

OUCH!

Vaš mesečni bilten za podizanje svesti o bezbednosti informacija

# Kupujte bezbedno preko interneta

## Uvod

Sezona praznika približava se za mnoge od nas i uskoro će milioni ljudi širom sveta biti u potrazi za savršenim poklonima. U potrazi za najboljim ponudama i kako bi izbegli gužve i čekanja u dugačkim redovima, mnogi od nas će poklone kupovati na internetu. Nažalost, sajber kriminalci će takođe biti aktivni, kreirajući lažne sajtove za kupovinu i koristeći druge taktike da prevare ljude. U nastavku će biti pojašnjeno kako da kupujete preko interneta na bezbedan način i kako da izbegnete da postanete žrtva.

## Lažne internet prodavnice

Sajber kriminalci kreiraju lažne prodavnice na internetu koje oponašaju izgled pravih sajtova ili koriste imena poznatih prodavnica ili brendova. Kada ste u potrazi za najboljim ponudama na internetu, možete se naći na nekom od ovih lažnih sajtova. Kupovinom putem ovakvih sajtova možete završiti sa falsifikovanim ili ukradenim predmetima, a može se desiti i da ono što ste kupili nikada ne bude isporučeno. Zaštitite se od lažnih internet prodavnica primenom sledećih saveta:



Kad god je to moguće, kupujte preko internet prodavnica koje već poznajete, u koje imate poverenja i sa kojima ste ranije poslovali. Sačuvajte linkove internet prodavnica koje ste posetili ranije i kojima verujete.



Budite obazrivi kod cena koje su značajno povoljnije od onih koje su objavljene na zvaničnim internet prodavnicama. Ako ponuda deluje previše dobro da bi bila istinita, moguće je da je lažna.



Budite sumnjičavi ako veb sajt liči na onaj koji ste ranije koristili, ali su domensko ime ili naziv prodavnice malo drugačiji. Na primer, navikli ste da kupujete preko Amazona, čija internet adresa je [www.amazon.com](http://www.amazon.com), ali nepažnjom možete završiti na lažnom veb sajtu koji ima sličnu adresu i gde je slovo „o“ zamenjeno brojem „0“.



Unesite ime internet prodavnice ili njenu veb adresu u pretraživač da biste videli šta su drugi kupci pisali o njoj. Potražite pojmove kao što su „prevara“, „nikad više“ ili „lažni“ (eng. „fraud“, „scam“, „never again“, „fake“).



Koristite jedinstvenu lozinku za svaki od vaših naloga na internetu. Ne možete da se setite svih vaših lozinki? Razmislite o tome da ih sačuvate u menadžeru lozinki.

## Prevare na zvaničnim veb sajtovima

Vodite računa čak i kada kupujete preko pouzdanih veb sajtova. Velike internet prodavnice često u ponudi imaju proizvode koje prodaju različite osobe ili kompanije od kojih neke imaju nameru da vas prevare. Takve internet destinacije nalik su stvarnim trgovinskim centrima gde su neki prodavci pouzdaniji od drugih. Proverite reputaciju svakog prodavca pre nego što napravite porudžbinu. Budite oprezni sa prodavcima čija internet prodavnica je nova ili koji prodaju proizvode po neuobičajeno niskim cenama. Upoznajte se sa politikom poslovanja zvaničnog veb sajta vezano za kupovine kada su u pitanju treća lica. Kada ste u nedoumici, kupujte proizvode koje direktno prodaju internet prodavnice, a izbegavajte proizvode koje treća lica prodaju putem ovakvih veb sajtova.

## Plaćanje putem interneta

Redovno proveravajte izveštaje sa vaših platnih kartica kako biste otkrili sumnjive transakcije. Ako je dostupno kao opcija, omogućite da vam se svaki put kada je sa vaše platne kartice izvršena naplata pošalje obaveštenje (putem mejla, sms porukom ili kroz aplikaciju). Ukoliko otkrijete bilo kakvu sumnjivu aktivnost, odmah pozovite banku kod koje imate račun i prijavite ovu aktivnost. Izbegavajte korišćenje debitnih kartica za internet plaćanja kad god je to moguće. Debitnim karticama novac se skida direktno sa vašeg bankovnog računa, pa će vam u slučaju prevare biti potrebno mnogo više vremena da povratite svoj novac. Druga opcija je da za kupovinu preko interneta koristite poznate servise za internet plaćanje, kao što je PayPal, koji ne zahtevaju da otkrijete broj vaše platne kartice prodavcu. Na kraju, razmotrite korišćenje poklon kartice za internet kupovinu.

Ako internet prodavnica ima dobar dizajn i izgleda profesionalno, to ne znači i da je zakonita. Kada se ne osećate prijatno dok koristite određeni veb sajt, prestanite da ga posećujete. Umesto toga, idite na poznate sajtove koji su pouzdani ili ste ih bezbedno koristili u prošlosti. Možda nećete naći fenomenalnu ponudu, ali ćete sigurno nabaviti legalan proizvod i nećete biti prevareni.

## Verzija na srpskom

Telekom Srbija kao društveno odgovorna telekomunikaciona kompanija pomaže prevođenje i distribuciju ovog biltena kako bi se unapredila svest korisnika informaciono-komunikacionih tehnologija o bezbednosti informacija.

## Gost urednik

**Leni Zeltser** je zadužen za IT bezbednost u kompaniji Axonius i viši je instruktorka i autor kurseva na SANS Institutu. Možete ga pratiti na Tviteru, kao [@lennyzeltser](https://twitter.com/lennyzeltser) i čitati njegov blog na [zeltser.com](http://zeltser.com).



## Dodatni materijal

Socijalni inženjering: <http://www.sans.org/u/X7k>

Prevare putem društvenih mreža: <http://www.sans.org/u/X7p>

Napravite lozinku na jednostavan način: <http://www.sans.org/u/Xu9>

*OUCH!* bilten objavljuje SANS Security Awareness program i distribuira se pod [Creative Commons BY-NC-ND 4.0 licencom](https://creativecommons.org/licenses/by-nc-nd/4.0/). Biltene je dozvoljeno distribuirati ili koristiti za svoj program unapređenja svesti o bezbednosti informacija pod uslovom da se sadržaj ne modifikuje. Za pitanja u vezi prevoda ili za dodatne informacije, kontaktirajte [www.sans.org/security-awareness/ouch-newsletter](http://www.sans.org/security-awareness/ouch-newsletter). Redakcija: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Preveli: Dragan Ristić i Gordana Živanović