Oslavte s námi Den bezpečnějšího internetu

7. 2. 2023

Den bezpečnějšího internetu 2023

Společně za lepší internet

Safer Internet Centrum | Česká republika

CZ.NIC JSNS.CZ DĚTSKÉ KRIZOVÉ CENTRUM linka bezpečí

European Commission

INHOPE insafe

O Dni bezpečnějšího internetu

Den bezpečnějšího internetu se připomíná ve více než 180 zemích po celém světě, a to vždy druhé únorové úterý. Letos tento den připadá na 7. února a slavíme ho již po dvacáté. Koordinátorem tohoto dne pro Českou republiku je národní Safer Internet Centrum, které spravuje sdružení CZ.NIC.

Historie

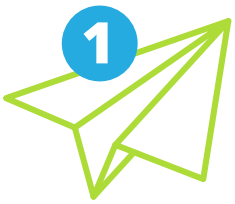
V průběhu let se Den bezpečnějšího internetu stal významnou událostí v online kalendáři bezpečnosti. Akce začala původně jako iniciativa projektu EU SafeBorders v roce 2004, poté ho převzala síť Insafe jako jednu ze svých prvních akcí v roce 2005. Původní akce se konala na území Evropské unie, postupem času se Den bezpečnějšího internetu začal slavit po celém světě.

Kdo se může zapojit?

Zapojit se do tohoto dne může úplně každý. Pod heslem „Společně pro lepší internet“ vyzýváme všechny, aby se přidali a připomenuli všechny aktivity,

které mohou pomoci udělat internet lepším a bezpečnějším místem. Akce není určena jen organizacím, které se zabývají bezpečností, prevencí, vzděláváním a intervencí na internetu, ale je vítaná účast široké veřejnosti včetně dětí, studentů a rodičů samotných nebo státních a vzdělávacích institucí.

Sdílejte a označujte



Dejte nám vědět, pokud jste se rozhodli do Dne bezpečnějšího internetu zapojit. Nezapomeňte své příspěvky na internetu a sociálních sítích označovat oficiálními hashtagy **#SaferInternetDay** a **#SID2023**, snáze tak vyhledáte i aktivity ostatních.

Oficiální odkazy pořadatelů Dne bezpečnějšího internetu

Safer Internet Centrum Česká republika (CZ)
WWW Safer Internet Day (ENG)
Facebook Safer Internet Day (ENG)
Twitter (ENG)

Zde si můžete stáhnout oficiální grafiku (CZ)

Jednotlivé tipy v příručce sestavilo

Safer Internet Centrum
E-bezpečí – projekt Pedagogické fakulty Univerzity Palackého v Olomouci
Člověk v tísni – Jeden svět na školách
Policie České republiky

Jak se zapojit?

V oblasti bezpečného chování na internetu vzniká v České republice řada preventivních programů, osvětových materiálů včetně těch audiovizuálních, které jsou na vysoké úrovni. Na následujících stránkách naleznete vybrané aktivity a tipy pro jednotlivé věkové skupiny, díky kterým se můžete zapojit do Dne bezpečnějšího internetu.

Pro nejmenší

První krůčky v kyberprostoru můžete s dětmi probírat například s knihou ON-LINE ZOO, která seznamuje nejmenší čtenáře se základy bezpečného chování na internetu. S knihou navštívíte zoologickou zahradu, kde všechna zvířátka používají internet. Projděte si jednotlivé příběhy s dětmi a bavte se s nimi o nich.

Pro knihu vznikla metodika, která je určena především pedagogům na nižším stupni ZŠ, ale mohou v ní najít inspiraci i rodiče. Každá kapitola koresponduje s jednotlivými příběhy v knize, které se zabývají nomofobií, kyberšikanou, kybergroomingem, on-line nákupy a sextingem. Veškeré pojmy jsou zde podrobně vysvětleny a váží se k nim doporučené skupinové aktivity a pracovní listy. Aktivity poslouží dětem k zamyšlení a k lepšímu zažití problému. Pracovní listy zase pomohou těm nejmenším, aby se na chvíli odreagovaly u jiné aktivity, jako je vymalování obrázku, stříhání či hledání rozdílů.

Knihu ONLINE ZOO můžete **zdarma stáhnout** na stránkách Edice CZ.NIC. K dispozici je také **audioverze** nebo **básničky**.

Ke stažení:

metodika

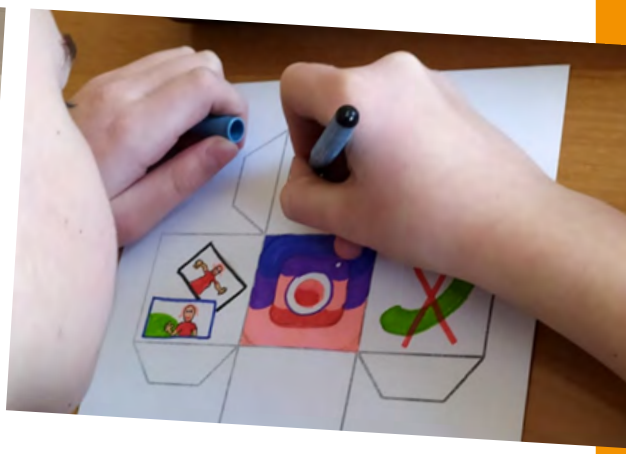
pracovní listy

Základní škola, Nový Bydžov, F. Palackého, kterou navštěvují žáci se speciálními vzdělávacími potřebami

A protože pohádek není nikdy dost, můžete si přečíst nebo poslechnout se svými dětmi i **kyberpohádky** od **Centra kybernetické bezpečnosti** nebo si přečíst povídky **Vanda a Eva v @nline světě**, které seznamují děti s riziky pohybu na internetu.

První stupeň základních škol

Děti na prvním stupni základních škol už čile používají internet a začínají experimentovat se sociálními sítěmi. Nejlepší formou, jak si s dětmi tento den připomenout je prostřednictvím kreativních úkolů. Ukazujte internet jako užitečný nástroj, nebojte se ale dětí zeptat i na jeho možná rizika. Velice vhodná je i forma divadelních představení nebo situačních scének.



Kreativní práce
žáků ZŠ Dyjákovice

S výtvarnými pracemi se pochlubte v prostorách školy nebo na veřejných místech. Tam můžete i umístit různé letáky, plakáty nebo nástěnku bezpečného internetu. Vytisknout se dá i **komiks** od Dětského krizového centra.

Informace o bezpečném
využívání internetu, odkazy
na linky pomoci
vyvěste na frekventované
místo

Online kvíz a hra

Žáci prvního stupně základních škol si mohou své znalosti ověřit formou zábavného **online kvízu** nebo si také mohou vyzkoušet online hru **Internet Highway** od **E-Bezpečí**, která je zábavným způsobem seznámí s problematikou ochrany osobních údajů a digitálními stopami. K dispozici jsou zatím dva levely plné zábavy a ponaučení.

Studenti ZŠ, SŠ, gymnázií

Kurzy

Osvětový video kurz **Jsem netvor na střední** je určen studentům prvního a druhého ročníku středních škol. Za devadesát minut se studenti dozví mnohé o kybernetické bezpečnosti.

Online kurzy mediálního vzdělávání

Zábavné **videokurzy** pro žáky, které se věnují pěti důležitým tématům mediální gramotnosti: dezinformace, kyberbezpečí, zpravodajství, marketing a reklama a sociální bubliny. Každým kurzem provází Janek Rubeš, kterému pomáhají teenageři Lucka s Matyášem. Kurzy jsou interaktivní, kromě chatování s průvodci a sledování krátkých videí z pořadu Mediální ring 2 obsahují vzdělávací minihry a kvízy, nabízí odměny v podobě digitálních odznaků a také certifikát o zdárném ukončení každého kurzu.

Hry pro děti (ne)jen s handicapem

Pro děti nejen s dyslexií, na druhém stupni základních škol, doporučujeme moderní vzdělávací aplikaci **Tablexia** na podporu rozvoje kognitivních schopností. Tablexii tvoří v současné době 10 her, z nichž se každá zaměřuje primárně na trénink jedné kognitivní schopnosti. V jednotlivých hrách si hráč procvičí pracovní paměť, sluchové vnímání, prostorovou

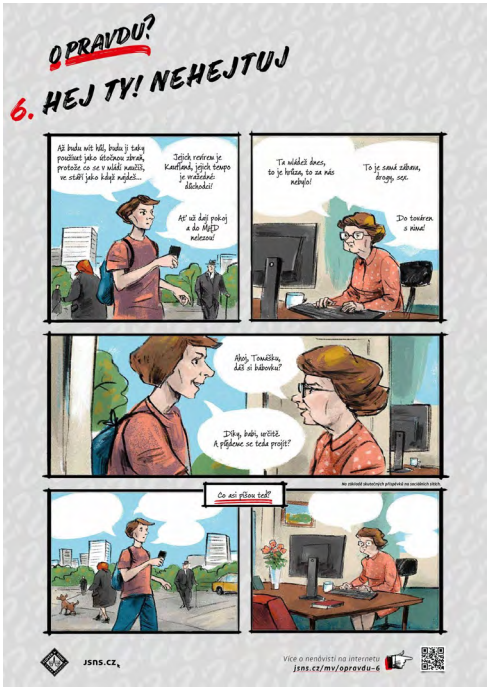
orientaci, zrakovou paměť, pozornost, zrakovou a sluchovou serialitu, zrakové rozlišování, sluchovou paměť a verbální schopnosti. Hry jsou propojené atraktivní detektivní tématikou a prostředí aplikace navozuje atmosféru 30. let minulého století. Hráč vystupuje v roli mladého detektiva, který za dohledu svého staršího kolegy trénuje schopnosti potřebné pro toto náročné povolání.

Komiks

Osvětový komiks **Digitální stopa: příběh svůďáka o internetu**, kybergroomingu, digitální stopě a identitě seznámí žáky 4. a 5. třídy ZŠ s tím, co dělat, když je někdo vydírá na internetu.

Výukové plakáty

Plakáty **O pravdu?** jsou určené především žákům druhého stupně základních škol a studentům středních škol. Hravou a interaktivní formou přibližují rozmanitá mediální témata (manipulace s obrazem, ověřování zdrojů, bezpečnost na internetu, hate speech, atd.) Doprovází je texty, které přináší základní informace k tématům jednotlivých plakátů spolu s odkazy na **výukové aktivity**. Stáhnout si je můžete **na webové stránce jsns.cz.**



Plakáty **Mediální gramotnost se vyplatí** zábavnou formou vybízí žáky vyřešit úlohy týkající se problematiky:

- konspiračních teorií a otázek, jak poznat důvěryhodné informace (**Naivátor**),

- digitální stopy, kterou zanecháváme na sociálních sítích, a možnostech jejího zneužití (**Vykecávačka**),

- přesvědčovací techniky reklamy a nakupování na internetu (**Výhodný telefon**).

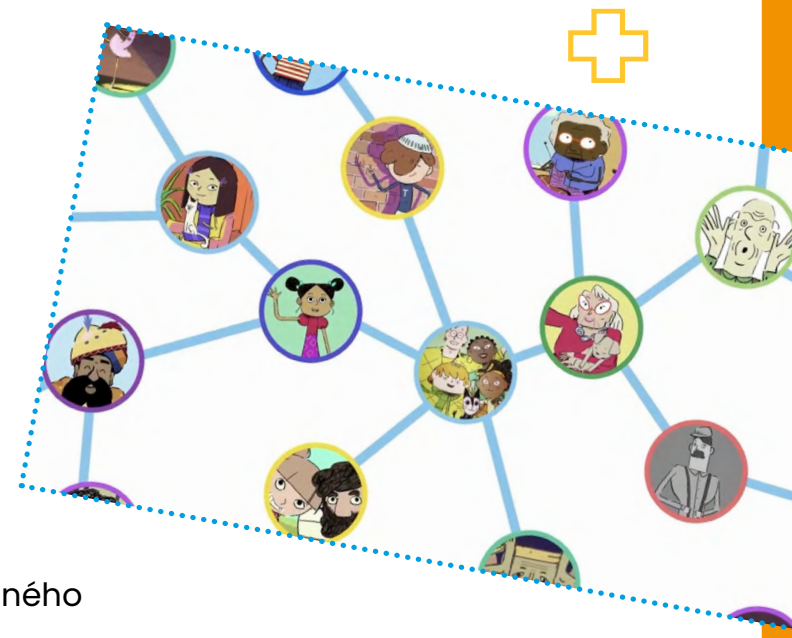
Další tipy pro učitele

V České republice průběžně vzniká celá řada výborných vzdělávacích materiálů do výuky. Představíme vám některé z nich. Pokud budete mít zájem se v této oblasti vzdělávat, pravidelně pro vás připravujeme semináře, webináře, kurzy a workshopy zaměřené na různá témata. Všechny jsou **zdarma** a není-li uvedeno jinak, **akreditované MŠMT**. Chcete se naučit nebo si připomenout, jak nejlépe používat audiovizuální materiály ve výuce? **Sledujte nabídku a přihlaste se**.

V digitálním světě

Je sada **15 audiovizuálních lekcí**, které seznamují žáky s některými aspekty fungování online světa a s pravidly bezpečného chování v něm. Sada je svým audiovizuálním stylem a obsahem určena žákům prvních až šestých tříd základních škol.

K dispozici je i online publikace **V digitálním světě**, která obsahuje:



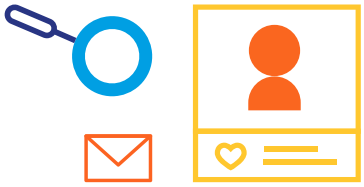
- rady a doporučení, jak s příručkou pracovat,

- návod na úvodní průzkum mezi žáky k získání přehledu o digitální a mediální gramotnosti třídy,

- prakticky využitelné audiovizuální materiály a aktivity do výuky, které vychází ze zábavného animovaného seriálu V digitálním světě,

- kvíz pro žáky: Co víte o digitálním světě?,

- infografiku k vybraným tématům mediálního vzdělávání.



Výuková videohra Digistories: Nela

Materiál, díky kterému lze ve výuce otevřít téma kyberšikany interaktivní a poutavou formou.

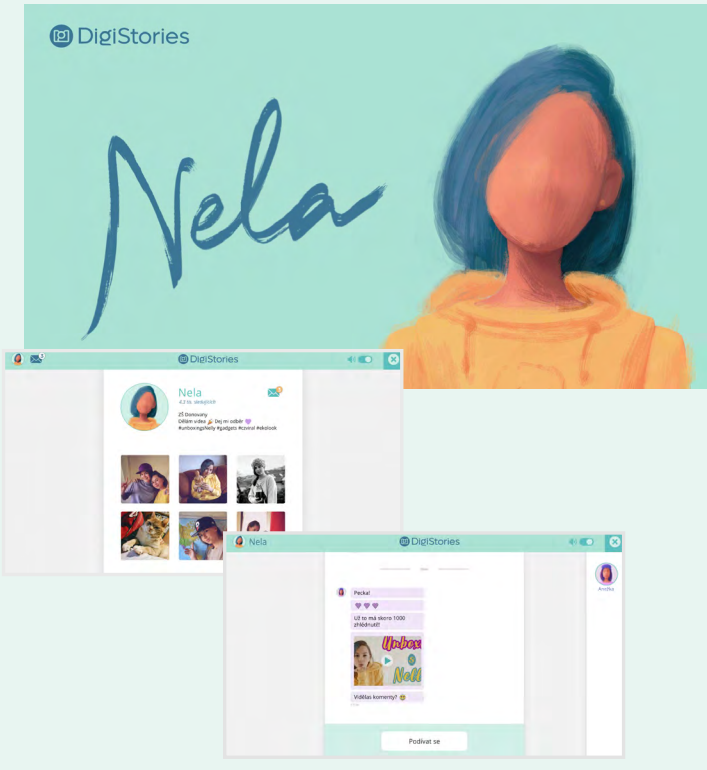
Ukazuje průběh kyberšikany realistickou formou.

Simuluje konverzaci na sociální síti.

Umožňuje pochopit podobu i následky kyberšikany prostřednictvím vlastního prožitku – hráč se ocitá v roli oběti.

Vhodná pro žáky ve věku 11 – 15 let.

Není určena jako samostatný výukový materiál (ve vyučovací hodině je potřeba pokračovat reflexí a následnou diskuzí s žáky).



Kde čerpat inspiraci

MQposilovna

E-cvičebnice MQposilovna obsahuje 10 tréninkových lekcí. Ty jsou vhodné zejména pro žáky 8. a 9. tříd ZŠ a SŠ. Každá lekce začíná krátkým videem, na které navazuje několik úloh. E-cvičebnice je připravena tak, aby s ní žáci mohli pracovat zcela samostatně na počítači, tabletu či mobilu.

Safer Internet Centrum ČR

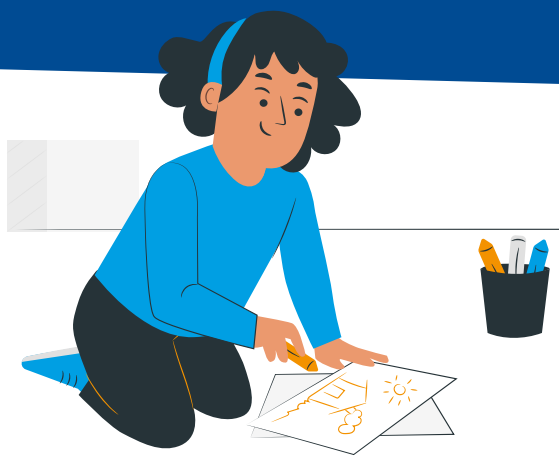
Nabízí ke stažení filmy, seriály, knihy nebo metodiky. Podívejte se **na stránky**, všechny materiály jsou zdarma pro nekomerční využití.

JSNS.cz

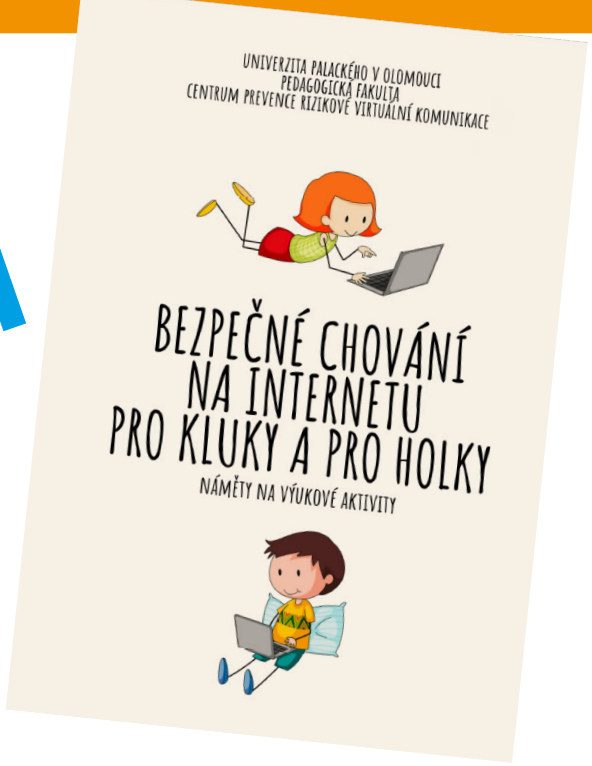
Na vzdělávacím portále jsns.cz jsou pro učitele dostupné (po registraci) audiovizuální lekce (370+), které obsahují audiovizuální materiál (filmy, videa,..), aktivity do hodin předem testované ve výuce, informační texty a doporučené materiály pro rozšíření výuky. Vyzkoušet si mimo jiné lze dvě nové lekce **S kým si píšeš?** a **Znáš celý příběh?**. Jsou postavené na krátkých spotech, které otevírají téma bezpečnosti mladých lidí v online prostoru a jejich duševní pohody.

E-Bezpečí

Projekt E-Bezpečí nabízí učitelům akreditované vzdělávací akce zaměřené jak na oblast online bezpečnosti, tak i problematiku mediální gramotnosti. Kurzy zahrnují více než 20 témat: kyberšikana, kybergrooming, sexting, nebezpečné výzvy, sociální sítě a jejich rizika, ale také např. témata dezinformace, misinformace a hoaxy, online podvody, kybernemoci, rizika netolismu apod. Kurzy jsou k dispozici jak v online, tak i offline - prezenční podobě. Učitelé mohou využívat jak **internetové stránky**, tak i naše kanály **Youtube**, **Instagram** a **Twitter**.



Publikace



V roce 2022 byla vydaná pro učitele publikace, která nabízí pedagogům (a žákům) všech typů škol návrhy na výukové aktivity v podobě ucelené knížky **Bezpečné chování na internetu pro kluky a pro holky - náměty výukových aktivit**.
Tuto publikaci je možné **stáhnout zde**.

Využívat můžete také např. tematické stránky věnované mediální výchově - **Fastcheckingu** a **Hoaxům**

Učitelům jsou k dispozici také tematická vzdělávací videa z cyklu:
Abeceda médií (oblast mediální výchovy)
Převíti na síti (oblast online podvodů)

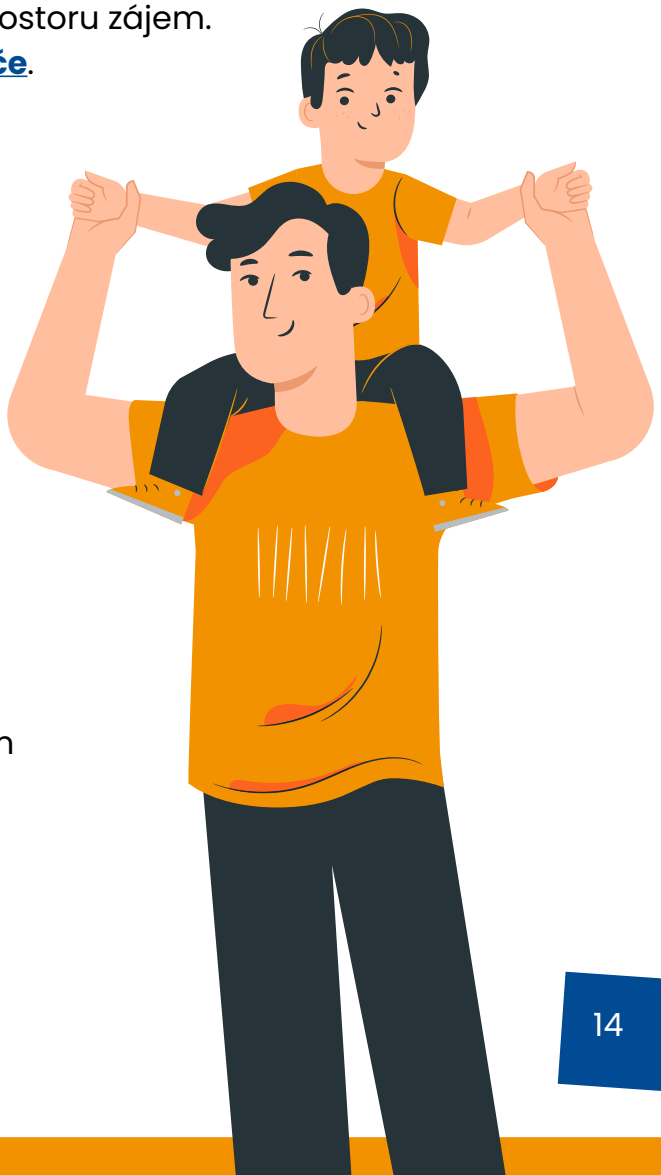
Nebojte se ozvat

- **Linka bezpečí - telefon 116 111, chat nebo e-mail**
- **Dětské krizové centrum - Linka důvěry telefon 241 484 149, on-line chat nebo e-mail**
- **STOPonline.cz - linka pro hlášení závadného obsahu na internetu.**
- **Napiš nám - poradna projektu E-bezpečí**

Rodiče

Rodiče mají klíčovou roli ve vzdělávání a podpoře dětí, aby používaly digitální technologie zodpovědně, s respektem, kriticky a kreativně. Vliv rodičů a vzdělávání má skutečně významný a dlouhodobý dopad na bezpečnost a pohodu dětí v online světě. Je mnoho způsobů, jak se zapojit do Dne bezpečnějšího internetu, ať už tím, že zajistíte otevřený dialog se svými dětmi nebo je budete vychovávat k bezpečnému a pozitivnímu používání digitálních technologií.

Být rodičem ve zrychleném online světě není jednoduché. Děti dost často bývají technologicky napřed před svými rodiči. Zkuste se kromě otázky „Jak bylo ve škole?" ptát i na to „**Jak bylo na internetu?**". Diskutujte o tom, jaké služby děti na internetu využívají a proč. Nechte si věci ukázat a projevte o aktivity dětí v online prostoru zájem. Přečtěte **desatero „kybernetického" rodiče**.



Podívejte se společně na film nebo seriál

Přemýšlíte, jak otevřít debatu s dětmi o rizicích internetu? Zkuste se spolu podívat na seriál nebo film k tomuto tématu. Důležité je, se nejen s dětmi dívat, ale následně si o tom i povídat.

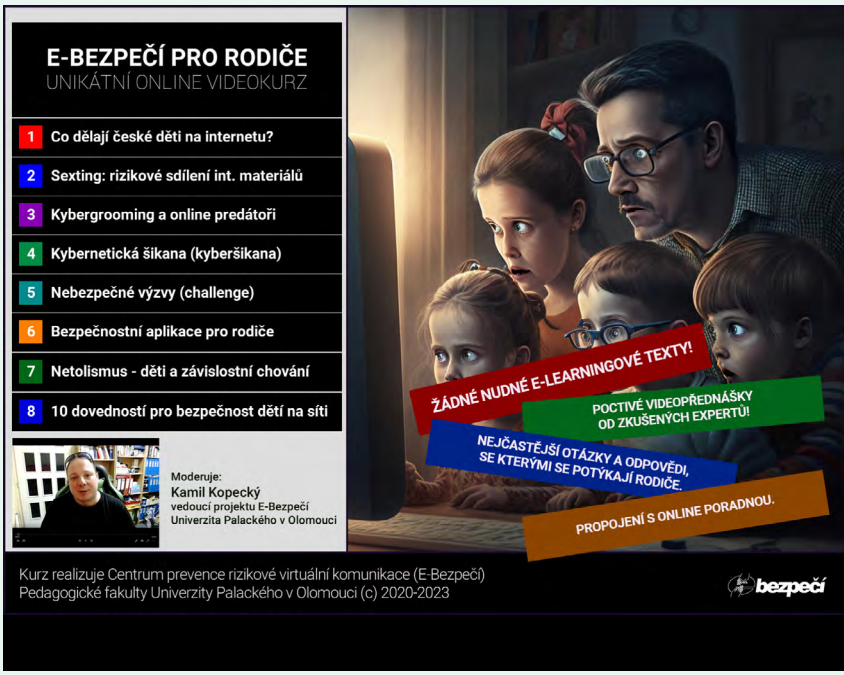
Film **Na hory** - od režiséra Braňo Holička. Příběh o tom, co dětem může způsobit obyčejné brouzdání po internetu. A rodičům změnit život. Krátký film s **metodikou**, jak s dětmi mluvit o tématech seznamování, vydírání nebo kybergroomingu. Doporučený věk 12+.

#Martyisdead - seriál o kyberšikaně, který získal mnoho ocenění, včetně mezinárodní ceny Emmy. Co vedlo dosud bezproblémového patnáctiletého Martina přezdívaného Marty, k tomu, aby vzal do ruky mobil a natáčel se v situacích, ze kterých mrazí? Podívejte se na seriál i doprovodná videa. Doporučený věk 12+.

Pokud vlastníte Netflix, podívejte se s dětmi na seriál o kyberšikaně **13 důvodů proč** (13 Reasons Why). Využít můžete také film **V síti** s metodikou pro pedagogy a rodiče, která je k dispozici na **www.vsitifilm.cz**.

Může se stát, že se jako rodiče ocitnete v situacích (krizových nebo výchovných), se kterými si nebudete vědět rady. Pak neváhejte a zavolejte **Rodičovskou linku.**

Komplexní online videokurz pro rodiče nabízí také projekt E-Bezpečí Pedagogické fakulty Univerzity Palackého v Olomouci. Kurz je tvořen tematickými videi zaměřenými na klíčová témata spojená s prevencí rizikového chování v online prostředí. Více najdete na webu **http://e-bezpeci.cz/rodice**. E-Bezpečí také nabízí celou řadu dalších vzdělávacích kurzů pro rodiče, které si můžete **objednat zde**.



Policie varuje - Pozor na podvody u her, promluvte si se svými dětmi

Dnešní počítačové hry jsou oblíbené jak u dětí tak i dospělých. Nejžádanější on-line hry vytváří početné komunity hráčů, ve kterých vznikají virtuální přátelství, najdeme zde ale také silnou rivalitu. Tyto hry jsou většinou poskytovány zdarma, umožňují však různá vylepšení prostřednictvím tzv. mikrotransakcí, tedy prodejem doplňkového obsahu (různých vylepšení herní postavy, nákupem zbraní, herní měny apod). Takto nakoupený obsah mohou hráči směňovat případně ho prodat. Tyto doplňky hráči nakupují prostřednictvím platebních karet spárovaných s herními účty, běžná jsou vylepšení v řádu stokorun. Někteří hráči jsou však ochotni utratit i částky v řádu tisíců korun.

Takto vylepšené herní profily přitahují pozornost různých útočníků a hackerů. Jejich cílem je získat přihlašovací údaje k hernímu účtu, převzít nad ním kontrolu a celý účet nebo jednotlivá vylepšení zpeněžit.

Nejčastější formy útoků - útočník se vydává za administrátora hry a kontaktuje hráče s tím, že potřebuje vyřešit nějaký technický problém s jeho herním profilem a zašle mu odkaz, přes který se má do svého účtu přihlásit.

Jak se nejlépe bránit? Naučte děti tyto pravidla

- **Základem by mělo vždy být kvalitní heslo, které rozhodně nikomu nesděluj.**
- **Pokud hraješ na cizím zařízení, neukládej si zde heslo a po hře proveď bezpečné odhlášení.**
- **Pozor na lákavé nabídky na herní předměty a různá vylepšení.**
- **Administrátor ani nikdo jiný po tobě nemůže chtít tvé přihlašovací údaje.**
- **Pokud budeš chtít ve hře nějaké placené vylepšení, vždy si to nejprve domluv s rodiči.**

[Odkaz na preventivní video od MVČR.]

Státní i soukromé organizace a jednotlivci

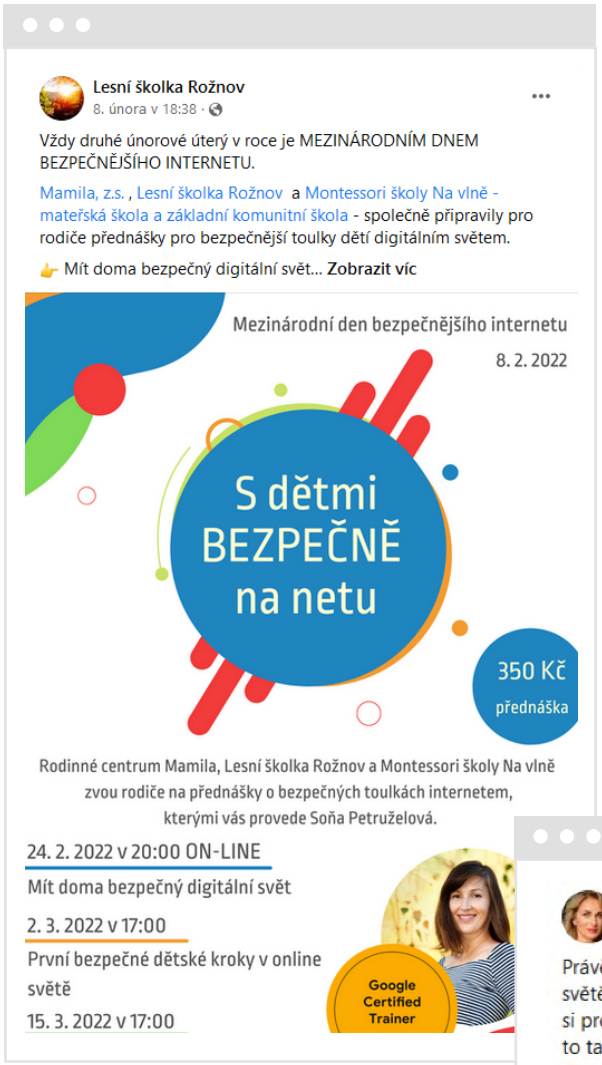
Státní, ale i soukromé organizace si mohou na tento den připravit **workshop** pro zaměstnance nebo rodiče. Tématem může být internetová bezpečnost, prevence rizikového chování dětí a mnoho dalších témat.

Připomeňte si tento den na sítích

Jestliže chcete Den bezpečnějšího internetu podpořit jako soukromá osoba, ideální jsou k tomu sociální sítě. Připomeňte si tento den a označte příspěvky oficiálními hashtagy **#SaferInternetDay** a **#SID2023**, snáze tak vyhledáte i aktivity ostatních.

Zapojit se mohou politici, úřady či městské části.

V Seznam.cz pro zaměstnance připravili v prostorách firmy infografiky


Lesní školka Rožnov
8. února v 18:38 ·
Vždy druhé únorové úterý v roce je MEZINÁRODNÍM DNEM BEZPEČNĚJŠÍHO INTERNETU.
Mamila, z.s. , Lesní školka Rožnov a Montessori školy Na vlně - mateřská škola a základní komunitní škola - společně připravily pro rodiče přednášky pro bezpečnější toulky dětí digitálním světem.
Mít doma bezpečný digitální svět... Zobrazit víc
Mezinárodní den bezpečnějšího internetu
8. 2. 2022
S dětmi BEZPEČNĚ na netu
350 Kč
přednáška
Rodinné centrum Mamila, Lesní školka Rožnov a Montessori školy Na vlně zvou rodiče na přednášky o bezpečných toulkách internetem, kterými vás provede Soňa Petruželová.
24. 2. 2022 v 20:00 ON-LINE
Mít doma bezpečný digitální svět
2. 3. 2022 v 17:00
První bezpečné dětské kroky v online světě
15. 3. 2022 v 17:00
Google Certified Trainer


Avast Software
23 h ·
O vaši online bezpečnost se staráme každý den. Užijte si tento týden Den bezpečnějšího internetu bez starostí 🙌 Jako extra bonus přinášíme tipy od našich odborníků, jak bezpečně používat smartphone. Dodržujete všechna pravidla? ➤ https://ava.st/32Vbbo9
Užijte si Den bezpečn internetu obav
Avast
Avast Software
Softwarová společnost

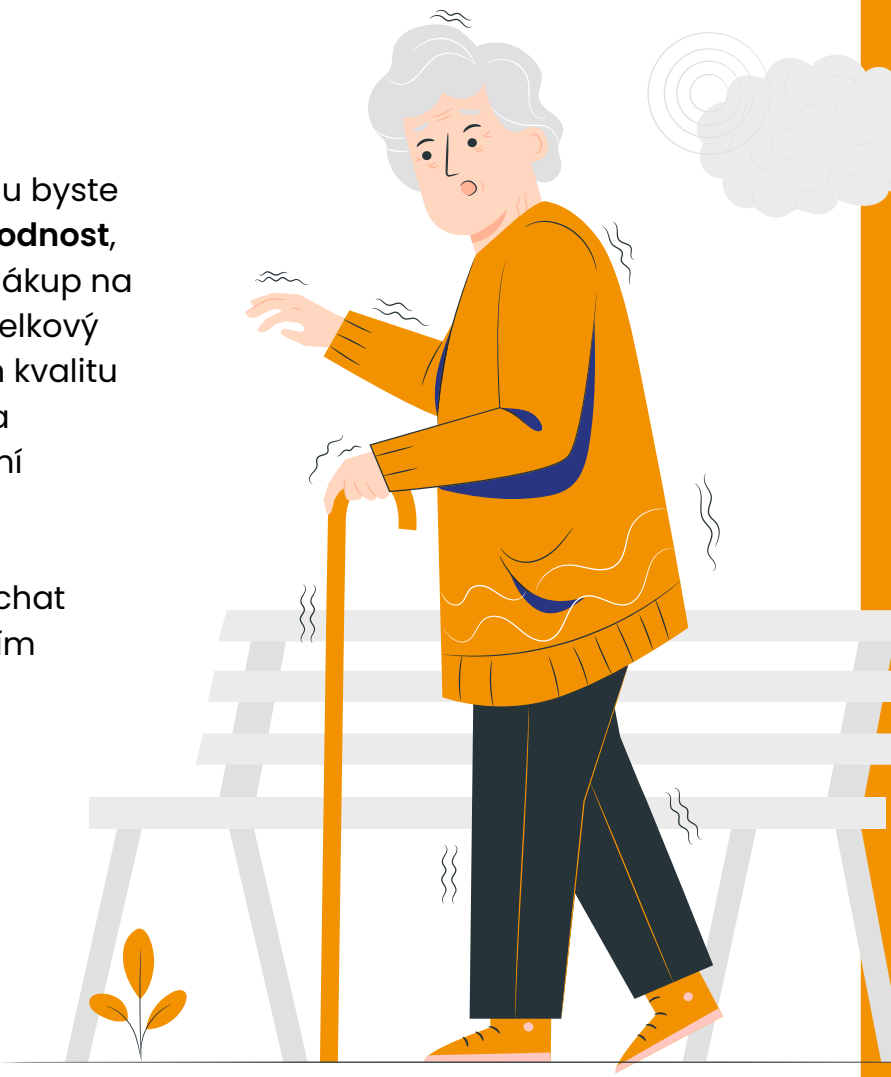
Česká pirátská strana
8. února v 15:47 ·
Dnes je Den bezpečnějšího internetu a my si přejeme co nejbezpečnější internetové prostředí pro naše děti. 🙏 Hlavně nyní, ve chvíli, kdy děti v digitálním světě tráví více času, než kdykoliv předtím. Děti přitom při pohybu v online prostoru patří mezi nejohroženější skupiny. O možných hrozbách je proto potřeba dostatečně mluvit a ohrožené skupiny vzdělávat.
👉„Oblast internetu je naprosto zásadním i klíčovým prostředím, které nás dnes všechny ovlivňuje v našich pracovních i... Zobrazit víc
CHCEME Z INTERNETU UDĚLAT BEZPEČNĚJŠÍ MÍSTO PRO NAŠE DĚTI
DEN BEZPEČNĚJŠÍHO INTERNETU
PIRÁTSKÁ STRANA


Dita Charanzová
8. února v 9:01 ·
Právě dnes je Den bezpečnějšího internetu. Spousta rodičů po celém světě stráví půl hodiny se svým dítětem a bude si s ním dívat na to, co si prohlíží na svém mobilním zařízení. A povídat si s ním o tom. Zkuste to taky, až dnes přijdete domů. Uvidíte, na co přijdete. Děkuju
#SaferInternetDay #SID2022
renew europe.

Senioři

Senioři jsou významnou součástí online prostoru a brzy se stanou největší ekonomickou skupinou na internetu. Toho mohou zneužívat podvodníci, zloději nebo různí manipulátoři.

Jestliže patříte mezi seniory na síti, záleží vám na generaci vašich rodičů a prarodičů nebo pracujete v organizacích, které se starají o seniory, přečtěte si následující témata, jež jsou vnímaná jako důležitá a ohrožující. Pokud budete mít možnost o tom diskutovat ve skupině, udělejte to.



Podvodné e-shopy

Při výběru internetového obchodu byste si nejdříve měli ověřit jeho **věrohodnost**, obzvláště pokud je to váš první nákup na tomto e-shopu. Zaměřte se na celkový vzhled webových stránek – jejich kvalitu zpracování, úroveň češtiny, a zda obsahují informace jako kontaktní údaje, obchodní a reklamační podmínky či funkcionality jako možnost sledování zásilky nebo chat s technickou podporou. V ideálním případě si název domény ověřte na stránkách **České obchodní inspekce**, která zveřejňuje **seznam rizikových e-shopů**.

Spousta lidí si prodejce ověřuje pouze z hodnocení zákazníků, na které ale nelze stoprocentně spoléhat. Nejbezpečnější

varianta je ta, kdy zvolíte e-shop, na kterém jste již v minulosti nakupovali, nebo vám ho doporučil někdo z rodiny nebo známých.

Dále doporučujeme, abyste si zboží vyhledali u **více prodejců**. Varující totiž může být i výrazně nižší cena v porovnání s jinými cenovými nabídkami. Je zde riziko, že vám zakoupené zboží nikdy nedorazí či se bude jednat o jiný produkt nebo falsifikát originálního výrobku, který je vyrobený z levnějších materiálů a často ani nemá deklarované funkce.

Pozor na platební metodu!

Obezřetní buďte hlavně při výběru platební metody, jakmile zkoušíte internetový obchod poprvé, nechte si zboží zaslat **na dobírku**. Tento způsob mimo jiné zajišťuje větší jistotu vrácení peněz v případě podvodu. U online plateb si hlídejte, aby probíhaly na zabezpečených protokolech (https, tls/ssl), na bezpečné platební bráně anebo aby bylo využito aktivní zabezpečení 3D Secure. Údaje o platební kartě nebo pro přihlášení do internetového bankovnictví si chraňte a **s nikým je nesdílejte, zejména CVV/CVC ověřovací kód z druhé strany platební karty**.

Jakmile vám balíček dorazí, nečekejte s otevřením a zkontrolujte jeho obsah. Pokud neodpovídá tomu, co jste si objednali, a prodejce nereaguje nebo nechce zboží vyměnit, kontaktujte Policii České republiky. Policisté mohou zajistit hotovost, kterou jste za balíček platili, online platbu může zadržet banka. V obou případech ale rozhoduje čas, proto **je třeba jednat co nejrychleji.**

Preventivní rady a doporučení, jak nenaletět podvodným e-shopům:

- Ověřte si věrohodnost prodejce, doménu si zkontrolujte v seznamu rizikových e-shopů na stránkách České obchodní inspekce.

- Pokud je to možné, vybírejte si ty online obchody, se kterými máte sami již zkušenost nebo vám je doporučila rodina či známí.

- Cenové nabídky si porovnejte u více prodejců, vyhněte se podezřele nízkým cenám.

- Jakmile na e-shopu nakupujete poprvé, nechte si zboží zaslat na dobírku.

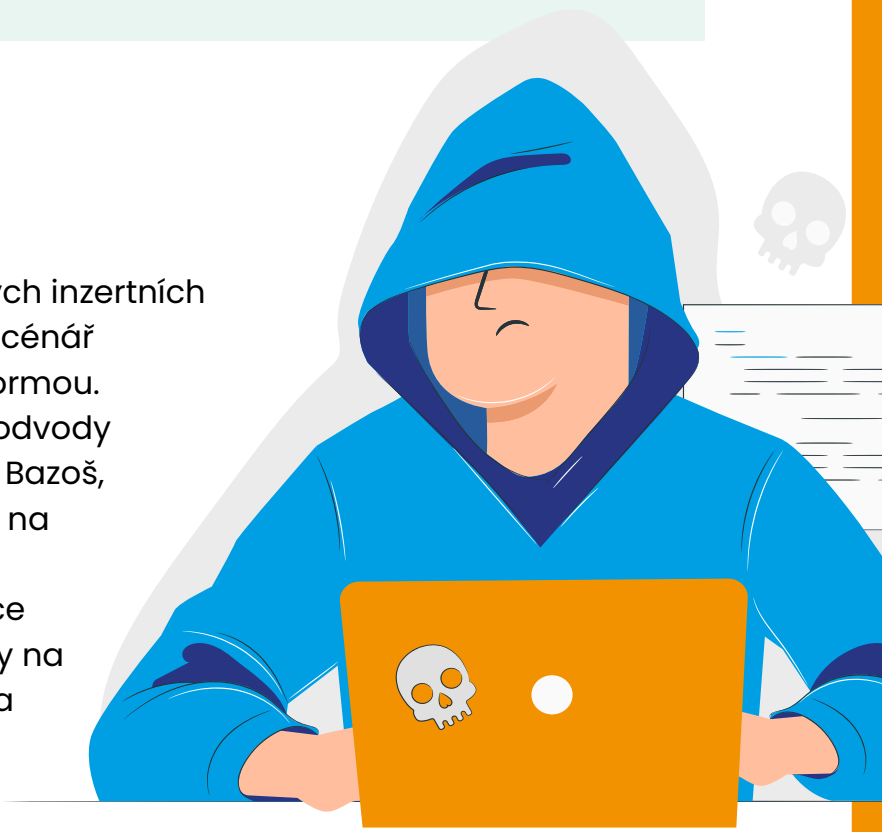
- Buďte obezřetní při online platbách, údaje k platební kartě a pro přihlášení do internetového bankovnictví si chraňte.

- Až vám balíček dorazí, co nejdříve zkontrolujte jeho obsah pro případnou reklamaci.

- Pokud se stanete obětí podvodného jednání, kontaktujte Policii České republiky na tísňové lince 158 nebo na policejní služebně.

Inzertní podvody

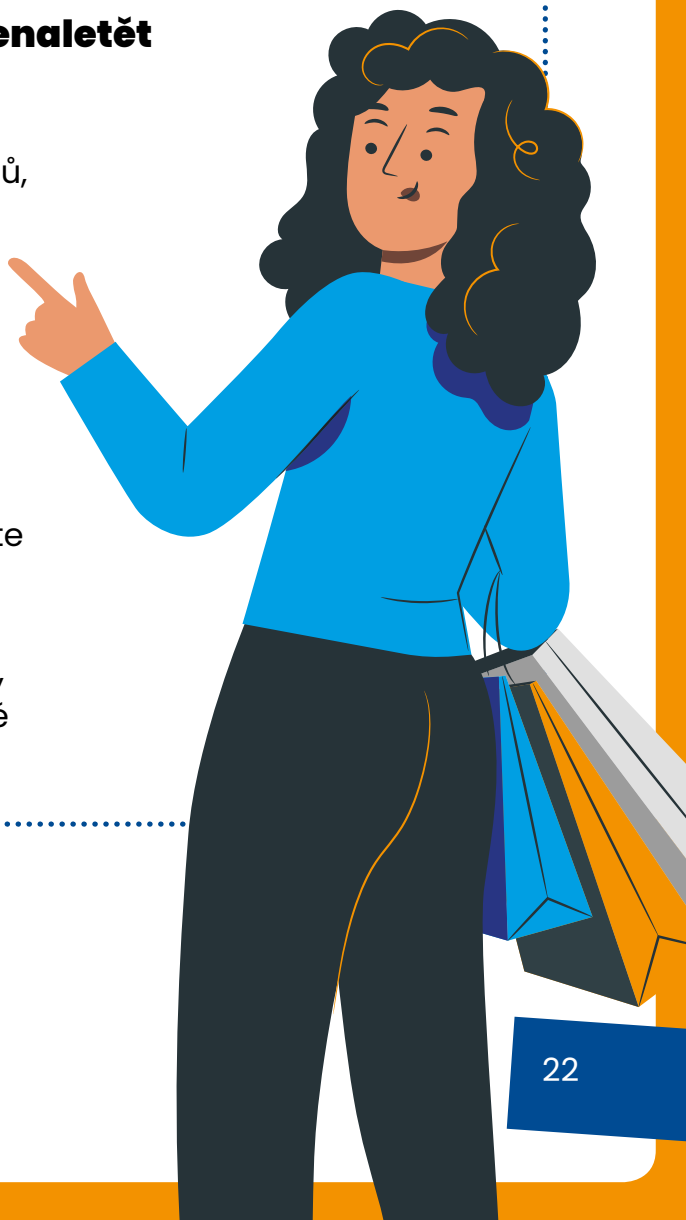
Podvodná jednání na internetových inzertních portálech mají většinou totožný scénář a probíhají zpravidla písemnou formou. Velmi často evidujeme inzertní podvody na online bazarech jako je Aukro, Bazoš, Sbazar, Vinted nebo Marketplace na platformě Facebook.
Aby podvodníci nalákali co nejvíce obětí, nejčastěji zveřejňují inzeráty na žádané položky jako je elektronika nebo značkové zboží. Cena pak bývá velmi výhodná, někdy



až podezřele nízká. Při komunikaci se budou vyhýbat osobnímu předání a zaslání zboží na dobírku, jelikož si tak můžou co nejvíce zachovat svoji anonymitu. Aby z vás dostali peníze co nejrychleji, často budou tvrdit, že má o položku zájem i jiný uživatel, ale pokud zašlete peníze ihned, věc připadne vám. Jakmile budou mít platbu u sebe, přeruší veškerou komunikaci nebo se ještě různými sliby a ujišťováním budou snažit oddálit moment, kdy zjistíte, že jste byli podvedeni.
Pokud se rozhodnete něco objednat z online bazaru, domluvte se s prodejcem na zaslání na dobírku nebo osobním odběru. Nepodléhejte nátlaku, že musíte za zboží zaplatit co nejdříve, dejte si na čas a koupi si promyslete. Balíček si po obdržení rozbalte a zkontrolujte, zdali přišlo, co jste si objednali. V případě podvodu kontaktujte policii, a to i když částka pro vás nebude nijak vysoká. Škody způsobené jedním pachatelem se v těchto případech sčítají a je možné, že podvodníka, který připravil o peníze vás, mají policisté již v hledáčku. Chráníte tak bezpečí budoucích nákupů svých i ostatních.

Preventivní rady a doporučení, jak nenaletět podvodníkům na online bazarech:

- Cenové nabídky si porovnejte u více prodejců, vyhněte se podezřele nízkým cenám.
- Domluvte se s prodejcem na osobním předání nebo na zaslání na dobírku.
- Nepodléhejte nátlaku, koupi si promyslete.
- Až vám balíček dorazí, co nejdříve zkontrolujte jeho obsah pro případnou reklamaci.
- Pokud se stanete obětí podvodného jednání, kontaktujte Policii České republiky na tísňové lince 158 nebo na policejní služebně.



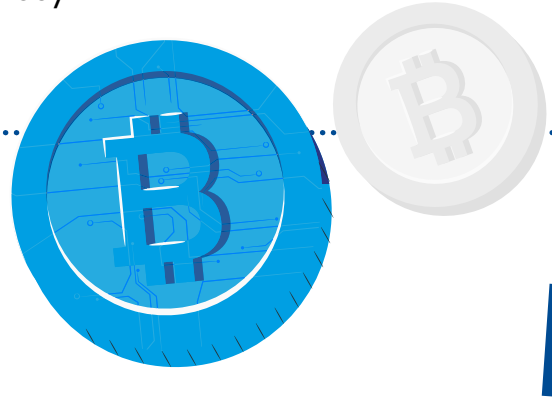
Odkaz na preventivní video od Policie ČR:
Policie ČR: Volač a klikač II. - YouTube

Vishing a spoofing

V poslední době hodně diskutované využívání nástrojů sociálního inženýrství, kdy se podvodníci vydávají za bankéře a následně i policisty a pod legendou ohrožení finančních prostředků na bankovním účtu manipulují svoji oběť do provádění finančních transakcí. Nic netušící majitel bankovního účtu z obavy o své peníze převádí peníze přímo podvodníkům.
Ve stejném duchu probíhá také výzva k vybrání hotovosti z „ohroženého“ bankovního účtu a dočasné vložení finančních prostředků do kryptoměn. Tím mají být peníze ochráněny do doby, než se problém s ohroženým účtem vyřeší. Realita je ovšem taková, že tyto peníze nenávratně mizí ve virtuálních peněženkách podvodníků. Vystrašená oběť dostává zcela přesné instrukce i QR kódy, na jaké konkrétní uložiště má za hotovost nakoupenou kryptoměnu odeslat. Oproti online převodům je tento přístup ještě více rizikový. Hotovostní transakce nemůže banka v případě podezření zastavit ani zablokovat a jakmile je převod na kryptoměnu realizován nejde ho už prakticky nijak zastavit či zvrátit.

Preventivní rady a doporučení, jak nenaletět podvodníkům:

- Vždy si důvody takových telefonátů ověřujte na oficiálních kontaktech bankovních či finančních společností či dalších organizací, za které se podvodníci v dané chvíli vydávají.
- Pamatujte, že banky ani Policie České republiky s provozovateli tzv. vkladomatů nespolupracují.
- Případné ohrožení bankovních účtů klientů řeší banky samy a nepotřebují k tomu zasílání přístupových údajů či údajů z platebních karet.
- Nikdy nenakupujte kryptoměny na adresy, které Vám někdo jiný předá ani je na takové adresy nepřevádějte, pokud nejde o legitimní a vámi zamýšlenou platbu.



Investiční podvody

Pokud zvažujete, jak zhodnotit své úspory, vybírejte velmi obezřetně, do čeho a s jakými poradci budete investovat. Podvody, ve kterých hrají roli přislíbené vysoké zisky z investic, jsou velmi propracované a naletět je poměrně snadné.
Vše většinou začíná velmi výhodnou nabídkou, např. v podobě internetové reklamy. Vedle investic různého charakteru nabízejí podvodníci také pomoc s nákupem virtuálních měn, často s příslibem velkého výnosu. Komunikace mezi pachatelem a obětí je většinou dlouhodobá. Oběť je utvrzována, že vše běží podle plánu, např. přístupem do falešného portfolia či virtuálních peněženek na různých demo stránkách. Opět pro zvýšení důvěryhodnosti jsou vyžadovány pravidelné vklady, často s podmínkou vyplacení výnosů až po delším časovém úseku. O tom, že místo zhodnocení finančních prostředků zbydou jen oči pro pláč, se tak poškozený dozvídá až po delší době.
Pachatelé vystupují profesionálně, mají několik úrovní „pracovníků“ (operátory, poradce, techniky, manažery) a jejich legendy jsou propracované s cílem maximalizace zisku.
Pokud chce oběť investované peníze vybrat, přejdou ke strategii komplikací, kdy je nutno zaslat ještě tu „jednu poslední platbu“ a pak už budou velké peníze vyplaceny. Tato psychická manipulace se označuje jako tzv. sunk cost fallacy (česky: utopené náklady). Podstatou je úvaha oběti: „Už jsem do toho dal tolik, teď přece nepřestanu platit, když jsem tak blízko!“
Často oběť podvodníkům, kteří se vydávají za investiční poradce, poskytne kromě osobních údajů, snímků dokladů totožnosti či platebních karet také vzdálený přístup ke svému počítači.
K vybílení účtu pak už nebrání prakticky nic.

Preventivní rady a doporučení, jak nenaletět podvodníkům:

- Ke každé investici přistupujte jako k rizikové (obzvláště u tak volatilního aktiva jako kryptoměny) a nikdy k investování či nákupu kryptoměn nepoužívejte celé své jmění.

- Před tím, než se rozhodnete investovat do kryptoměn, zjistěte si, jak fungují velké burzy a investiční platformy a nákup a prodej kryptoměny.

- Vždy pečlivě ověřujte věrohodnost investičního poradce či společnosti. Rozhodně nespoléhejte jen na internetové recenze, ty může napsat kdokoliv, tedy i podvodník.

- Nespoléhejte na to, že podvodný web poznáte podle vzhledu, podvodné stránky investičních platforem bývají profesionálně zpracované, často umožňují vytvoření uživatelského účtu a sledování, samozřejmě podvrženého a fiktivního, portfolia.

- Za žádných okolností neposkytujte vzdálený přístup ke svému počítači.

- Chraňte svá osobní, přístupová hesla a údaje z platebních karet.

- Pokud údaje o svém bankovním účtu pod vlivem manipulace poskytnete podvodníkovi, ihned kontaktujte svou banku.

- Pozor na reklamy! Podvodníci si mohou jednoduše zaplatit reklamní kampaň u velké platformy (např. Google, Facebook…) s odkazy na svoje podvodné stránky. Takové reklamy se pak mohou objevit kdekoli, klidně i na prověřených stránkách.

Děkujeme, že nám pomáháte dělat internet bezpečnější.

Ilustrations by stories / Freepik