

OUCH!

U OVOM IZDANJU...

- Lažne Internet prodavnice
- Vaš računar / mobilni uređaj
- Vaša kreditna kartica

Bezbedna kupovina na Internetu

Sezona kada je neophodno biti na oprezu

Sezona praznika (Nova godina, Božić) se bliži i uskoro će milioni ljudi širom sveta početi potragu za savršenim poklonima. Mnogi od nas će se, u potrazi za povoljnijim cenama i da bi izbegli gužve, odlučiti za kupovinu preko Interneta. Nažalost, ovoj je takođe i omiljeni period godine svih sajber kriminalaca, pošto se najveći broj transakcija online kupovinom, a samim tim i sajber finansijskih prevara, dogodi u to vreme. U ovom izdanju objasnićemo opasnosti vezane za Internet kupovinu i kako da se zaštitite.

Gost urednik

Jonathan Homer ([@JonathanLHomer](#)) je priznati stručnjak u industriji sajber bezbednosti i aktivan kako u državnom tako i u privatnom sektoru. John je specijalista za obuke koje podrazumevaju angažovanje učesnika i napredne tehnike treninga.

Lažne Internet prodavnice

Većina Internet prodavnica je legitimna, ali postoje i one koje to nisu, lažne Internet stranice postavljene od strane sajber kriminalaca. Sajber kriminalaci kreiraju lažne Internet stranice tako što kopiraju izgled ili koriste ime dobro poznatih, renomiranih Internet prodavnica. Onda te Internet stranice koriste da namame lakoverne osobe u potrazi za najboljim ponudama. Kada ste na Internetu u potrazi za apsolutno najnižim cenama, velika je verovatnoća da će te biti usmereni na jednu od ovakvih lažnih Internet prodavnica.

Prilikom odabira Internet prodavnice za kupovinu proizvoda, budite veoma oprezni ako su oglašene cene drastično jeftinije nego u odnosu na ostale prodavnice, ili ako nude proizvode koji nije moguće kupiti na drugim mestima. Razlog zbog čega su njihovi proizvodi toliko jeftiniji ili dostupni može da leži u činjenici da nisu legalni, falsifikovana ili ukradena roba, ili vam proizvod u stvari nikada i neće biti isporučen. Da bi ste se zaštitili pratite sledeće savete:

- Proverite da li Internet prodavnica ima legitimnu adresu el. pošte i telefonski broj za prodaju ili podršku. Ako vam nešto izgleda sumnjivo, pozovite i proverite.
- Potražite očigledne znake upozorenja, na primer loš pravopis ili gramatika.
- Budite oprezni sa Internet stranicama koje izgledaju kao replike dobro poznatih Internet stranica koje ste ranije koristili, ali se domen Internet stranice ili ime prodavnice malo razlikuju. Na primer, možda ste u prošlosti koristili

Bezbedna kupovina na Internetu

<https://amazon.com> za kupovinu na Amazonu, ali budite veoma oprezni ako se nađete na Internet stranici koje izgleda kao Amazon a koristi Internet adresu (URL) <http://store-amazon.com>. To nije isto.

- Unesite ime prodavnice u Internet pretraživač i proverite komentare i iskustva drugih ljudi koji su već kupovali. Potražite termine „prevara“, „nikad više“ ili „lažni“. Nedostatak komentara takođe nije dobar znak pošto ukazuje da je Internet prodavnica veoma nova.

Zapamtite, samo zato što Internet stranica izgleda profesionalno ne znači da je legitimna. Ako vam se nešto učini sumnjivim, odvojite malo vremena i istražite. Ako niste sigurni u neku Internet prodavnicu, nemojte je koristiti. Umesto toga nađite dobro poznatu, renomiranu i pouzdanu, neku koju ste koristili ranije. Možda nećete dobiti ogroman popust ili ulaznice koje je veoma teško nabaviti, ali je veoma verovatnije da ćete dobiti legitiman proizvod i čist kreditni izveštaj.

Vaš računar / mobilni uređaj

Osim kupovine u legitimnim Internet prodavnicama, morate da budete sigurni da je vaš računar ili mobilni uređaj bezbedan. Sajber kriminalci uvek vrebaju priliku da kompromituju neki uređaj u cilju prikupljanja informacija o bankovnim računima, kreditnim karticama i lozinkama. Da bi ste zaštitili svoje uređaje pridržavajte se sledećih saveta:

- Ako imate decu u kući, uzmite u obzir korišćenje dva uređaja, jedan za decu a drugi za odrasle. Deca su znatiželjna i interaktivna sa tehnologijama, tako de je veća verovatnoća da će svoj uređaj inficirati. Korišćenjem posebnog računara ili tableta samo za on-line transakcije, na primer on-line bankarstvo ili kupovina, smanjujete mogućnost infekcije tog uređaja. Ako poseban uređaj nije opcija, onda koristite različite naloge na zajedničkom računaru, i budite sigurni da deca nemaju administratorske privilegije.
- Povezuj te se samo sa bežičnim mrežama kojima sami upravljate, vaša kućna mreža, ili onima za koje ste sigurni da su pouzdane za finansijske transakcije. Korišćenje javnih Wi-Fi mreža kao što je vaš omiljeni kafić može da bude sjajno za čitanje vesti ali nikako za pristupanje vašem bankovnom računu.
- Redovno ažurirajte svoje uređaje, posebno anti-virusni softver. Na taj način prilično otežavate sajber kriminalcima da inficiraju vaš uređaj.



Zaštitite se prilikom kupovine na Internetu tako što ćete kupovati samo u pouzdanim Internet prodavnicama sa proverenom reputacijom.

Bezbedna kupovina na Internetu

Vaša kreditna kartica

Pratite stanje svojih kreditnih kartica da bi ste mogli da uočite sumnjive transakcije. Barem jednom mesečno proverite sve transakcije po svojim karticama. Neke banke imaju opciju da vas obaveštavaju tekstualnom porukom svaki put kada je promena na kartici izvršena ili kada je suma iznad postavljenog limita. Druga opcija je da imate posebnu karticu samo za Internet kupovinu, tako da u slučaju da je kompromitovana možete lako da je zamenite bez uticaja na vaša druga plaćanja. Ako vam se učini da ste žrtva prevare pozovite odmah svoju banku i objasnite situaciju. U takvim slučajevima kreditne kartice su u velikoj prednosti u odnosu na debitne. Kod debitnih kartica se novac direktno povlači sa vašeg računa, tako da ako ste žrtva prevare, daleko teže možete da povratite svoj novac.

Konačno, postoje i novi načini plaćanja koji vam omogućavaju da plaćate bez izlaganja broja vaše kreditne kartice. Uzmite u obzir kreditne kartice koje generišu jedinstveni broj kartice svaki put kada kupujete na Internetu ili koristite dobro poznate servise za plaćanje, kao što je PayPal, koji prodavcu ne otkrivaju vaš broj kartice.

Saznaj Više

Prijavi se na OUCH! mesečni bilten bezbednosnih saveta za korisnike računara, pristupi prethodnim OUCH! izdanjima i saznaj više o SANS rešenjima u vezi svesnosti bezbednosti informacija na našoj internet prezentaciji

<http://www.securingthehuman.org/>.

Dodatne informacije

Pet ključnih pravila za vašu bezbednost: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201410_se.pdf

Kako obezbediti kućnu mrežu: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201401_se.pdf

Bezbednost tvog novog tableta: https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201312_se.pdf

SANS tip dana: https://www.sans.org/tip_of_the_day.php

OUCH! Objavljuje SANS Securing The Human 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 bezbednosne svesti uz uslov da sadržaj nije modifikovan. U vezi prevoda ili za dodatne informacije, kontaktiraj ouch@securingthehuman.org.

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Preveo: Nenad Varinac



securingthehuman.org/blog



[/securethehuman](https://www.facebook.com/securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



[securingthehuman.org/gplus](https://www.securingthehuman.org/gplus)