

VELIKI VODIČ KROZ KARTIČNE PRIJEVARE

Telegram i Erste banka donose
50 savjeta koje svatko treba znati

Uvod

Sve više plaćamo karticama, neovisno o tome je li riječ o kupnji putem interneta ili na POS uređajima u fizičkim trgovinama. Ovaj način plaćanja donosi brojne prednosti, poput brzine, jednostavnosti te mogućnosti kupnje s globalnim dosegom. No, unatoč prednostima, s porastom upotrebe kartica raste i broj prijetnji u digitalnom svijetu. Naime, kartične prijevare postale su ozbiljan problem. Prevaranti koriste sofisticirane tehnike kako bi došli do podataka, a pritom im je sve teže ući u trag.



589.468.666

ukupan broj transakcija platnim karticama
koje su izdane u Hrvatskoj u 2023. godini

84,98%

debitne kartice

15,01%

kreditne kartice

Među najpoznatijim metodama kartičnih prijevara ističe se **phishing**, pri čemu prevaranti putem lažnih e-mailova ili SMS poruka pokušavaju navesti korisnike da otkriju svoje osobne podatke i podatke o kartici, često preko lažnih web-stranica koje nalikuju onima pravih banaka.

Vrlo česta praksa je i **skimming**, koji podrazumijeva postavljanje posebnih uređaja na bankomate ili POS terminalе radi kopiranja podataka s kartica, uključujući broj kartice i PIN, što prevarantima omogućuje neovlašteno korištenje tih podataka.

Treći oblik prijevare je **malware** napad, pri kojem se zlonamjerni softver instalira na korisničke uređaje putem sumnjivih linkova ili preuzimanja, omogućujući prevarantima praćenje unosa osjetljivih podataka, uključujući brojeve kartica i lozinke





Iako se sigurnost kartičnog plaćanja razvija svakodnevno, važno je podizati svijest o zaštiti kartičnih podataka. Upravo zbog toga, u suradnji s Erste bankom, kreirali smo sveobuhvatan vodič za zaštitu plaćanja.

U nastavku pročitaj čak
50 savjeta za prevenciju
prijevare i krađe
kartičnih podataka.

Opće mjere opreza

- 1 Redovito provjeravajte izvatke računa i transakcije.**
Kako biste brzo uočili neovlaštene transakcije i odmah reagirali.
- 2 Postavite obavijesti za svaku transakciju na svojoj kartici.**
Pravovremene obavijesti omogućuju brzo prepoznavanje sumnjivih aktivnosti.
- 3 Ne dijelite PIN ni s kim.**
Dijeljenjem PIN-a povećavate rizik od zloupotrebe kartice.
- 4 Nikada ne zapisujte PIN na papiru ili u digitalnim dokumentima.**
Zapisivanje PIN-a povećava šanse za krađu podataka.
- 5 Držite karticu na sigurnom mjestu i uvijek je nosite sa sobom.**
Gubitak kartice važno je brzo prijaviti kako biste spriječili neovlašteno korištenje.
- 6 Ako izgubite karticu, odmah je blokirajte.**
Blokiranje kartice sprječava neovlaštene transakcije nakon gubitka.
- 7 Koristite kartice samo kod provjerenih trgovaca i na sigurnim web stranicama.**
Nepouzdane lokacije povećavaju rizik krađe podataka.
- 8 Izbjegavajte koristiti javne Wi-Fi mreže za online transakcije.**
Javne mreže su često nesigurne i olakšavaju pristup vašim podacima.
- 9 Nikada ne odgovarajte na e-mailove ili poruke koje traže podatke o kartici.**
Phishing poruke primarno traže takve podatke.
- 10 Redovito mijenjajte lozinke za svoje bankovne račune.**
Česte promjene lozinki smanjuju rizik od neovlaštenog pristupa.

Online kupnja

- 11 Koristite samo sigurne web stranice s "https://" u adresi.**
"HTTPS" osigurava da su podaci šifrirani tijekom prijenosa.
- 12 Provjerite recenzije online trgovca prije kupnje.**
Recenzije pomažu otkriti pouzdanost trgovca i izbjegći prijevare.
- 13 Koristite virtualne kartice za online transakcije.**
Virtualne kartice smanjuju rizik zloupotrebe podataka glavne kartice.
- 14 Aktivirajte dodatnu autentifikaciju (npr. SMS kod ili aplikaciju).**
Dodatni sloj sigurnosti sprječava neovlaštene transakcije.
- 15 Izbjegavajte spremanje podataka o kartici na web stranicama.**
Spremljeni podaci mogu biti ukradeni tijekom hakiranja stranice.
- 16 Koristite aplikacije za plaćanje koje nude sigurnosne značajke.**
Aplikacije s enkripcijom štite vaše podatke tijekom plaćanja.
- 17 Ne klikajte na sumnjive linkove u e-mailovima ili porukama.**
Sumnjivi linkovi često vode na lažne stranice za krađu podataka.
- 18 Izbjegavajte online trgovine koje traže previše osobnih podataka.**
Prekomjerni zahtjevi za informacijama mogu biti znak prijevare.
- 19 Koristite antivirusni softver na uređajima koje koristite za online kupnju.**
Antivirus štiti od zlonamjernog softvera koji cilja vaše podatke.
- 20 Postavite limit za online transakcije.**
Limiti smanjuju potencijalnu štetu u slučaju krađe podataka.

ODIGRAJ NAŠU IGRICU I TESTIRAJ SVOJE PONAŠANJE ONLINE

Možeš li prijeći sve razine?



Korištenje na fizičkim lokacijama

- 21 Koristite bankomate samo na sigurnim lokacijama.**
Bankomati na izoliranim mjestima češće su meta manipulacija.
- 22 Provjerite ima li bankomat sumnjivih dodataka na čitaču kartica.**
Lažni čitači kartica mogu krasti podatke.
- 23 Rukom sakrijte PIN dok ga unosite.**
Skrivanjem PIN-a sprječavate da ga netko vidi i zabilježi.
- 24 Ne dajte svoju karticu trgovcima izvan vašeg vidokruga.**
Kartica izvan vašeg nadzora može biti kopirana ili zloupotrijebljena.
- 25 U restoranima i kafićima, tražite prijenosni uređaj za naplatu.**
Prijenosni uređaji smanjuju rizik od zloupotrebe kartice.
- 26 Redovito čistite čip kartice kako bi ispravno radila.**
Neispravan čip može otežati transakcije i povećati rizik od manipulacije.
- 27 Izbjegavajte davanje kartice drugima, čak i privremeno.**
Svaka osoba koja drži vašu karticu može zloupotrijebiti podatke.
- 28 Koristite beskontaktno plaćanje kad god je moguće.**
Beskontaktno plaćanje smanjuje rizik od fizičkog oštećenja kartice.
- 29 Provjerite račun nakon svake transakcije kako biste bili sigurni da je iznos ispravan.**
Brza provjera smanjuje šanse za pogreške ili prijevare.
- 30 Držite kartice odvojene od dokumenata poput osobne iskaznice.**
Odvojeno držanje otežava krađu svih vaših podataka odjednom.

Sigurnosne značajke

- 31 Aktivirajte 3D Secure za online plaćanja.**
Ova autorizacija dodatno je osiguranje za vaše transakcije.
- 32 Koristite aplikacije banaka za praćenje transakcija u stvarnom vremenu.**
Pravovremene obavijesti omogućuju brzo reagiranje na neovlaštene transakcije.
- 33 Postavite geografska ograničenja za korištenje kartice.**
Ograničenja smanjuju mogućnost zloupotrebe u inozemstvu.
- 34 Koristite kartice s tehnologijom tokenizacije za dodatnu sigurnost.**
Tokenizacija zamjenjuje osjetljive podatke s privremenim tokenima.
- 35 Isključite funkciju beskontaktnog plaćanja ako je ne koristite.**
Isključena funkcija smanjuje mogućnost nenamjernih transakcija.
- 36 Redovito provjeravajte rok valjanosti kartice i naručite novu na vrijeme.**
Nevažeća kartica može uzrokovati poteškoće i povećati rizik prijevare.
- 37 Blokirajte transakcije u inozemstvu ako ih ne planirate raditi.**
Blokiranje smanjuje rizik od zloupotrebe izvan zemlje.
- 38 Postavite dnevne limite za transakcije.**
Limiti štite od velikih finansijskih gubitaka u slučaju prijevare.
- 39 Koristite opciju zamrzavanja kartice kad je ne koristite.**
Zamrzavanje kartice sprječava sve transakcije dok je ne aktivirate.

Zaštita od krađe podataka

- 40 Nikada ne dijelite fotografije kartice.**
Fotografije olakšavaju zloupotrebu podataka.
- 41 Izbjegavajte ostavlјati podatke o kartici u javnim dokumentima ili aplikacijama.**
Podaci na javnim mjestima lako mogu biti zloupotrebљeni.
- 42 Uništite stare kartice rezanjem kroz broj i čip.**
Uništavanje kartice sprječava njenu ponovnu upotrebu.
- 43 Budite oprezni s osobama koje tvrde da su iz vaše banke i traže podatke.**
Banke nikad ne traže osjetljive podatke telefonom ili e-mailom.
- 44 Nemojte unositi podatke o kartici na javnim računalima.**
Javna računala mogu biti zaražena zlonamernim softverom.
- 45 Redovito pratite obavijesti banke o sigurnosnim prijetnjama.**
Informacije pomažu u pravovremenoj zaštiti od novih oblika prijevare.
- 46 Koristite dvofaktorsku autentifikaciju za pristup aplikacijama banaka.**
Dodatni sloj zaštite otežava neovlašteni pristup.
- 47 Ne dijelite podatke o kartici telefonom osim ako ste sigurni u identitet sugovornika.**
Nepoznati pozivi mogu biti pokušaji prijevare.
- 48 Educirajte se o najnovijim oblicima kartičnih prijevara.**
Informiranost smanjuje šanse za postajanje žrtvom prijevare.
- 49 Budite oprezni s novim, nepoznatim tehnologijama za plaćanje.**
Nove tehnologije mogu imati neotkrivene sigurnosne propuste.
- 50 Ako sumnjate na prijevaru, odmah kontaktirajte banku i prijavite incident.**
Brza reakcija ograničava štetu i osigurava povrat sredstava.

Ako sumnjate na neovlašteno korištenje kartica potrebno je:

odmah blokirati karticu pozivom u Kontakt centar Erste banke na broj telefona **072 555 555** (poziv iz inozemstva **+385 51 365 591**).

U slučaju prijevare bilo koje vrste ili čak sumnje na istu, kontaktirajte svoju banku. U Erste banci radi poseban tim stručnih djelatnika s višegodišnjim iskustvom nadležnih za kartičnu sigurnost tako da im se uvijek možete obratiti. Imajte na umu da Erste banka osigurava razvijen sustav autorizacije, praćenja i provjeravanja transakcija 24 sata. Osim toga, bankomati Erste banke opremljeni su suvremenim, tehničkim oblicima zaštite koji onemogućavaju kopiranje podataka s kartice, odnosno krađu podataka s kartica.

Na ovaj način banka svojim korisnicima omogućuje sigurniju kupnju na internetu, štiti svoje korisnike i nudi im dodatne opcije zaštite. Ako niste korisnik, privatni ili poslovni, u Erste banci, a strahujete da biste mogli biti ili jeste prevareni - kontaktirajte svoju banku, a uvijek se možete javiti i nadležnoj policijskoj upravi.