

Jutarnji list

Stručnjaci savjetuju

Četiri stvari koje webshop mora imati prije nego stisnete „kupi“: ‘Za dvije minute se može procijeniti 80 posto rizika!’

Online prijevare je sve teže prepoznati i njihov broj zabrinjavajuće raste iz dana u dan

Piše: Ivan Luzar/Sponzorirani sadržaj

Objavljeno: 30. ožujka 2026. 16:44



Online kupovina donijela je nešto što generacije prije nas nisu imale, mogućnost da za nekoliko minuta, iz vlastite fotelje, usporedite cijene, pročitate recenzije i naručite gotovo bilo što na svijetu. Brza je, praktična i sve dostupnija. Više se za neke stvari koje možda nisu dostupne u domaćim fizičkim trgovinama ne mora ići preko granice, već je dovoljno samo jedno pretraživanje interneta. No kao i svaki alat koji postaje masovan, privlači i one koji ga koriste na pogrešan način.

Zamislite da naručite tenisice, a u paketu stignu otpadne tkanine poput izlizanih traperica. Ili naručite mobitel, pa u kutiji nađete ciglu. Zvuči kao vic ili priča za zastrašivanje, ali to su stvarne priče koje u policijskim izvještajima završavaju pod rubrikom 'računalna prijevara'. Na razini Hrvatske broj takvih slučajeva raste između 10 i 12 posto godišnje, a ukupna evidentirana šteta u 2024. godini premašila je 18 milijuna eura.

Istovremeno, online kupovina nikad nije bila popularnija. Broj paketnih dostava u Hrvatskoj je 2024. godine porastao je za rekordnih 22,8 posto u odnosu na godinu ranije. Više kupaca znači i više potencijalnih žrtava na koje prevaranti mogu ciljati. A alati kojima raspolažu nikad nisu bili dostupniji: s nekoliko klikova i bez tehničkog znanja mogu kopirati bilo koju legitimnu stranicu i u nju ubaciti vlastite načine kako vam ukrasti novac.

Za procjenu rizika dovoljne su samo dvije minute

Marcel Majsan, predsjednik i osnivač Udruge eCommerce Hrvatska, godinama prati tržište online trgovine u regiji i s njim razgovaramo o tome kako u kratkom vremenu procijeniti je li web-shop legitiman. Njegova lista provjere je kratka, ali i učinkovita.

- Tko stoji iza shopa? Tražim naziv tvrtke, OIB, adresu, kontakt telefon. Ako toga nema, odustajem od kupnje. Koliko dugo postoje? Ukucam njihov brend u Google i tražim neki društveni dokaz. Ako su otvoreni jučer, a nude velike popuste, to je prvi signal za oprez. Realno, za dvije minute se može procijeniti 80 posto rizika – otkriva nam Majsan.



Marcel Majsan, eCommerce Hrvatska

/Ustupljena Fotografija

Stručnjaci CARNET-ovog Nacionalnog CERT-a s kojima smo razgovarali sliku dopunjuju tehničke strane. Najčešći vizualni pokazatelj je sumnjiva web-adresa. Umjesto službene domene brenda, pojavljuju se varijacije s dodacima poput 'hrvatska', 'outlet', 'akcija' ili 'popust'. Česte su gramatičke pogreške, miješanje različitih jezika i tekst u kojemu svaka riječ počinje velikim slovom, što je karakteristično za loše automatizirane prijevode.

Nerealno niske cijene, navodi o velikom popustu na sve proizvode, nepostojanje telefonskog kontakta i odsutnost podataka o tvrtki, sve su to alarmi. No Majsan ističe jedan signal koji je gotovo uvijek prisutan kod lažnih web shopova.

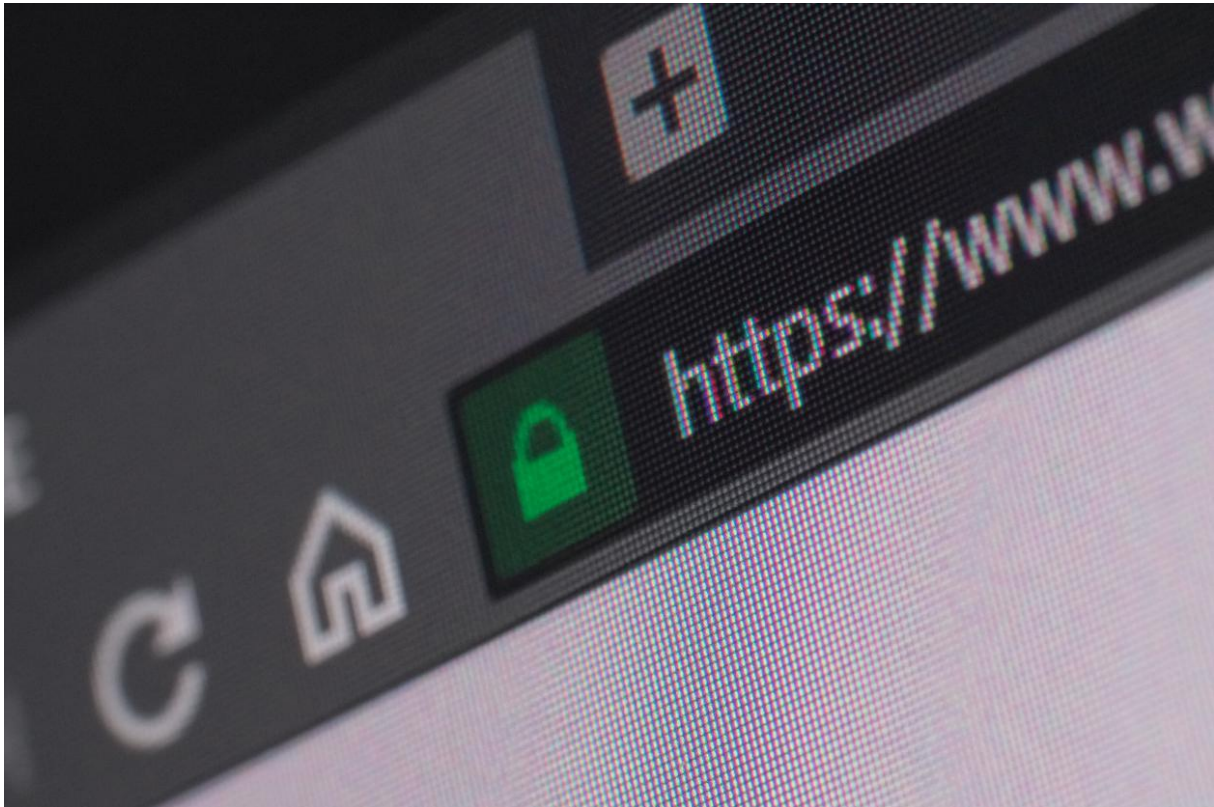
- Lažni web shopovi često nude samo kartično plaćanje jer im je cilj samo uzeti novac ili podatke kartice. Pouzeće im ne odgovara jer tada moraju stvarno poslati paket. Ako nema pouzeća niti PayPala, to je ozbiljan *red flag* – smatra Majsan.

Zeleni lokot kod adrese ne mora ništa značiti

Jedna od najrasprostranjenijih zabluda je da ta HTTPS protokol, koji se pokazuje kao zeleni lokot u adresnoj traci preglednika, jamči sigurnost

stranice. Stručnjaci CARNET-ovog Nacionalnog CERT-a objašnjavaju da i lažne trgovine danas mogu besplatno pribaviti HTTPS certifikat. Protokol znači samo to da je komunikacija između vašeg preglednika i servera šifrirana, ali ništa ne govori o tome tko je na drugom kraju te šifrirane veze.

- Lokot više ne znači sigurnost! Postojanje HTTPS protokola („lokota“) nekada se navodilo kao pokazatelj sigurnosti web stranice, danas to više nije tako – objašnjavaju nam iz CARNET-ovog Nacionalnog CERT-a.



Lokot uz adresu webshopa nekada nije dovoljan indikator sigurnosti

Robertax/Getty Images

Kriminalci su i inače korak ispred intuicije prosječnog kupca. Stručnjaci CARNET-ovog Nacionalnog CERT-a opisuju jedan tipičan modus operandi. Korištenjem dostupnih alata, kriminalci vrlo brzo mogu kopirati legitimne stranice i kreirati lažne. Privid legitimnosti stvaraju korištenjem naziva i logotipa poznatih brendova te osmišljavanjem popratne priče o zatvaranju trgovine ili nekog drugog razloga za niske cijene. Često se i reklamiraju na društvenim mrežama gdje korisnici u trenutku nepažnje mogu nasjesti na prijevaru.

Majsan to iz iskustva svog rada s web-shopovima potvrđuje:

- Ako je oglas agresivan, cijena ekstremna, a brend nepoznat, oprez! Ako neka ponuda izgleda predobro da bi bila istinita, onda to obično i jest tako – ističe Majsan.

Postoje alati koji zaista pomažu

CARNET-ov Nacionalni CERT razvio je CERT iffy, dostupan na iffy.cert.hr. Dovoljno je upisati adresu sumnjive stranice, a sustav provjerava nalazi li se ona na popisu domena koje su već prijavljene i potvrđene kao lažne. Važno upozorenje: alat provjerava samo već evidentirane stranice, pa negativan rezultat nije potvrda sigurnosti, samo potvrda da ta stranica još nije prijavljena.

Udruga eCommerce Hrvatska vodi popis certificiranih web-shopova na safeshop.hr, a provjeru domene nudi i na check.ecommerce.hr.

- Oznaka povjerenja ili *trustmark* potvrđuje da je webshop prošao provjeru od nezavisne strane. Naravno da se sama oznaka lako može kopirati, no naš sustav omogućuje da klikom na nju vidite profil certificirane trgovine i njihove recenzije - objašnjava Majsan.

Za domaće shopove, OIB koji navode na stranici može se provjeriti u Sudskom registru ili na FINA-i.

- Ako nešto krene po zlu, bez tih podataka nemate kome poslati ni prigovor, a kamoli tužbu - kaže Majsan.

Kako platiti da bude sigurno?

A što u situaciji kada možete kupiti samo od prodavača kojeg niste ranije probali, a baš samo on ima proizvod koji vam treba? Napravili ste sve provjere: potražili ste tvrtku u registru, provjerili CERT iffy, pregledali Google recenzije, pa sve izgleda u redu. No ipak niste sigurni. Što je siguran izbor u takvoj situaciji?

Platiti se može na više načina. Pouzećem novac dajete tek kad paket stigne, PayPal nudi mehanizam prigovora koji je relativno lako aktivirati, a najpopularnije, kartično plaćanje, je sigurno ako ide kroz poznate payment *gatewaye*. U Hrvatskoj su to npr. Monri, Corvus i ostali e-commerce provideri kartičnog plaćanja. Šanse za legitimnost su veće jer je tvrtka prošla i njihovu provjeru.

A za situacije kad kupujete na mjestima koja tek isprobavate, postoji i četvrta opcija koja sve navedene dopunjuje logičnom mjerom predostrožnosti: jednokratna virtualna kartica.

Virtualna kartica u ponudi Zagrebačke banke

Mastercard jednokratna virtualna kartica uz tekući račun u eurima ili osnovni račun dostupna je svim korisnicima aplikacije m-zaba, a ugovara se u rubrici Kartice u svega nekoliko sekundi, bez naknade i bez odlaska u poslovnicu. Postupak aktivacije traje svega nekoliko sekundi. U rubrici Kartice odabire se opcija ugovaranja jednokratne virtualne kartice, bez naknade i potpuno digitalno. Prilikom prvog izdavanja potrebno je prihvatiti Ugovor za izdavanje i upotrebu jednokratne virtualne kartice koji stiže na e-mail. Prilikom sljedećih izrada virtualne kartice nema potrebe za novim ugovorima. Odmah nakon aktivacije dostupni su svi podaci potrebni za plaćanje te ih je moguće jednostavno kopirati u obrazac za kupnju.

Korisnik sam odabire iznos koji želi staviti na raspolaganje, do maksimalno 1.300 eura, a podaci kartice odmah su dostupni i jednostavno se kopiraju u obrazac za plaćanje na bilo kojoj web-stranici. Cijeli proces traje kraće nego što treba za pronalazak fizičke kartice u novčaniku.

Ono što ovu Mastercard karticu Zagrebačke banke čini posebno prikladnom za kupnju na novim ili manje poznatim web-mjestima jest to da broj kartice vrijedi samo za jedno plaćanje, a nakon toga automatski prestaje važiti. Budući da su podaci jednokratni, nema mogućnosti neovlaštenih ponovnih naplata ni zlouporabe kartičnih podataka, pa korisnik može sigurno kupovati online bez brige da će broj kartice završiti u pogrešnim rukama. Zbog jednokratne prirode kartica nije pogodna za pretplate ili rezervacije sredstava, za što i dalje služi standardna kartica.

Logika je jasna. Ako ne znate dovoljno o web-shopu, zašto mu davati broj kartice koja vrijedi godinama? Jednokratnom virtualnom karticom dajete mu točno onoliko koliko ste odredili i ništa više.

Dakle, čak i u scenariju kada nasjednemo na prijevaru, primjerice platili smo 60 eura za robu koja neće stići, ostatak računa ostaje zaštićen. Broj kartice koji prevaranti dobiju više ne funkcionira ni za što.

Majsan virtualnu karticu promatra kao trend koji potvrđuje zrelost domaćeg tržišta:

- Jednokratne virtualne kartice smanjuju rizik zlouporabe jer ograničavaju iznos i trajanje kartice. To je pametan alat kad kupujete na novim ili manje poznatim webshopovima – kaže Majsan.

A što kada nasjednemo?

Unatoč svim provjerama, može se dogoditi da nasjednemo, pogotovo zbog toga što su prevaranti, a time i prevare, svakim danom sve bolje i sve teže za prepoznati. U tom scenariju, brzina reakcije je presudna, a mjeri se u minutama, ne satima.

Ako ste unijeli podatke bankovne kartice, odmah zovite banku i zatražite blokadu i prijavite slučaj. Ne odobravajte nikakve autorizacije plaćanja koje sami niste pokrenuli i uključite dvofaktorsku autentifikaciju i obavijesti o transakcijama ako ih već nemate. Ako ste unijeli lozinku, promijenite je odmah, na svim servisima gdje koristite istu. Ostavili ste email ili broj telefona? Pojačajte oprez, jer mogu uslijediti *phishing* poruke i sumnjivi pozivi.

Sumnjive adrese mogu se, kako smo već naveli, prijaviti Carnetovom Nacionalnom CERT-u putem iffy.cert.hr, što uvelike pomaže u evidentiranju i uklanjanju takvih stranica, a prijevaru i lokalnoj policiji.

Tri važna koraka

Na pitanje koje bi tri navike preporučili svima koji redovito kupuju online, i CARNET-ov Nacionalni CERT i Majsan govore istim jezikom, no s drugačijim naglaskom.

Stručnjaci CARNET-ovog Nacionalnog CERT-a stavljaju na prvo mjesto svjesnost. Biti svjestan da prijevare postoje i da su sofisticirane nije paranoja, nego osnovna digitalna pismenost. Tko zna da prijevare postoje, teže na njih nasjedne. Zatim dolazi pauza, ako vas web-shop uvjerava da uskoro ističe ponuda i da su ostali zadnji komadi, to nije signal za žurbu. Naprotiv.

- Googlajte ime webshopa plus riječ 'iskustva' ili 'prijeara'. Provjeri jesu li navedeni podaci o tvrtki u uvjetima poslovanja. Koriste li neki siguran način plaćanja. I ako nešto izgleda predobro da bi bilo istinito, ono u 90 posto slučajeva i jest. Rizik postoji, ali internet je samo alat. Zdrav razum je i dalje najbolji recept protiv bilo kakve prijevare – zaključuje Majsan.