

Workshop 1: Prevence kyberpodvodů ve financích

#nePINdej a sdílej



**Pavel
Šašek**

**Payment Security and
Fraud Prevention**

Komerční banka

Co se na této interaktivní přednášce dozvíte?

01

Seznámíte se s 5 typy kyberpodvodů, se kterými se žáci setkávají.

02

Naučíte se je rozpoznat v praxi a poznat jejich typické znaky.

03

Zjistíte, jak na podvody správně reagovat a jak se před nimi chránit.

04

Získáte tipy, jak zařadit téma kyberbezpečnosti do výuky a kde najít vhodné materiály.

Co je to kyberbezpečnost?

- **Kybernetická bezpečnost (kyberbezpečnost)** představuje soubor opatření, dovedností a znalostí, které nám umožňují být na internetu v bezpečí a včas odhalit útoky online podvodníků.
- V širším kontextu jde o schopnost nenechat se nachytat ve světě online financí a bezpečně se rozhodovat v digitálním prostředí.

V roce 2025 kyberzločinci způsobili: Škody přesahující 2,1 miliardy Kč. Klienti bank loni čelili téměř 91 tisícům útoků. Oproti předchozímu roku je to nárůst o víc než 700 milionů Kč.



Proč se kyberbezpečnosti věnovat ve výuce?

Nárůst online podvodů, kterému čelí nejen dospělí, ale **stále častěji i děti** a **studenti**.

Podvody zaměřené na studenty středních škol: tzv. „**lajkovací podvody**“, **deepfake videa** užívající tváře známých influencerů

Z dat ČBA dlouhodobě vyplývá nejnižší informovanost seniorů a dětí ve věku 12–17 let.

Výuka pomáhá žákům poznat **konkrétní nástroje** a **techniky** podvodníků.

Výuka vede k rozvoji **digitální kompetence** a **bezpečnému** a **kritickému** užívání digitálních technologií.

Časté podoby kyberpodvodů

#nePINdej a sdílej

Čemu se budeme věnovat?

Obsah

1. Podvodné wi-fi sítě
2. Podvodné zprávy a e-maily
3. Online nakupování: falešné e-shopy a bazarové podvody
4. Rychlé peníze a lajkovací podvody
5. Podvodná volání a deepfake videa

Proč?

Jedná se o výběr kyberpodvodů, které často cílí na děti ve věku 12 – 17 let a se kterými se tak děti setkávají nejčastěji.

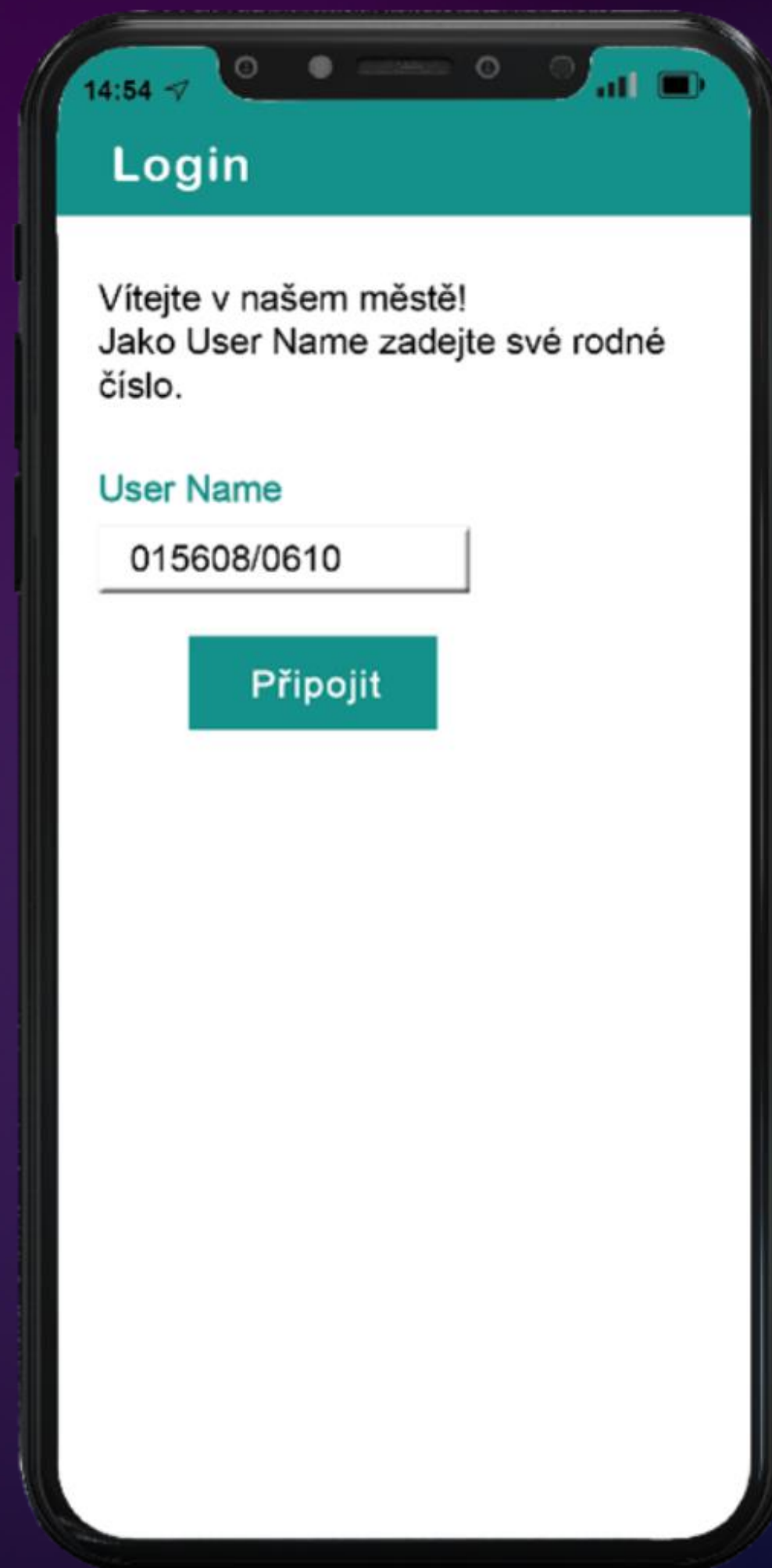
Podvodné Wi-Fi sítě

1. Útočníci vytvářejí v kavárnách, na letištích nebo v obchodních centrech vlastní WiFi sítě, které se jmenují podobně jako ty oficiální (např. „Free_Mall_WiFi“).
2. Jakmile se připojíte, mohou „odposlouchávat“ vše, co na internetu děláte.
3. Sází na pohodlnost a potřebu být neustále online.

NEJČASTĚJŠÍ CHYBY

Automatické připojování k jakékoli volné síti bez hesla a následné přihlašování do e-mailu, sociálních sítí nebo bankovníctví na této nezabezpečené síti.



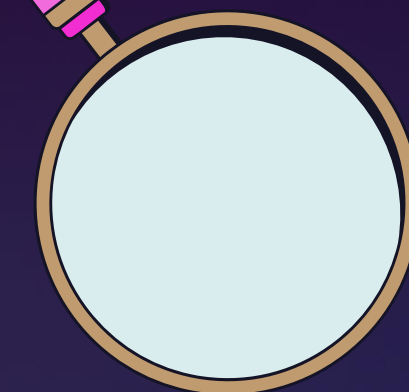


Kdy zbystřit?

Útočníci vytvářejí sítě se jmény velmi podobnými těm oficiálním (např. „Free_Mall_WiFi“) na letištích, v kavárnách či obchodních centrech.

Absence hesla a podezřelé vstupy: Při přihlášení mohou vyžadovat nestandardní údaje, jako je například rodné číslo.

Co dělat, pokud jste naletěli?



- Ihned se odpojte
- Zapněte si mobilní data
- Neprodleně si změňte hesla ke všem službám, které jste použili.

**POKUD ŠLO O FINANCE,
KONTAKTUJTE SVOU BANKU.**

KVÍZOVÁ OTÁZKA

Co je nejbezpečnějším pravidlem při používání veřejné Wi-Fi sítě v obchodním centru?

- a) Připojit se jen k té, která má nejsilnější signál.
- b) Nikdy se přes veřejnou Wi-Fi nepřihlašovat k bankovníctví ani do e-mailu.
- c) Mít v telefonu nastaveno automatické připojování ke všem dostupným sítím.

Podvodné zprávy a emaily

- Podvodníci rozesílají zprávy, které se tváří jako oficiální upozornění od banky, pošty nebo třeba státního úřadu. Často však obsahují odkazy na falešné webové stránky, které slouží k ukradení hesel nebo údajů o kartě.



Klíčovým nástrojem útočníka je práce s emocemi, zejména **vyvolávání strachu** (např. „Váš účet byl zablokován“) nebo pocitu **časové tísně**.

NEJČASTĚJŠÍ CHYBY

Klikání na odkazy přímo v doručených SMS (smishing) nebo e-mailech (phishing) a následné vyplňování citlivých údajů na neprověřených stránkách.



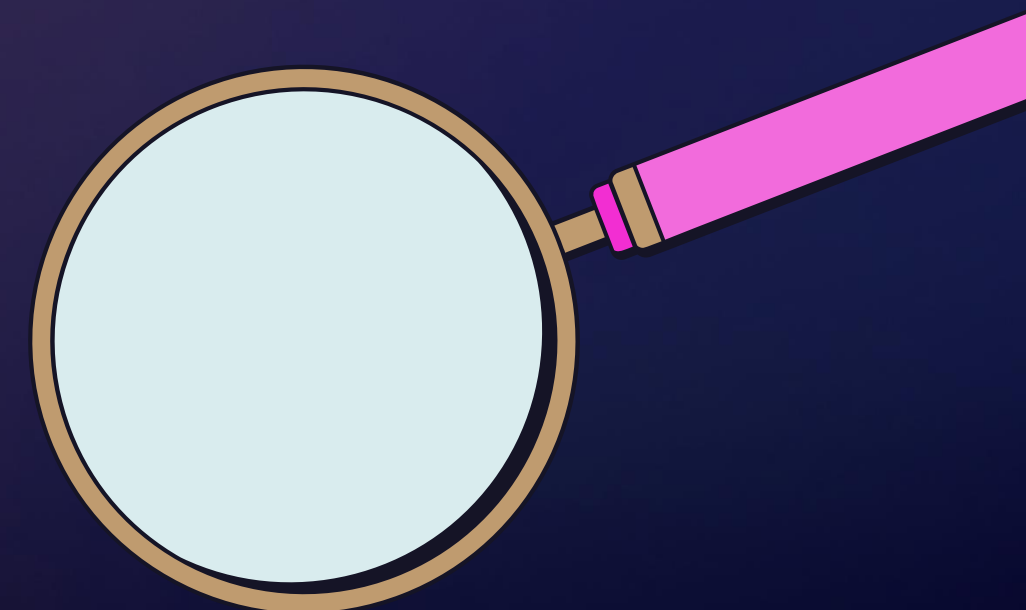
Kdy zbystřit?

Varovným signálem jsou netypické e-mailové adresy odesílatele a přímé vyžadování osobních nebo přístupových údajů.

Podvodníci se maskují za banky, poštu nebo státní úřady, ale zprávy často obsahují odkazy na falešné webové stránky.

Co dělat, pokud jste naletěli?

Pokud jste na podezřelý odkaz klikli a zadali jakékoli údaje, okamžitě kontaktujte svou banku a neprodleně si změňte přístupová hesla k zasaženým službám.



KVÍZOVÁ OTÁZKA

Jaký je nejčastější varovný signál, že je doručená zpráva podvodná?

- a) Zpráva obsahuje vaše celé jméno a správné číslo účtu.
- b) Zpráva vás nutí k okamžité akci pod pohrůžkou zablokování účtu nebo pokuty.
- c) E-mail přišel z oficiální adresy vaší školy.

Online nakupování: falešné e-shopy, bazarové podvody

- Útočníci vytvářejí falešné e-shopy s nereálně levným zbožím nebo se vydávají za kupující na bazarech (např. Vinted, Bazoš). Často pošlou odkaz na falešnou stránku dopravce (např. Zásilkovna, PPL), kde máte pod záminkou „přijetí platby“ vyplnit údaje ke své platební kartě.



Podvodníci využívají kombinaci euforie z výhodného nákupu a časové tísně. Podvodník se často chová velmi ochotně a tvrdí, že „už vše zařídil a zaplatil“, čímž nutí k neuváženému kliknutí na odkaz.

NEJČASTĚJŠÍ CHYBY

Důvěra v neznámé prodejce bez recenzí a především zadávání údajů z karty do odkazů, které vám někdo pošle v chatu, místo používání oficiálních platebních metod v rámci dané aplikace.



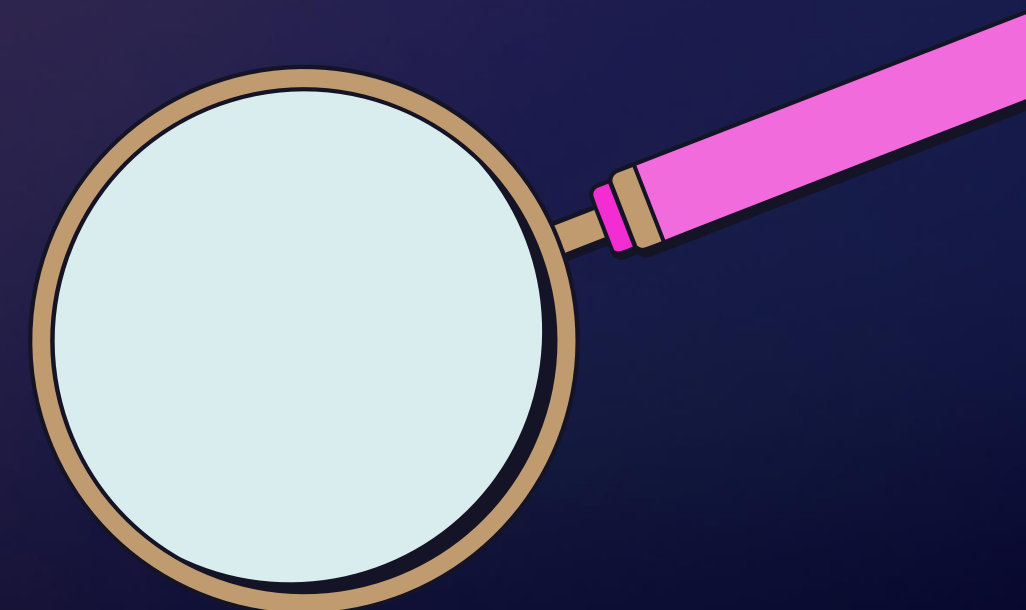
Kdy zbystřit?

Falešné e-shopy lákají na extrémně nízké ceny, které neodpovídají tržní realitě.

Kupující (útočník) se chová velmi ochotně, tvrdí, že už vše zařídil a zaplatil, a vyvíjí na vás časový nátlak, abyste obchod dokončili.

Co dělat, pokud jste naletěli?

Pokud jste zadali údaje ke kartě na podezřelém webu, okamžitě kartu zablokujte ve svém bankovníctví nebo kontaktujte banku. Podvod nahlase na Policii ČR.



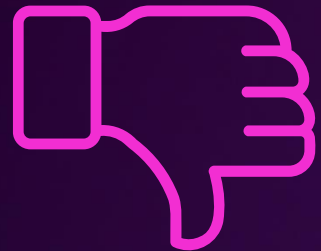
KVÍZOVÁ OTÁZKA

Co by vás mělo nejvíce varovat při prodeji věci na on-line bazaru?

- a) Kupující chce poslat zboží přes oficiální službu (např. Balíkovna).
- b) Kupující vám pošle odkaz, kam máte vyplnit údaje o své kartě, aby vám mohl „poslat peníze“.
- c) Kupující se ptá na stav prodávaného zboží a chce další fotky.

Rychlé peníze a lajkovací podvody

- Podvodníci oslovují mladé lidi s nabídkou snadného a rychlého přivýdělku z domova. Úkolem je pouze „lajkovat“ videa nebo příspěvky na sociálních sítích.

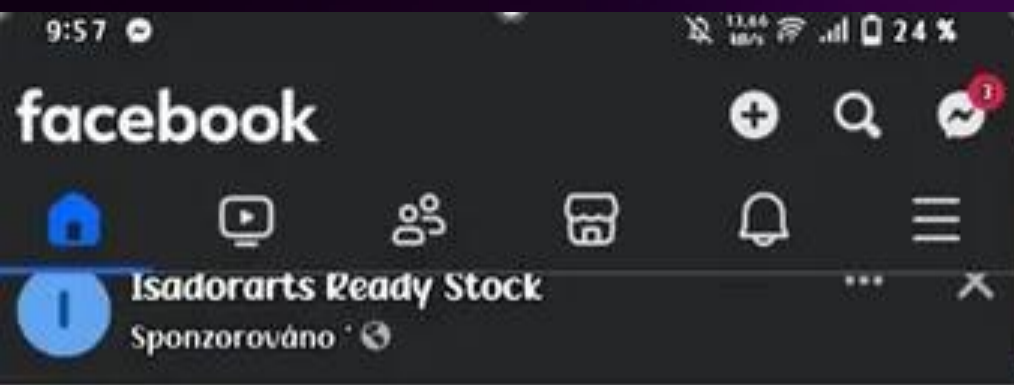


Pracuje s vidinou rychlých peněz a buduje falešnou důvěru. Často na začátku skutečně vyplatí malou odměnu, aby oběť přesvědčil k následnému „vkladu“ vlastních peněz pro získání mnohem vyšších zisků.

NEJČASTĚJŠÍ CHYBY

Zasílání vlastních úspor jako „vstupních poplatků“ nebo sdílení přístupových údajů k bankovnímu účtu pod vidinou výplaty odměny.





PROVÁDÍME NÁBOR

práce na částečný úvazek
Sledujte videa pomocí Tiktok

Podívejte se na 1 video = 25 Kč
Podívejte se na 5 videí = 150 Kč
Podívejte se na 10 videí = 300 Kč

Sledujte videa a nechte si zaplatit
Denní mzda je vyplácena včas



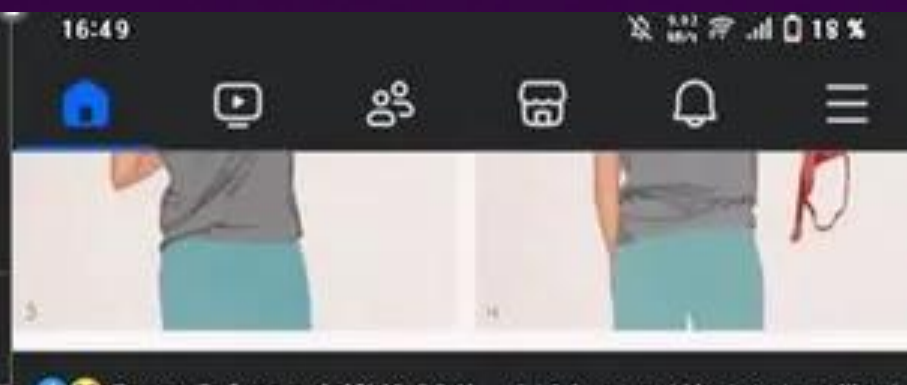
ecommerce-platforms.com
12 nejlepších platforem elektronického obchodu pro rok 2024 - doporučení od...

[Další informace](#)

😊 Vy a další (1) 1 komentář

😂 Haha [Komentář](#) [Sdílet](#)

Tetiana Tanla
Stories · 1 hod · გელა გნოლიძე & ლამის შოუ... · [...](#)



[To se mi líbí](#) [Komentář](#) [Odeslat](#) [Sdílet](#)

Financial Advisor-3
Sponzorováno

Místo: Videoti
Role: Videokomentář.
Pozice: Asistent video služeb.... [Zobrazit víc](#)

Přijímáme zaměstnance

Práce na částečný úvazek pomocí Tiktok
Podívejte se na video

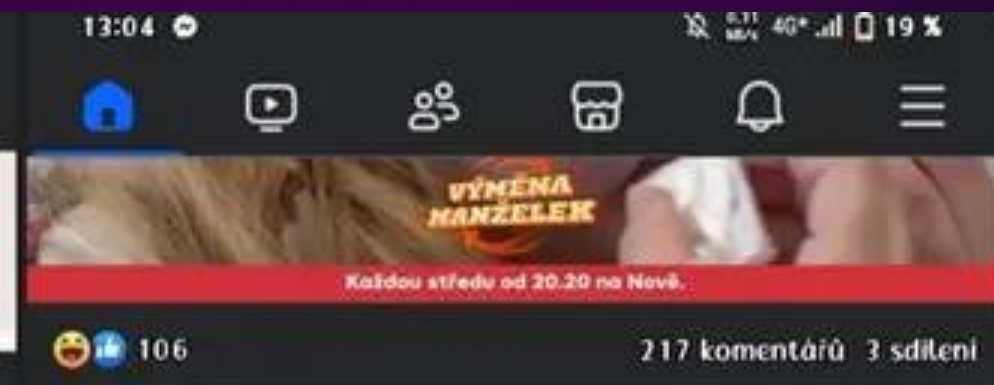
Plat	Podívejte se na 1 videí = 25Kč
Denně	Podívejte se na 10 videí = 250Kč
	Podívejte se na 20 videí = 500 Kč

Sledujte videa a získejte výplatu Mzda se vyplácí denně

FORMULÁŘ NA FACEBOOKU [Zaregistrovat se](#)

😊 Lussy Liu

👍 [Komentář](#)



[To se mi líbí](#) [Komentář](#) [Odeslat](#) [Sdílet](#)

周奕辰
Sponzorováno

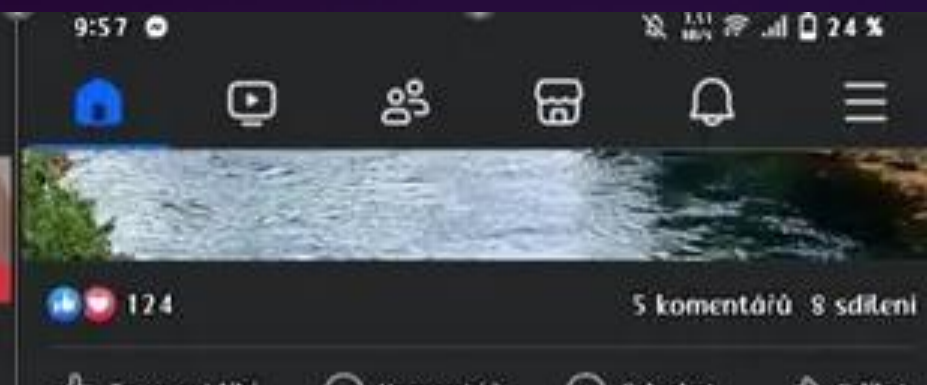
Naším posláním je být společností na Zemi, která se nejvíce zaměřuje na zákazníky. Dělat maximum pro naše zákazníky je místo, kde čerpáme ene... [Zobrazit víc](#)

Vyděláváme peníze sledováním videí,

- 1 Získejte odměny za provoz.
- 2 Mzda: 200-600 Kč/hod
- 3 Bonusy se rozdávají každý den, pokud chcete vydělávat více,
- 4 Přidáním získáte 200 Kč

FORMULÁŘ NA FACEBOOKU [Zaregistrovat se](#)

👍 2 3 komentáře



[To se mi líbí](#) [Komentář](#) [Odeslat](#) [Sdílet](#)

School прилуцька
Sponzorováno

Místo: Videoti
Role: Videokomentář.
Pozice: Asistent video služeb.... [Zobrazit víc](#)

PROVÁDÍME NÁBOR

zaměstnanci na částečný úvazek
Získejte zaplacen za sledování videí Tik Tok

Podívejte se na 1 video = 25 Kč
Podívejte se na 5 videí = 150 Kč
Podívejte se na 10 videí = 300 Kč

Nejsou vyžadovány žádné zkušenosti
Vyplácejte denní mzdu včas

potřeba 35 lidí

[Kontaktujte nás a dozvíte se více](#)

bazos.cz
Inzerce, inzeráty, bazar - Bazos.cz [Další informace](#)

Inzerce zdarma, internetový bazar - ku... 1 komentář

[To se mi líbí](#) [Komentář](#) [Sdílet](#)

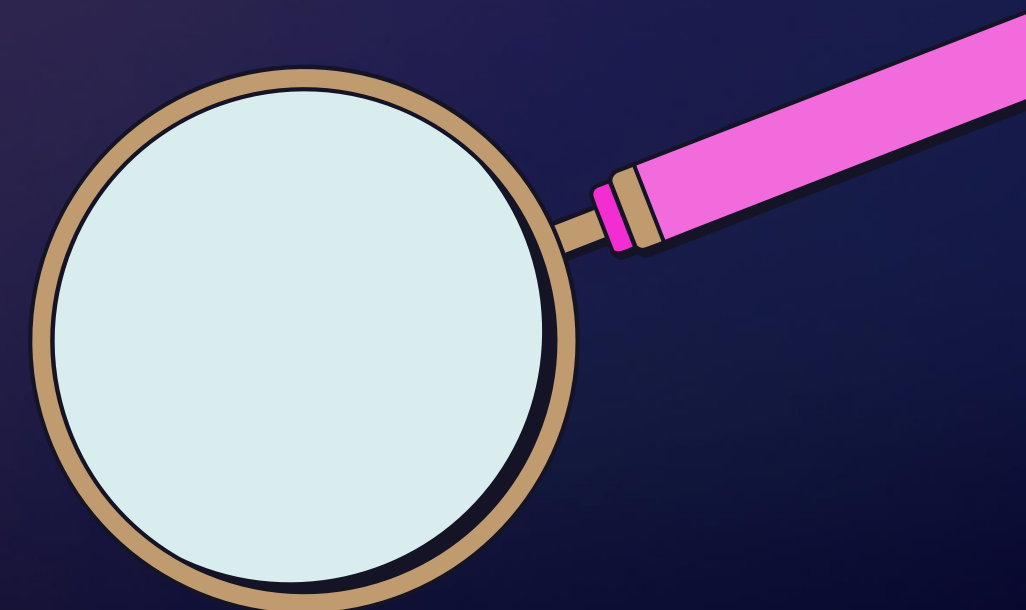
Kdy zbystřit?

Inzerát slibuje příliš snadný a rychlý výdělek.

Jakmile po vás někdo začne chtít peníze na vstupní poplatky k potenciální online brigádě, okamžitě ukončete komunikaci.

Co dělat, pokud jste naletěli?

Pokud jste již sdíleli údaje ke kartě, ihned kontaktujte svou banku.



KVÍZOVÁ OTÁZKA

Jaký je hlavní cíl „lajkovacích podvodů“?

- a) Zvýšit popularitu neznámých influencerů na internetu.
- b) Vylákat z oběti peníze pod záminkou investice do „výnosnějšího“ balíčku úkolů.
- c) Získat zdarma marketingovou pomoc pro nové e-shopy.

Podvodná volání & deepfake videa

- = Podvodníci využívají tzv. vishing (podvodná volání) a stále častěji i deepfake videa, ve kterých AI napodobuje obličeje známých influencerů na sociálních sítích. Tito falešní influenceréři pak lákají na „zaručené“ investice nebo soutěže.



Hlavním nástrojem je práce s emocemi, zejména vyvolávání strachu a extrémní časové tísně. Útočník se může vydávat za bankéře nebo policistu a tvrdit, že vaše peníze jsou v nebezpečí a musíte je okamžitě převést jinde.

NEJČASTĚJŠÍ CHYBY

Přílišná důvěra v to, co vidí a slyší ve videu na sociálních sítích, a strach ukončit hovor, který se zdá být oficiální.



Ukázka reálných DEEP FAKE videí

Influencer
Kovy

Guvernér
ČNB



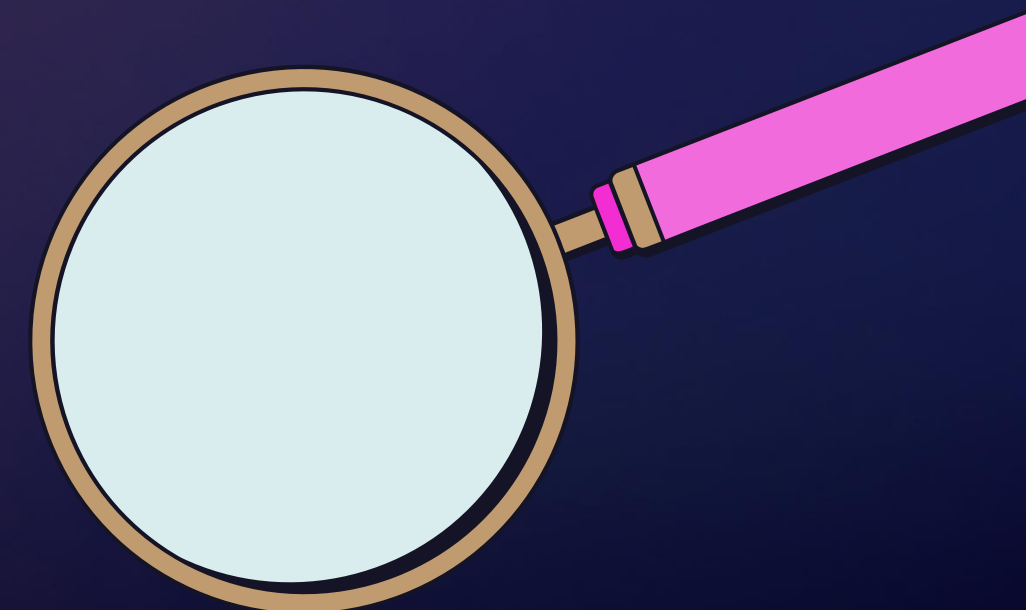
Kdy zbystřit?

Útočník tvrdí, že vaše peníze jsou v nebezpečí a musíte je okamžitě převést na „bezpečný účet“.

Pokud známá tvář propaguje “zaručenou investici s vysokým výnosem”.

Co dělat, pokud jste naletěli?

Pokud máte pochybnosti, okamžitě zavěste. Informaci si ověřte zavoláním na oficiální linku instituce. Pokud jste již sdíleli citlivé údaje, ihned kontaktujte svou banku.



KVÍZOVÁ OTÁZKA

Jaký je doložený rekord v délce jednoho podvodného hovoru, během kterého útočník udržel oběť pod neustálým tlakem, než ji připravil o peníze?

- a) 1:30 hodiny – pak to oběť obvykle prokoukne
- b) 2:45 hodiny – než se vybije baterie telefonu
- c) 5 hodin – podvodníci dokážou oběť manipulovat i takto dlouho

Kyberbezpečnost ve výuce

#nePINdej a sdílej

Úvodní tipy



PRÁCE S KONKRÉTNÍMI PRVKY:

učte žáky poznat hlavní nástroje
kyberpodvodů
– časový nátlak, podezřelé
e-mailové adresy, vyžadování
osobních údajů atd.



NESTRAŠIT

informovat a učit, jak
technologie a média
využívat k užitku,
neděsit před riziky.



PRŮŘEZOVÉ TÉMA

Ize zařadit do českého
jazyka, občanské
výchovy, informatiky.

Úvodní tipy



AUTENTICKÉ MATERIÁLY

Vycházejte z reálných e-mailů, SMS a screenshotů, i ze svých. Autenticita zvyšuje pozornost.



OBRÁCENÉ ROLE

= žák v roli učitele. Nechte žáky být experty, zeptejte se jich „Přišla mi tahle SMS, co mám dělat?“, dejte prostor k diskuzi.



BADATELSKÝ PŘÍSTUP

Nechte žáky chyby v podvodech najít samostatně nebo ve skupinových pracích. Vhodné je objevování, práce s příběhy, diskuze.

*** |
KYBERTEST

Desatero bezpečnosti Typy podvodů O projektu Partneri [Spustit test →](#)

#nePINdej!

Bud'te na internetu v bezpečí

Odhalíte včas, že na vás útočí online podvodníci?
Vyzkoušejte si náš nový **interaktivní test** a zjistěte,
jak jste na tom. Vítězí ten, kdo nePINdá!

#nePINdej!

[Spustit test →](#) [O projektu](#)

E-šmejdi chtějí
okrást i tebe!
#nePINdej!

www.kybertest.cz

CyberGame 2025

- Celonárodní on-line soutěž zaměřená na znalosti v oblasti kyberbezpečnosti
- **2. stupneň ZŠ + víceletých gymnázií (13–15 let) a SŠ (15–17 let)**
- Dvě kola: Třídní – Z každé třídy postupují dva nejúspěšnější.
Finálové – Souboj nejlepších postupujících.
- Tři nejúspěšnější dvojice získají pro své třídy finanční odměnu.
- Termín: podzim/zima 2026
- Účast zdarma

www.cybergame.cz

RedFlags

- Projekt aktuálně tvořený ve spolupráci s Nekrachni a Mastercard
- Součástí bude swipe hra a edukativní prvky v rámci aplikace Nekrachni
- Zaměřeno na mladé
- Bude spuštěno v dubnu 2026

www.redflags.cz

Plán výukové lekce

- VLOŽÍME QR KÓD A WWW NA ČBA DO SEKCE VZDĚLÁVÁNÍ

Děkuji za pozornost...

**...a nezapomeňte se mít před kyberšmejdý
na pozoru!**