučaju teže zaraze računala lakše ga je vratiti u ranije stanje sa System Restore nego očistiti od kakvog gadnijeg virusa.