

THE HUMAN READINESS COMPANY
CYBERREADY

**NAKUPUJTE
BEZPEČNĚ
BĚHEM TOHOTO
ČERNÉHO PÁTKU**



Jak fungují podvody při nákupu

Podvody při nákupu se soustředí na získání vašich finančních informací. Způsoby jsou například:

Reklamní pasti, které vás lákají vstoupit na falešnou webovou stránku a poskytnout informace o vaší kreditní kartě

Platební metody, které vás nutí zadat informace o vaší kreditní kartě (spíše než používat digitální peněženku nebo platební službu)

Push upozornění lákající prostřednictvím e-mailu nebo SMS, které vás svádí ke kliknutí na škodlivé odkazy o očekávaném doručení



Proč jsme v tomto ročním období zranitelnější vůči podvodům?

Jsme zahlceni rozhodnutími, nabídkami a časově omezenými akcemi a v těchto dnech jsme neustále rozptýleni.

Obklopují nás vzrušující nové produkty a možnosti; nové informace o doručování zaplavují naše smartphony a my si zvykáme posílat peníze pouhým klepnutím prstu.

Tyto faktory oslabují náš úsudek:

- Webové stránky obchodu jsou naším jediným referenčním bodem
- Časově omezené nabídky znesnadňují hledání podrobností
- Neznámí odesílatelé nám často posílají zprávy a e-maily
- Sledování našich bankovních poplatků může být náročné

Hackeri to vědí a útočí více.



Co mohu dělat?



Před nákupem

Vždy zadávejte URL sami.
Nepoužívejte odkaz z reklamy
nebo e-mail

Používejte oficiální nákupní
aplikace značek na svém
smartphonu

Během nakupování



Zkontrolujte přítomnost
symbolu zámku
vedle
URL adresy webové
stránky

Použijte metodu třetí strany,
která nepřenáší
informace o kreditní kartě
prodejcům (například PayPal
či Venmo)
nebo použijte kartu na jedno
použití

Po nákupu:

Navštivte web a podívejte se
na aktualizace. Neklikejte na
odkazy v e-mailech nebo
textech, které tvrdí, že
poskytují aktualizace
objednávek

Hlídejte na svém finančním
úctu jakékoli neoprávněné
transakce



Všimli jste si podvodu?

Nahlste ho příslušné znače.



Máte pocit, že jste byli podvedeni?

Upozorněte místní policii.