

# Ne budi i ti hrvatski naivac



Svake godine vrlo velik broj ljudi u Hrvatskoj zbog vlastite naivnosti nasjedne na neku od internetskih prevara. Kako i vi ne biste ispali naivni, pročitajte priče o velikim hrvatskim naivcima i iz njihovih primjera naučite kako se zaštititi i surfati sigurnije.

**CERT.hr**  
surfaj sigurnije



Sufinancirano  
instrumentom  
Europske unije za  
povezivanje Europe

# Veliki hrvatski naivci



## Mirta Rogonja

~ Nepostojeća humanitarna akcija ~

Mirta je bila tip osobe koja se lako rasplače. Suza je kanula i kad je vidjela mail poruku kojom se traži novčana pomoć za hranu malim psićima koji još nemaju svoj zauvijek dom. „Ima još dobrih ljudi na svijetu“, naivno je pomislila uplaćujući novac za nekoliko vreća pseće hrane za štence. Nažalost, repom su od sreće mahali samo prevaranti koji su i psiće i humanitarnu akciju izmislili.

Prevaranti na društvenim mrežama i internetskim stranicama često iskorištavaju dobrotu ljudi. Bolesna djeca, napušteni psi ili siromašne obitelji česta su tema izmišljenih humanitarnih akcija na koje svatko od nas može lako nasjesti. Kod ovakvih prevara posebno je opasno što dovode u sumnju i prave projekte koji pokušavaju pomoći onima kojima je pomoć stvarno potrebna. Zato i dalje činite dobro, ali s određenom dozom skepse - uvijek se zapitajte tko vam šalje poruku, provjerite pišu li o akciji mediji, jesu li vaši prijatelji sudjelovali u skupljanju pomoći i zvuči li poruka sumnjivo.

*Svaka sličnost sa stvarnim osobama i događajima je slučajna.*

**CERT.hr je nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj, dio je Hrvatske akademske i istraživačke mreže – CARNET.**

**naivci.hr cert.hr tel.: +385 1 6661 650 e-pošta: ncert@cert.hr**

Sadržaj letka isključiva je odgovornost Nacionalnog CERT-a. Fornska unija nije odgovorna za bilo kakvu uporabu informacija sadržanih u letku.



## Luka Mišura

~ Lažne stranice s apartmanima ~

Ljetovanje s obitelji na Siciliji nikad nije bilo bliže - cijela vila s bazenom za samo 40 eura dnevno! „Kako to da ljudi još nisu otkrili ovu stranicu za iznajmljivanje...“, naivno je pomislio Luka, zadovoljno uplaćujući cijeli iznos odjednom. Nažalost, vrlo brzo nakon slijetanja na Siciliju cijela je obitelj morala u potragu za „zimmer-frei babama“. Unaprijed plaćena vila za 40 eura dnevno - ne postoji.

Danas je putem raznih internetskih servisa moguće rezervirati i platiti smještaj. Nažalost, nemaju svi korisnici takvih servisa plemenite namjere te se može dogoditi da se iza profila prekrasne morske vile krije zlonamjerni prevarant. Svakako pokušajte utvrditi stvarni identitet osobe s kojom komunicirate i ostvariti s njom neposrednu komunikaciju. Također, popularne stranice mnogo ulažu u sigurnosne mehanizme pa vam savjetujemo da svu komunikaciju i transakcije vršite isključivo putem službenih i globalno poznatih stranica. Tada, čak i ako dođe do zlonamjerne aktivnosti, nadležne službe moći će vam pomoći u rješavanju problema.

**NAIVNA ČINJENICA:** u svijetu je 2017. putem online prevara ukradeno oko 130 milijardi funti.



## Danijel Čabrava

~ Lažno predstavljanje ~

*U svome selu poznat kao „stari momak“, Danijel se naivno ponadao da je našao ljubav koja će taj nadimak učiniti prošlošću. Bila je riječ o Amini, nigerijskoj djevojci koju je upoznao na novom online dating servisu. Za ljubavni happy end, Amini je trebao samo novac za autobusnu kartu od Lagosa do Gospića. „Ma možda dugo stoje na granici“, pomislio je Danijel čekajući i čekajući na gospićkom kolodvoru.*

Internet zlonamjernim korisnicima omogućava predstavljanje drugim identitetom te ostvarivanje novčane ili druge dobiti od naivnih i nedovoljno opreznih korisnika. Važno je da prilikom bilo kakve komunikacije internetom nedvosmisleno potvrdite stvarni identitet osobe s kojom komunicirate. Zlonamjerni se korisnik može predstaviti kao poznanik, prijatelj, predstavnik vaše banke ili tvrtke ili čak slavna osoba kako bi vas iskoristio i ostvario svoju korist na vašu štetu.



## Ena Bubalo

~Bonovi~

Ena je bila offline šopingoholičarka. Kad je na mail dobila nevjerojatnu ponudu za bonove velikog trgovačkog lanca ni trenu nije oklijevala - samo je trebala riješiti anketu, proslijediti je prijateljima i bon od 1700 kuna popusta bit će njen, naivno se ponadala. Na njenu žalost dio te „ankete“ bio je i slanje osobnih podataka poput OIB-a. Na uzorku od jednog ispitanog, ta anketa je pokazala - Ena je prevarena. Koristeći njen OIB prevaranti su kupovali mobilne uređaje i potpisivali dugoročne ugovore koje je ona morala plaćati.

Surfajući internetom često nađemo na ponudu koja djeluje predobro da bi bila istinita i najčešće ispadne da zaista je tako. Iako je katkad teško procijeniti predstavlja li poruka potencijalnu prijetnju, važno je imati na umu kako zdrav razum predstavlja najbolju obranu. Ovakve ponude dolaze u raznim oblicima, ali najčešće kao skočni prozori (engl. PopUp) ili neželjena pošta (engl. Spam). Napadači često od žrtava traže osobne podatke ili da poruku prosljede na adrese prijatelja. Upravo zato je veoma važno prepoznati prijetnju i zapitati se je li riječ o prevari jer o vašoj odluci ovisi i sigurnost drugih ljudi.

**NAIVNA ČINJENICA:** čak 30% zlonamjernih poruka bit će otvoreno, a na link unutar njih kliknut će 12% primatelja.



Josip Švigir

~ Dijeljenje osobnih podataka ~

*Potaknut vlastitom ćelavošću, Josip je nesmotreno poslao osobne podatke nepoznatim osobama odgovarajući na email koji mu je nudio čudotvorni lijek za tu mušku „bolest“. Naivno je mislio „Ma neće mi ni dlaka s glave pasti“. Ono što je palo je količina novca na Josipovom tekućem računu. Koristeći njegove podatke prevaranti su mu lako ukrali novac.*

Upisivanje povjerljivih podataka na nesigurnoj stranici veoma je opasno i može imati nesagledive posljedice. Napadači mogu presresti vaše podatke te se njima poslužiti kako bi nešto platili ili ih iskoristili za daljnji napad. Prilikom upisivanja povjerljivih podataka, svakako se uvjerite da je riječ o legitimnoj stranici usluge koja vas traži podatke. Također, valja imati na umu kako će vas rijetko koja tvrtka ili pojedinac tražiti da svoje podatke šaljete elektroničkom poštom. U slučaju da dobijete takav zahtjev na svoju adresu elektroničke pošte, svakako drugim kanalom komunikacije provjerite je li on legitiman.

**NAIVNA ČINJENICA: 12% građana ne izbjegava otkrivati svoje osobne podatke na internetu.**



## Ivana Paladino

~ Brza zarada ~

Ivana je bila, kako to Amerikanci kažu, između dva posla. Tako je jedan dan, besposleno surfajući internetom, naišla na oglas „Rad od doma, brza i lagana zarada surfajući! Klikni i zaradi preko 10000 kuna odmah!“. Brže-bolje je kliknula, naivno se pribojavajući da bi neki drugi kandidat mogao dobiti taj super posao prije nje. Nažalost, jedino što je Ivana dobila bio je virus koji joj je s računala ukrao sve osobne podatke kojima su prevaranti brzo i lako došli do Ivanina novca.

Internetske su stranice pune oglasa koji nude prilike za brzu zaradu. Nažalost, gotovo sve takve ponude iza sebe kriju zlonamjernog prevaranla koji vas želi iskoristiti za ostvarivanje svojih ciljeva. Pristupanjem na poveznice koje nude brzu i laku zaradu u opasnost dovodite svoje podatke i računalo. Vješt napadač može iskoristiti vašu želju za zaradom kako bi vas nagnao da preuzmete zlonamjerni sadržaj na svoje računalo. Nakon što preuzmete zlonamjerni sadržaj, napadača više ništa ne sprečava da preuzme potpunu kontrolu nad vašim uređajem i podacima te brzo i lako zaradi.

**NAIVNA ČINJENICA:** u Hrvatskoj je u 2017. nekom vrstom zlonamjernog sadržaja bilo zaraženo približno 320 000 uređaja.



## Martin Kiš

~Prejednostavna lozinka~

Martinu bi srednje ime slobodno moglo biti Narcis. Naime, kupujući flambojantnu odjeću na sumnjivim web-stranicama uvijek je koristio jednu te istu šifru za sve - vlastito ime i prezime, naivno misleći da je neprobajna. Zločesti ljudi koji stoje iza tih lažnih web-trgovina Martinovu su šifru iskoristili kako bi ušli u sve njegove račune i tamo radili darmar kupujući stvari za sebe, naravno Martinovom lovom.

Korištenjem iste lozinke za više različitih servisa značajno se uvećava mogućnost probijanja te lozinke zato što ne koriste sve usluge jednako kvalitetne mehanizme za zaštitu podataka. Kompromitacijom jednog sustava i jedne lozinke dovodite u rizik sve sustave i usluge koji koriste tu lozinku. Iako, razni internetski servisi često su međusobno povezani što svakodnevno olakšava njihovo korištenje, ali istodobno uvelike povećava rizik jer pojedinac koji je došao do korisničkih podataka vezanih uz vašu elektroničku poštu lako može doći do korisničkih podataka za prijavu na društvene mreže.

**NAIVNA ČINJENICA:** 48% građana u zadnjih godinu dana nije promijenilo svoje lozinke, a 81% ih koristi istu lozinku za svaki servis.