

KYBER

jihočeské policie

RÁDCE

**VARUJEME
PORADÍME
VYSVĚTLÍME**

**jak NENALETĚT šmejdům
z ON-LINE SVĚTA**



KYBER RÁDCE

jihočeské policie

👉 NA ÚVOD

- Kybernetická kriminalita rychle roste a tvoří stále větší část trestné činnosti.
- Podvodníci útočí hlavně přes telefon a internet.
- Jsou dobře připraveni, vědí, jak zmanipulovat lidi a dostat vás do stresu.
- Naletět může každý.

👉 JAK PODVODY FUNGUJÍ

- Podvodníci neustále vymýšlí nové způsoby, jak se dostat k Vaším penězům.
- Často se vydávají za banky, investiční společnosti nebo za policisty.
- Jakmile se dostanou k Vaším penězům, převedou je co nejrychleji na jiné účty, nejčastěji do zahraničí.
- Umí téměř dokonale skrýt svou totožnost, jakmile Vám peníze ukradnou, bývá velmi těžké je získat zpět.

**Důležité je být vždy ostražitý
a ověřovat si informace ze spolehlivých zdrojů.**

NAPADENÝ BANKOVNÍ ÚČET? NESMYSL!

👉 JAK TO PROBÍHÁ?

- Zavolá vám „policista“ nebo „bankéř“, který bude tvrdit, že Váš účet je napadený, bude mluvit profesionálně.

👉 CO PO VÁS PACHATEL CHCE?

- Vaše peníze. Když mu uvěříte, nabídne Vám možnosti, jakými můžete své peníze „zachránit“:
 - převést je na „bezpečný účet“,
 - vložit do bitcoinu,
 - předat konkrétní osobě (např. policistovi, kurýrovi).

👉 NOVÝ TREND

- Podvodník jako policista přesvědčí oběť, že peníze nejlépe zachrání tím, že je předá konkrétní osobě.
- Bude se prokazovat falešným služebním průkazem policisty nebo kriminalisty, který Vám zašle na e-mail, případně na WhatsApp.

NAPADENÝ BANKOVNÍ ÚČET? NESMYSL!

👉 MANIPULACE

- Podvodník Vás přesvědčí, abyste o telefonátu s ním nikomu neříkali. Tvrdí, že jde o tajnou akci a věřit máte jen jemu.
- Svým telefonátem Vás vyděsí natolik, že zapomenete na zdravý rozum a ve strachu o své peníze jednáte bezmyšlenkovitě.

👉 RADY

- V České republice nemůže být bankovní účet nikým napaden bez toho, aniž by mu to majitel účtu sám umožnil.
- Peníze uložené v bankách jsou ze zákona pojištěné. Pokud z Vás někdo vyloudí přihlašovací údaje a přijmete o peníze vlastní neopatrností, pak se na Vás zákonné pojištění vkladu nevztahuje.
- Policista ani bankéř si k Vám pro peníze nikdy nepřijdou. Nikdy Vás nebudou nutit cokoliv kamkoliv převádět!
- Policista Vám nikdy nebude posílat svůj služební průkaz.
- Jakoukoliv informaci, která se týká Vašeho účtu, si vždy ověřte u Vašeho bankovního poradce či přímo ve Vaší bance.

INVESTICE ANO, ALE NE S PODVODNÍKY!

👉 JAK TO ZAČÍNÁ?

- Podvod obvykle začíná reklamou na internetu nebo sociálních sítích slibující vysoké zisky bez rizika.
- Po vyplnění formuláře Vás kontaktuje „poradce“, který Vás přesvědčí k první investici.
- Někdy Vás osloví sami s tvrzením, že u nich už máte zhodnocené peníze, které je potřeba neprodleně vybrat.

👉 CO SE STANE?

- Podvodník je opět velmi přesvědčivý a působí profesionálně. Nemá tak problém přesvědčit Vás k poslání prvních peněz určených k investování.
- Komunikace se poté přesune i na e-mail, kde podvodník posílá odkazy na falešné stránky s „rostoucí“ investicí a tím Vás přesvědčí k dalším vkladům.
- Podvodníci také nabízejí možnost spolupráce pomocí vzdáleného přístupu, chtějí nainstalovat program do Vašeho zařízení (např. AnyDesk, TeamViewer). Vysvětlí to tím, že Vám jako zkušení investoři vydělají více peněz za kratší dobu.

INVESTICE ANO, ALE NE S PODVODNÍKY!

👉 RIZIKO

- Pokud budete souhlasit se vzdáleným přístupem, prakticky tím pustíte pachatele ke svému internetovému bankovníctví.
- Můžete tak přijít nejen o všechny své peníze, ale pachatelé si u těchto případů sjednají na jméno oběti také tzv. předschválené bankovní úvěry. Budete tak splácet úvěr, ze kterého jste sami nic neutratili.
- Pojištění, které nabízejí pojišťovny i banky, v tomto případě nepomůže. Je to dáno tím, že jste pachatele k Vašemu účtu pustili prakticky sami.

👉 RADA

- Žádná investice není zcela bez rizika ztráty peněz. Buďte proto skeptičtí k vysokým výnosům a zaručeným ziskům. Rozhodnutí investovat prokonzultujte s někým zkušeným (bankovní poradce, někdo z rodiny, kdo již investuje).
- Společnost nebo investora, se kterým se rozhodnete investovat, si řádně ověřte.
- Nedovolte neznámým osobám vzdáleně vstupovat do Vašeho zařízení.

PRODÁVEJTE ZBOŽÍ TAK, ABYSTE PENÍZE VYDĚLALI, NE O NĚ PŘIŠLI!

👉 JAK TO PROBÍHÁ

- Rozhodli jste se prodat věci, které už doma nepotřebujete? Podvodníci reagují prakticky na každý nový inzerát, který se na internetových bazarových portálech objeví.
- „Zájemce“ se Vám většinou ozve se zprávou: „Dobrý den, je zboží stále k dispozici, mám zájem.“ nebo „Dobrý den, mám zájem o Vaše zboží, pošlu kurýra.“
- V případě, kdy na zprávu odpovíte kladně, přichází nabídka k využití přepravní společnosti. „Zájemce“ Vám bude tvrdit, že si zboží nemůže vyzvednout osobně.
- Poté Vás poprosí, abyste vyplnili údaje na stránkách přepravce, které Vám pošle. Tyto stránky jsou však falešné.
- Vy máte pocit, že prodáte své zboží bez práce, pohodlně, ale opak je pravdou. Místo vydělaných peněz ještě přijdete o ty, které máte na účtu.

PRODÁVEJTE ZBOŽÍ TAK, ABYSTE PENÍZE VYDĚLALI, NE O NĚ PŘIŠLI!

👉 CO PO VÁS PODVODNÍK CHCE

- Údaje z platební karty. Nabídne, že Vám za zboží zaplatí na platební kartu. Když mu údaje o své kartě dáte, je schopný ji okopírovat a platit s ní.
- Přístup do internetového bankovníctví. Na falešných stránkách přepravce se máte přihlásit do internetového bankovníctví. Jakmile zadáte přihlašovací údaje a kliknete na „přihlásit“, posíláte přihlašovací údaje přímo podvodníkům.

👉 RADA

- Při prodeji zboží preferujte osobní předání.
- Pokud chcete prodat zboží, pošlete zájemci své číslo účtu, kam Vám peníze má poslat, ne údaje o platební kartě (číslo karty, platnost, třímístný CVV/CVC kód).
- Číslo účtu zájemci musí stačit. Jakmile po Vás bude chtít cokoli jiného, zboží mu neprodávejte. Vše podstatné zná již z Vašeho inzerátu.

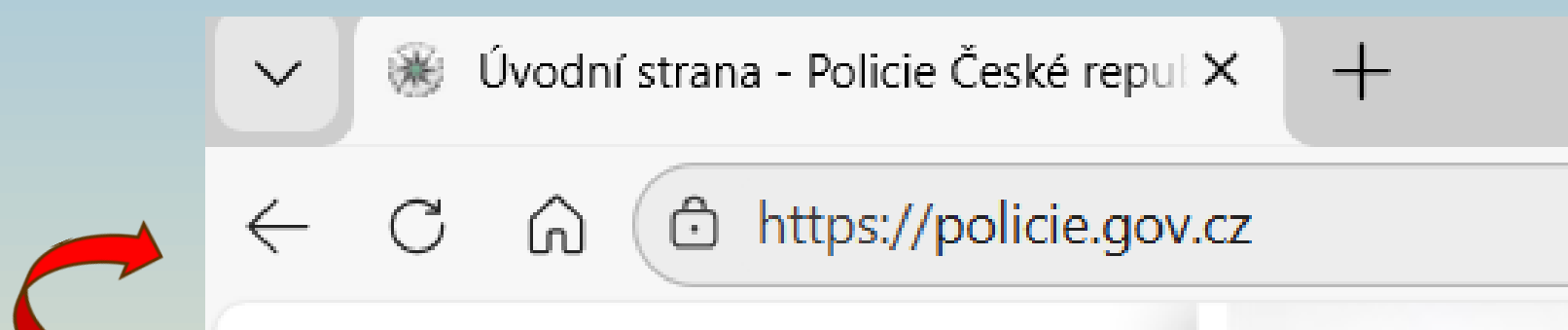
VÝHODNÉ NÁKUPY OPRAVDU VÝHODNĚ

👉 JAK TO PROBÍHÁ

- Rozhodli jste se nakoupit na internetu.
- Většina lidí hledá tu nejlepší nabídku.
- Nejnižší ceny však nemusí být vždy výhodou.

👉 VAROVNÉ SIGNÁLY

- Buďte obezřetní když:
 - je cena zboží podezřele nízká oproti nabídkám jiných prodejců,
 - nelze za zboží platit dobírkou,
 - kontakty na prodejce nejsou funkční, nelze se prodejci dovolat,
 - má prodejce na internetu negativní recenze,
 - zadáváte název prodejce do vyhledavače. Podvodníci mohou částečně pozměnit název webové stránky v příkazním řádku a tu pak vydávat za oficiální.



*příkazní řádek
s platnou adresou Policie ČR*

VÝHODNÉ NÁKUPY OPRAVDU VÝHODNĚ

👉 RADA

- Nakupujte na oficiálních stránkách e-shopů, vždy si zkontrolujte příkazní řádek s názvem prodejce.
- Ideální je nakupovat u prověřených a známých prodejců.
- Pravost e-shopu lze ověřit na stránkách České obchodní inspekce.
- Preferujte platbu dobírkou nebo převzetí zboží přímo na pobočce v kamenném obchodě.
- U méně známých prodejců si hledejte recenze, které jsou běžně dostupné na internetu.
- Kontrolujte adresu webu (URL) - dbejte na to, aby adresa začínala <https://> a aby název domény nebyl pozměněný (např. drobná změna písmen, přidání znak).

POHÁDKA: O ROZBITÉM TELEFONU A LIDECH V NOUZI.

👉 PŘÍBĚH

- „Ahoj mami/tati, potřebuji peníze. Mám problém se svým telefonem, píšu od kamaráda. Svůj telefon jsem ztratil a potřebuji peníze na nový. Pošlu ti číslo účtu, na který mi, prosím, pošli peníze.“

👉 REALITA

- Pachatelé se v tomto podvodu vydávají za syna, dceru nebo kamarády oběti, kterou kontaktují nejčastěji přes aplikaci WhatsApp.
- Vysvětlí Vám, proč píší z cizího čísla. Nejčastěji uvádí, že se telefon rozbil nebo že jim ho ukradli. Jednoduše ho nemohou použít.
- Napíší Vám číslo účtu, kam máte poslat své peníze, které „nutně“ potřebují. Přitom využívají toho, že každý se o své blízké, přátele a známé přirozeně bojí.

👉 RADA

- Neposílejte své peníze na neznámé účty na základě prosby někoho, koho jste nikdy neviděli a komunikujete s ním pouze po telefonu. Žádost si ověříte jednoduše tak, že tomu, kdo po Vás peníze chce, sami zavoláte na číslo uložené ve svých kontaktech.

SMS KÓDY A MOBILNÍ PLATBY

👉 JAK TO PROBÍHÁ

- Podvodníci v tomto případě nejčastěji působí na sociálních sítích, kde napodobují, případně ukradnou profil některého z uživatelů.
- Následně píší všem „přátelům“, které má uživatel na profilu přidané. „Ahoj, mám nové telefonní číslo, můžeš mi dát, prosím, na sebe mobilní telefon?“

👉 CO PO VÁS PACHATEL CHCE

- Peníze.
- Pokud pravdivost zprávy neověříte a své telefonní číslo pošlete, pachatel si na Vás na nějaké internetové stránce něco pořídí. Jako plátce transakce totiž zadá Vaše telefonní číslo. Jenže platba podléhá ještě unikátnímu potvrzovacímu kódu, který jako SMS přijde na Vaše telefonní číslo. A na přeposlání tohoto kódu podvodník čeká.

SMS KÓDY A MOBILNÍ PLATBY

👉 PŘÍBĚH

- *„Prosím tě, soutěžím v jedné soutěži o víkendový pobyt. Na mobil ti teď budou chodit zprávy s kódy. Čím víc kódů mi pošleš, tím větší šanci budu mít vyhrát. Pomůžeš mi?“*

👉 RADA

- Vždy si pravdivost informace ověřte. Kontaktujte pisatele jiným způsobem (telefonicky nebo mu napište přes jinou aplikaci).
- Neposílejte kódy, které obdržíte formou SMS zpráv. Jakmile kód odešlete, podvodník jej zadá a tím potvrdí internetovou nebo chcete-li mobilní platbu. Peníze Vám poté sice nezmizí z bankovního účtu, ale budou Vám naúčtovány v rámci Vašeho měsíčního tarifu u mobilního operátora.
- V domněnání, že známému nebo příbuznému pomáháte, nevědomky přicházíte o své peníze.

LÁSKA PŘES INTERNET

👉 JAK TO PROBÍHÁ

- Podvodník si Vás vyhlédne na internetu v prostředí sociálních sítí nebo na seznamkách. Snaží se s Vámi navázat komunikaci. Jeho cílem je vybudovat si s Vámi intenzivní virtuální vztah.
- Slibuje společnou budoucnost, získává si Vaši důvěru i citlivé informace. Vy se postupně zamilujete.

👉 CO PO VÁS PODVODNÍK CHCE

- Peníze. Ve skutečnosti tomu, kdo Vám píše, na Vás vůbec nezáleží.

👉 TRIKY

- Podvodníci se nejčastěji vydávají za vojáka, lékaře na misi či za studentku, kosmetičku, ale i za známé celebrity.
- V okamžiku, kdy podvodník nabyde dojmu, že už mu věříte, tak Vám napíše, že by za Vámi rád přijel a začal slibovaný společný život. Ale bohužel nemá k dispozici peníze na cestu nebo vymyslí jiný důvod, proč se jeho cesta za Vámi nemůže uskutečnit.

LÁSKA PŘES INTERNET

👉 POZOR

- V rámci již vybudovaného důvěrného vztahu se může stát, že po Vás podvodník bude chtít zaslat intimní materiály - fotografie nebo videa či citlivé informace o Vás.
- Pokud to uděláte, poskytnete mu tak prostředek, kterým Vás může začít teď nebo v budoucnu vydírat.

👉 RADA

- Nezapomeňte, že nikdy nevíte, kdo sedí za monitorem počítače nebo displejem mobilního telefonu.
- V dnešní době není problém se v prostředí internetu vydávat prakticky za kohokoliv.
- Když potkáte cizího člověka na ulici, také se před ním nesvlečete, neřeknete mu svá niterná tajemství a do ruky mu nedáte své mnohdy celoživotní úspory – tak proč to dělat přes internet?!

KYBERRÁDCE

jihočeské policie

POZOR

- Podvodníci se snaží dostat k Vaším úsporám za každou cenu, budou vymýšlet další nové triky, jak získat Vaše peníze.
- Kromě již popsaných podvodů se můžete setkat s nejrůznějšími falešnými odkazy, které Vám mohou přijít na e-mail, případně do textové zprávy.
- Zpráva či e-mail se mohou tvářit tak, že je posílá skutečná bankovní či státní instituce, firma nebo přepravní společnost. Chtějí po Vás např. doplatit částku za doručení balíčku, doplnit chybějící osobní údaje, např. adresu, uhrazení celního poplatku, nebo se tváří tak, že Vám chtějí zaslat třeba příspěvek na bydlení.
- Stále se můžete setkat s tzv. sezónními podvody. Zejména v období, kdy se řeší přeplatky na daních nebo na elektrice.
- Pozor také na výzvy k uhrazení pokut za rychlost ze strany podvodníků vydávajících se za Celní správu nebo Policii České republiky.

Nevyplňujte své osobní a citlivé údaje na odkazech, které jsou obsaženy v textových zprávách či e-mailech, které jste neočekávali. Odesílatele si vždy ověřte.

KYBER RÁDCE

jihočeské policie

...A NA ZÁVĚR MALÉ SHRNU TÍ...

👉 VAROVNÉ SIGNÁLY

- Tlak ze strany bankéře, zástupce investiční společnosti nebo policisty na Vaše rychlé rozhodnutí.
- Prosba o zaslání či sdělení přístupových hesel do Vašeho internetového bankovníctví, údaje k platební kartě, nainstalování aplikace do Vašeho zařízení umožňující vzdálený přístup.
- Podezřele výhodná koupě, snadný prodej nebo vidina rychlého zbohatnutí prostřednictvím investování, neobvyklá žádost o půjčku od kohokoliv zasláná na mobilní telefon.

👉 NIKDY

- Nikomu nesdělujte hesla, PIN nebo jakékoliv bezpečnostní kódy.
- Nepouštějte cizí osoby do svého zařízení ani přes vzdálený přístup.
- Nikomu neposílejte peníze, dokud si pravdivost jeho žádosti neověříte u toho, kdo po Vás peníze chce.

Než cokoliv uděláte, nezapomeňte se nadechnout, vydechnout, napočítat do deseti a případně se s někým osobně porad'te.

KYBER RÁDCE

jihočeské policie

👉 DOBRÁ RADA

- Pro platby na internetu si ke svému stávajícímu bankovnímu účtu zřídte jiný, s jinou platební kartou, na kterém budete mít minimální finanční částku určenou na online nákupy. Tento účet nastavte tak, aby si na něm případný podvodník nemohl sjednat úvěr. Poradte se ve své bance.
- Nepřihlašujte se do internetového bankovníctví a neplaťte, pokud jste připojeni přes veřejnou Wi-Fi síť.

👉 CO DĚLAT, KDYŽ NALÉTNETE

- **OKAMŽITĚ** kontaktujte banku - zablokujte platební kartu nebo reklamujte zadanou platbu.
- **POTÉ** nahlase podvod Policii ČR (158)
- Čím dříve to uděláte, tím větší je šance na záchranu Vašich peněz.

**POZVĚTE SI NÁS NA
PŘEDNÁŠKU**

974 221 207

602 422 301

krpc.tisk@policie.gov.cz



více info

