VIANOCE 2026

RÝCHLY NÁVOD PRE RODIČOV A STARÝCH RODIČOV

# Nákupy bez podvodu

Ako sa pri nakupovaní na internete nenechať nachytať podvodníkmi – od Black Friday až po Vianoce.

5

MINÚT ČÍTANIA

POŠLI TO ĎALEJ

**Prepošli to mame, ockovi aj babke. Na tvoje slovo dajú.**

ÚVOD

# Prečo vám to posielame práve teraz

## Milí rodičia,

tento krátky návod vám posiela niekto, komu na vás záleží. Nie preto, že by ste si nedávali pozor – ale preto, že podvodníci sú dnes oveľa šikovnejší ako pred pár rokmi.

Prečítanie zaberie päť minút a môže vám ušetriť peniaze aj nervy.

## 1 Obdobie veľkých nákupov a menšej ostražitosti

Black Friday už dávno nie je jeden piatok. Akcie trvajú od začiatku novembra cez Cyber Monday až po darčeky na poslednú chvíľu. Nakupujeme viac, rýchlejšie a v zhone, čakáme nízke ceny a bojíme sa, že nám zľava ujde. Presne s týmto podvodníci rátajú.

**76 %**
Slovákov začne s vianočnými nákupmi do konca novembra

**7 z 10**
kúpi aspoň polovicu darčekov na internete

**257 €**
je priemerný rozpočet na vianočné darčeky

Zdroj: Česko-slovenský E-commerce barometer 2026, ui42 a Ipsos.

## 2 Podvodníci pritvrdzujú – a technológie im pomáhajú

Umelá inteligencia im dnes za pár minút napíše bezchybnú správu po slovensky, skopíruje web známeho obchodu aj s fotkami a vymyslí desiatky „spokojných“ recenzií. Falošných e-shopov a podvodných SMS preto pribúda rýchlejšie ako kedykoľvek predtým.

**54 %**

obetí podvodov vo svete naletelo práve pri nakupovaní

GASA 2025

**236 €**

v priemere stratí Slovák, ktorý naletí online podvodu

Visa 2025

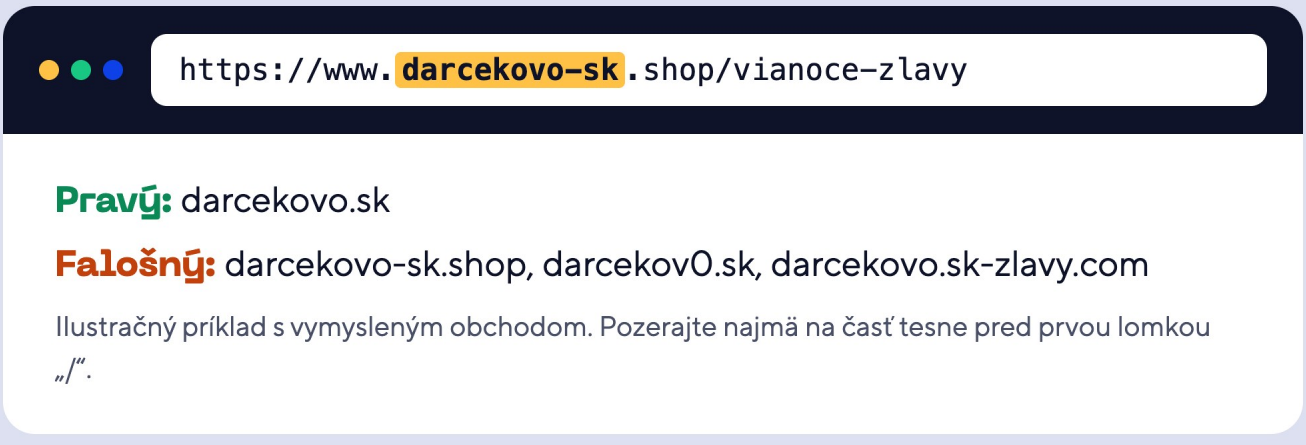
**155 mil. €**

ročne stoja online podvody Slovensko

Visa 2025

## 3 Podvod na prvý pohľad nespoznáte

Falošný web má rovnaké logo, farby aj fotky ako originál. SMS od „kuriéra“ príde práve vtedy, keď na balík naozaj čakáte. Rozdiel býva len v jednom písmene adresy. Preto sa nespoliehajte na to, ako vec vyzerá - **overujte**.




**Pravý:** darcekovo.sk

**Falošný:** darcekovo-sk.shop, darcekov0.sk, darcekovo.sk-zlavy.com

Ilustračný príklad s vymysleným obchodom. Pozerajte najmä na časť tesne pred prvou lomkou „/“.

# Nakupujete v e-shope prvýkrát?

Najväčšie riziko je, že obchod vôbec neexistuje. Pred zaplatením si dajte päť minút na kontrolu.

1. **Zistite, kto obchod prevádzkuje**
   Na stránke musí byť názov firmy, IČO a adresa. Keď kontakty chýbajú, nenakupujte.

2. **Prečítajte si adresu webu**
   Podvodníci menia jediný detail: pomlčku, písmeno navyše alebo koncovku ako .shop či .store.

3. **Príliš lacné je podozrivé**
   Značkový tovar o 70 – 90 % lacnejší ako všade inde je návnada. Porovnajte cenu v porovnávači cien.

4. **Recenzie hľadajte mimo e-shopu**
   Zadajte do Googlu názov obchodu a slovo „podvod“, pozrite Heureku. Žiadne alebo samé päťhviezdičkové recenzie sú zlý signál.

5. **Platte kartou alebo na dobierku**
   Ak obchod chce len prevod na účet alebo kryptomeny, odíďte. Pri karte vám banka vie peniaze najskôr vrátiť.

6. **Nedajte sa uponáhľať**
   „Posledné 2 kusy“ či odpočítavanie „ešte 10 minút“ majú vyvolať paniku. Je to dôvod spomaliť, nie zrýchliť.

# Nakupujete v obchode, ktorý poznáte?

Tu nehrozí, že obchod neexistuje. Hrozí, že sa zaň niekto vydáva – alebo že zľava nie je skutočná.

1 **Do obchodu vstupujte sami, nie cez odkaz**

Napíšte adresu do prehliadača alebo otvorte aplikáciu obchodu. Odkaz v e-maile, SMS či reklame môže viesť na dokonalú kópiu.

2 **Overte, či je zľava skutočná**

Ako pôvodnú cenu musí obchod uviesť najnižšiu cenu za posledných 30 dní. Históriu ceny ukáže porovnávač.

3 **Pozrite, kto tovar naozaj predáva**

Na veľkých trhoviskách často nepredáva samotný obchod, ale iný predajca. Skontrolujte jeho hodnotenia.

4 **„Zmenili sme číslo účtu" = podvod**

Takýto e-mail si vždy overte na zákazníckej linke z oficiálneho webu obchodu.

5 **Chráňte si svoj účet**

Pre každý obchod použite iné heslo a zapnite overenie cez mobil, ak ho obchod ponúka.

# Pozor na SMS, e-maily a telefonáty

Podvod nie je vždy o peniazoch hneď. Často chcú vaše údaje - a zneužijú ich neskôr.

**SMS · „KURIÉR"**
Vašu zásielku nemožno doručiť. Doplaťte clo 1,99 € a aktualizujte adresu: bit.ly/...

**Malá suma je návnada.** Na falošnej stránke vyplníte celú kartu a podvodník z nej potom čerpá oveľa viac. Stav balíka si overte priamo v e-shope.

**E-MAIL · „BANKA" ALEBO „OBCHOD"**
Váš účet bol zablokovaný. Overte svoju totožnosť do 24 hodín.

**Odkaz vedie na falošné prihlásenie.** Do banky sa prihlasujte vždy sami, cez aplikáciu alebo adresu, ktorú poznáte.

**TELEFONÁT · „BANKÁR" ALEBO „POLICAJT"**
Váš účet je ohrozený, peniaze musíme hneď presunúť na bezpečný účet.

**Žiadny „bezpečný účet" neexistuje.** Zložte a zavolajte do banky sami.

## Banka, polícia ani kuriér od vás nikdy nebudú chcieť:

- PIN ani kód, ktorý vám prišiel v SMS
- heslo do internetbankingu alebo údaje z karty
- presun peňazí na „bezpečný" účet

Keď váhate: **zložte a zavolajte na číslo zo zadnej strany vašej karty.**

KEĎ SA TO PREDSA STANE

# Naletieť môže každý

## Nie je to vaša chyba. A nie je sa za čo hanbiť.

Digitálny svet sa vyvíja extrémnou rýchlosťou. Aj keď dodržíte všetky rady, podvodníkom môžete naletieť – stáva sa to aj ľuďom, ktorí s technológiami pracujú každý deň.

**Povedzte to čo najskôr niekomu blízkemu.** Rýchly zásah môže v niektorých prípadoch vrátiť zaplatené peniaze alebo zabrániť zneužitiu vašich údajov.

1

KROK 1

### Okamžite volajte banku HNEĎ

Dajte zablokovať kartu a požiadajte o vrátenie platby. Čím skôr, tým väčšia šanca, že peniaze ešte zastavia.

2

KROK 2

### Zmeňte heslá

Ak ste na podozrivej stránke zadali prihlasovacie údaje, zmeňte ich všade, kde ste ich používali.

3

KROK 3

### Povedzte to blízkym

Pomôžu vám s ďalšími krokmi – a vy na to nebudete sami.

4

KROK 4

### Nahláste to

Na polícii aj pri menšej sume, priložte snímky objednávky a platby. Pri slovenskom e-shope aj Slovenskej obchodnej inšpekcii.

NA VYSTRIHNUTIE ALEBO NA CHLADNIČKU

# Naša dohoda

## Keď ťa niekto žiada o platbu, údaje alebo kód, najprv zavolaj mne.

MOJE MENO A ČÍSLO

ČÍSLO NA VAŠU BANKU

Nájdete ho na zadnej strane platobnej karty.

## Ak ponuka vyzerá príliš dobre na to, aby bola pravdivá, takmer vždy ide o podvod.

Spomaľte, overte si to a až potom platťte. Žiadna ponuka nepotrebuje akútne konanie z vašej strany.

---

**ui42 — podporujeme férové e-shopy.**

**ui42.sk** · Zdroje: Česko-slovenský E-commerce barometer 2026 (ui42, Ipsos), GASA Global State of Scams 2025, prieskum Visa 2025, FRA 2026.