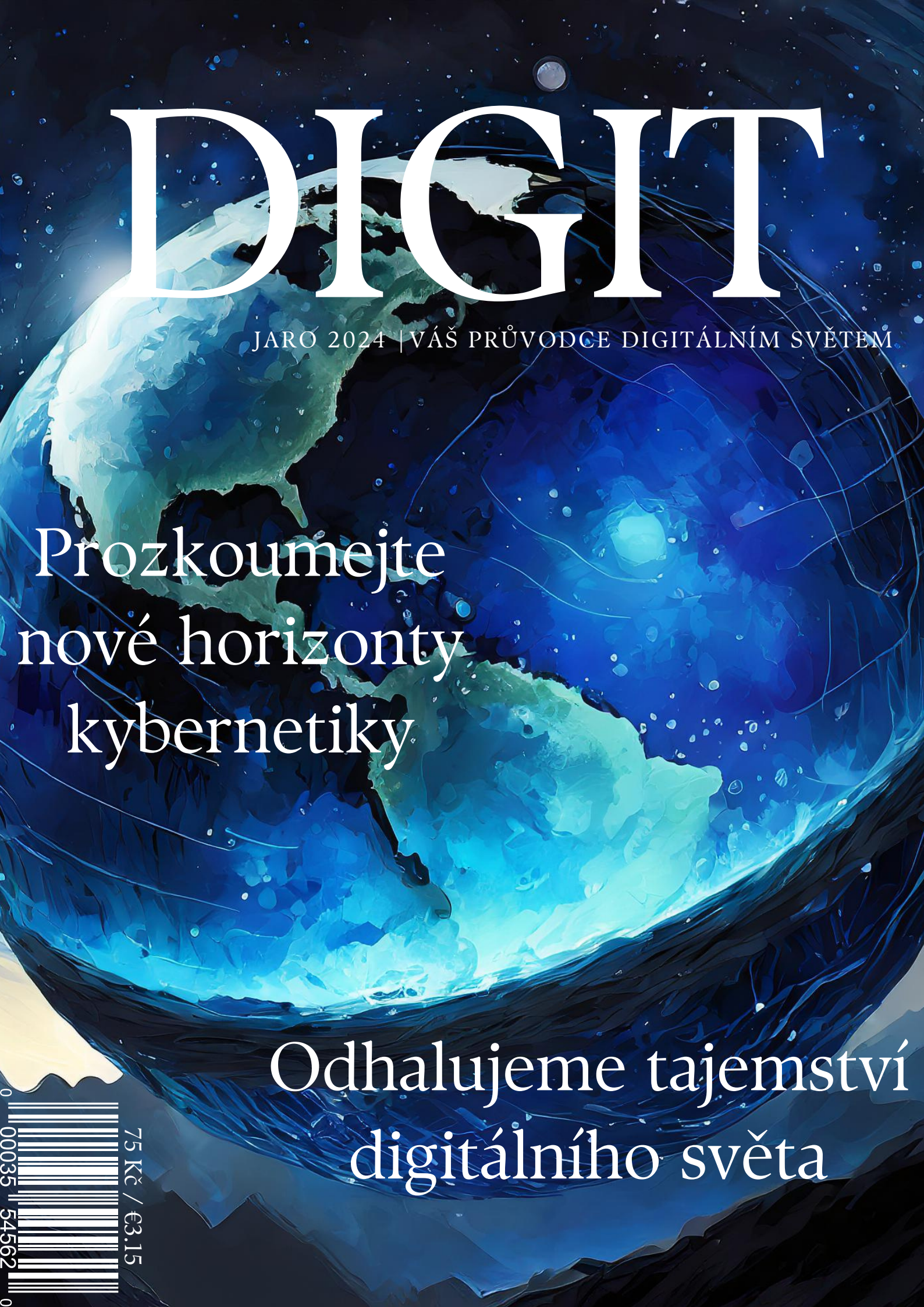


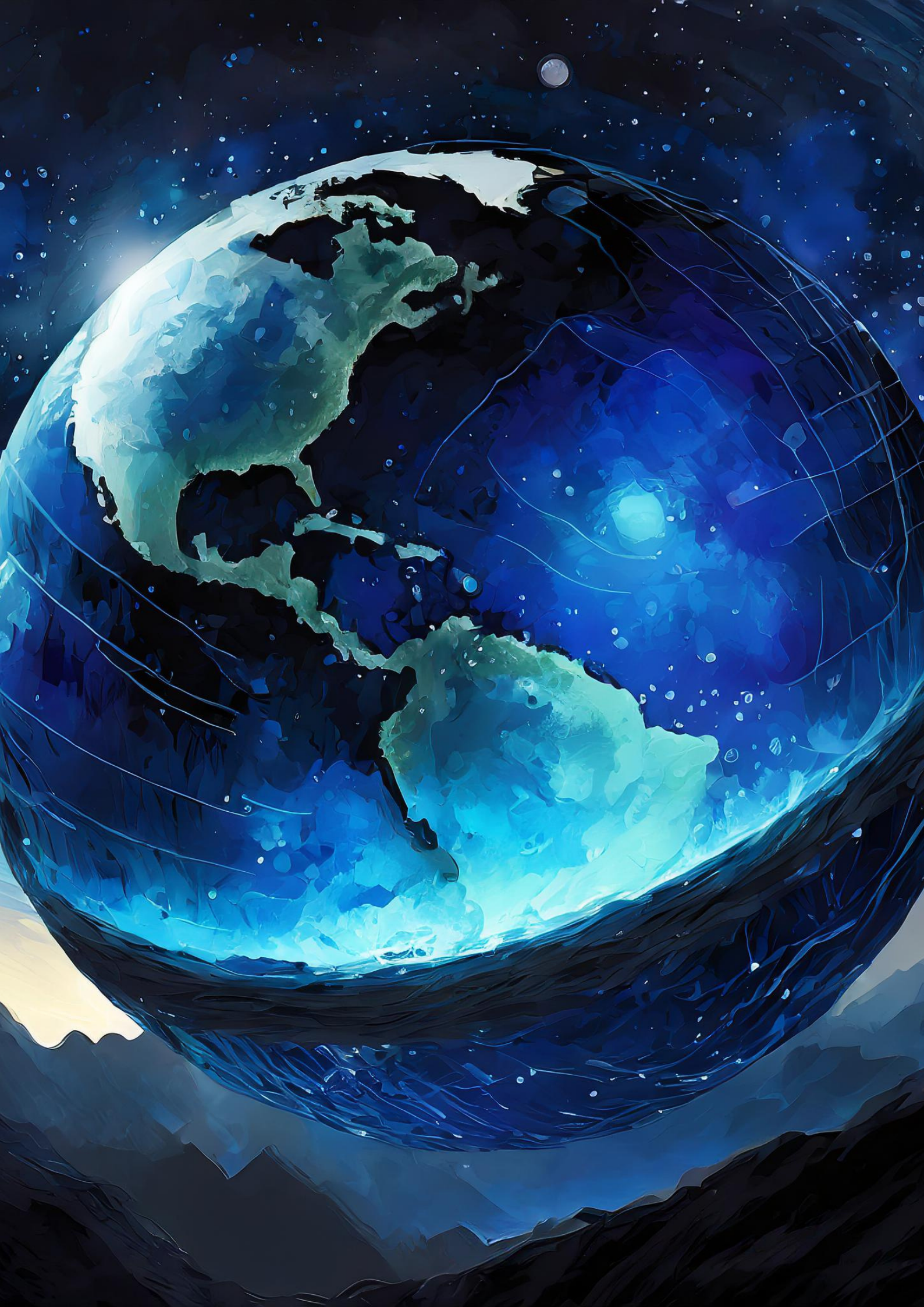
DIGIT

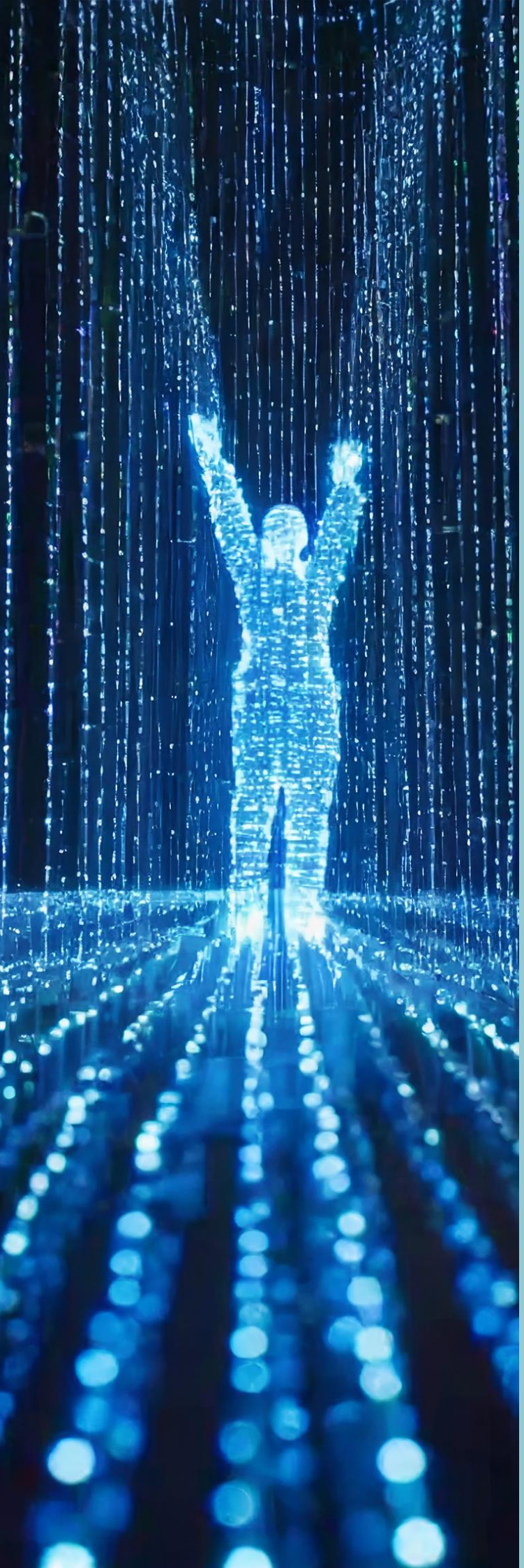
JARO 2024 | VÁŠ PRŮVODCE DIGITÁLNÍM SVĚTEM

Prozkoumejte nové horizonty kybernetiky

Odhalujeme tajemství digitálního světa

75 Kč / €3.15
0 00035 54562 0





Vážení čtenáři,
vítáme Vás u prvního a průlomového čísla našeho časopisu zaměřeného na bezpečnost na internetu a práva uživatelů. Jsme studentky s vášní a odhodláním, spojené snahou šířit povědomí o klíčových aspektech digitální bezpečnosti.
Naše stránky jsou věnovány nejenom informacím o aktuálních hrozbách a bezpečnostních opatřeních, ale také o osvětě o právech (i povinnostech?), které máte jako uživatelé internetu. Přinášíme Vám praktické rady, analýzy trendů a podnětné příklady, které Vám pomohou lépe porozumět digitálnímu světu. Naším cílem je obeznámit Vás, jak chránit své právo na bezpečné a svobodné používá online prostoru. Děkujeme vám, že jste s námi a těšíme se na sdílení této cesty bezpečnějším digitálním světem společně.
S přáním příjemného čtení,

Markéta Sůrová
Julie Lukášková
Klára Řeháková

OBSAH

5 Přehled aktuálních hrozeb v kybernetickém prostředí

Kybernetická temnota: Odhalujeme aktuální hrozby v digitálním světě

7 Hackeři a jejich metody

Zákulisí virtuálního zlodějství: Profil hackera a jeho skryté motivace

8 Reálné příběhy

Z očí do očí s kybernetickým nebezpečím: Reálné příběhy obětí kybernetických útoků

9 Ochrana bankovních účtů

Chráníme Vaše finanční bezpečí: Bezpečnostní opatření pro online bankovnictví

10 Prevence vykradení bankovního účtu

Poznáváme nebezpečné signály: Jak identifikovat příznaky možného kybernetického útoku

11 I internet je vyčerpávající

Digitální detox: jak najít rovnováhu ve světě online

12 Kdo si hraje, nezlobí

Umíte brouzdat internetem bezpečně

Proč chce internet chodit na terapie?
Má problémy s připojením a cítí se být odpojený od reality.

Kybernetická temnota:

Odhalujeme aktuální hrozby v kybernetickém světě

Vstupte do temných koutů digitálního světa, kde se pohybují nebezpeční kybernetičtí predátoři. V našem článku odkryjeme nejnovější hrozby, které hrozí každému uživateli online prostředí. Od záludných phishingových útoků až po sofistikované malware, připravte se na cestu do světa, který nikdy nespí a kde nebezpečí číhá za každým kliknutím. Je důležité mít na paměti, že každý online krok může zanechat digitální stopu.

Sociální sítě jsou důležitou součástí našeho každodenního života, ale mohou být i hnízdem různých kybernetických nebezpečí. Mnoho uživatelů čelí kyberšikaně, identitnímu krádeži a šíření falešných informací. Kromě toho jsou sociální sítě oblíbeným cílem pro phishingové útoky, kde útočníci využívají důvěryhodný vzhled stránek ke získání citlivých informací od uživatelů.

Phishing je taktika, kterou útočníci využívají k získání citlivých informací od uživatelů, jako jsou hesla, platební údaje nebo osobní údaje. Obvykle se to děje prostřednictvím falešných e-mailů, webových stránek nebo zpráv na sociálních sítích. Uživatelé by měli být obezřetní a vyhýbat se otevírání podezřelých odkazů nebo poskytování citlivých informací na neznámých webech.

Malware a viry jsou škodlivé programy, které mohou infikovat naše zařízení a způsobit vážné škody. Může se jednat o ransomware, který zablokuje přístup k datům až do zaplacení výkupného, nebo spyware, který sleduje naše aktivity a sbírá citlivé informace. Je důležité mít aktualizovaný antivirový software a vyhýbat se stahování souborů z neznámých zdrojů.

S rostoucím vlivem sociálních médií se šíření falešných informací a dezinformace stává stále větším problémem. To může vést k narušení důvěry veřejnosti v důležité informace a procesy.

Zákulisí virtuálního zlodějství: Profil hackera a jeho skryté motivace

Hackeři - tajemní jedinci pohybující se v digitálním podsvětí, kteří se nebojí využít své technické dovednosti k získání nepovoleného přístupu k informacím. Ale co je hnací silou těchto jedinců? Jaké jsou jejich motivace a cíle? Podívejme se na profil hackera a prozkoumejme, co se skrývá za jejich činy.

PROFIL HACKERA

Hackeři mají často vysokou úroveň technických znalostí v oblasti počítačového programování, sítí a bezpečnosti. Tyto dovednosti jim umožňují proniknout do cílových systémů a získat neoprávněný přístup k informacím.

Hackeři často projevují kreativitu a inovativní myšlení při hledání způsobů, jak obejít bezpečnostní opatření a získat přístup k citlivým datům. Jsou schopni využívat různé techniky a nástroje k dosažení svých cílů.

MOTIVACE HACKERA

Pro některé hackery je hlavním motivem finanční zisk. Může se jednat o krádež peněz, únos dat pro výkupné nebo provádění podvodných transakcí.

Někteří hackeři jednají z ideologických důvodů, jako je protest proti určité politické nebo společenské agendě, šíření politických zpráv nebo sabotáž cílových organizací.

Pro některé hackery je motivací prostě zábava a výzva. Mají zájem o zkoušení svých schopností a hledání nových cílů pro své útoky.

Co dělají hackeři na tanečním parketu?

Bezpečný Protokol:

Jak předcházet hackerům a chránit svůj digitální svět

Hackeři jsou nezvanými hosty v digitálním světě, kteří využívají své schopnosti k nekalým činům. Je důležité rozumět jejich motivacím a prevenci, abychom ochránili naše digitální prostředí. Použití bezpečnostních opatření a vzdělávání o kybernetických hrozbách mohou pomoci minimalizovat riziko úspěšného útoku a chránit naše osobní a firemní údaje.

Organizace by měly investovat do posílení svých bezpečnostních opatření, včetně firewallů, antivirových programů a monitorování sítového provozu,aby minimalizovaly riziko útoků.

Vzdělávání zaměstnanců a uživatelů internetu o kybernetických hrozbách a správných postupech v oblasti kybernetické bezpečnosti může pomoci snížit riziko úspěšného útoku.

Pravidelné provádění bezpečnostních auditů a aktualizace softwaru a systémů mohou pomoci odhalit a odstranit zranitelnosti, které by mohly být zneužity hackery. Uživatelé by měli pravidelně aktualizovat svůj software a systémy na nejnovější verze.

Uživatelé by měli používat silná a jedinečná hesla pro každý účet a implementovat vícefaktorovou autentizaci tam, kde je to možné. To zvyšuje bezpečnost účtu tím, že vyžaduje dodatečný ověřovací faktor kromě hesla, například SMS kód nebo biometrickou identifikaci.

Firewall je základní bezpečnostní prvek, který může zabránit neoprávněnému přístupu do sítě nebo zařízení. Správně nakonfigurovaný firewall může blokovat podezřelý sítový provoz a ochránit systém před útoky.

Pravidelné zálohování důležitých dat a informací může pomoci minimalizovat škody způsobené ransomwarem nebo jinými formami datových útoků. Zálohovaná data mohou být obnovena v případě úspěšného útoku, což umožní organizaci pokračovat v provozu bez významných přerušení.

Všechny své kroky zašifrují.

Z očí do očí s kybernetickým nebezpečím:

Reálné příběhy obětí kybernetických útoků

V dnešní době digitálních technologií jsou kybernetické útoky stále častější a jejich dopady mohou být devastující. Za těmito anonymními útoky stojí skuteční lidé, kteří čelí nejen ztrátě finančních prostředků, ale také emočnímu stresu a narušení soukromí. Podívejme se na několik reálných příběhů obětí kybernetických útoků a jak se s nimi vypořádali.

Paní Anna byla obětí phishingového útoku, ve kterém dostala e-mail, který vypadalo jako oficiální oznámení od její banky. Byla požádána, aby klikla na odkaz a přihlásila se ke svému bankovnímu účtu. Důvěřivě klikla a vyplnila své přihlašovací údaje. Bohužel se však ukázalo, že e-mail byl falešný a útočníci získali přístup k jejímu účtu. Paní Anna tak ztratila všechny své finanční úspory, které na účtu měla.

Poučení: Vždy dbejte na opatrnost při klikání na odkazy v e-mailech a nikdy nezadávejte citlivé informace, jako jsou přihlašovací údaje, na neověřených webových stránkách.

Pan Petr, malý podnikatel, se stal obětí ransomwarového útoku, který zablokoval přístup k důležitým souborům a dokumentům na jeho počítači. Útočníci požadovali výkupné za obnovení souborů, což by pro něj znamenalo obrovskou finanční zátěž. Pan Petr se musel obrátit na odborníky na kybernetickou bezpečnost, aby mu pomohli obnovit jeho data a zvážit další kroky k zabezpečení jeho systémů.

Poučení: Pravidelně zálohujte důležité soubory a používejte aktualizovaný antivirusový software k minimalizaci rizika infekce ransomwarem.

Paní Eva si uvědomila, že se stala obětí identitní krádeže poté, co zjistila neautorizované transakce na svých bankovních účtech a zaznamenala neobvyklé aktivity spojené s jejím jménem. Kromě finanční ztráty se musela potýkat s dlouhým procesem obnovy své identity a opravy škod, které útočníci způsobili.

Poučení: Pravidelně kontrolujte své bankovní výpisy a sledujte neobvyklou aktivitu spojenou s vaší identitou, abyste rychle odhalili případnou identitní krádež.

Tyto příběhy slouží jako připomínka toho, jak důležité je být obezřetný a chránit své osobní a finanční údaje před kybernetickými hrozbami. Prevence je vždy lepší než léčba, a proto je důležité dodržovat bezpečnostní opatření a být ostražitý při používání digitálních technologií.

Chráníme Vaše finanční bezpečí:

Bezpečnostní opatření pro online bankovnictví

V dnešní době, kdy se stále více obracíme k online bankovnictví, je zajištění bezpečnosti našich finančních prostředků a osobních údajů klíčové pro ochranu před kybernetickými hrozbami.

S nárůstem digitálních technologií však přichází i nové rizika a výzvy, kterým musíme čelit. Proto je důležité být obezřetní a uplatňovat bezpečnostní opatření při používání online bankovních služeb.

Zajištění bezpečnosti vašeho online bankovního účtu je zásadní pro ochranu vašich finančních prostředků a osobních údajů před kybernetickými hrozbami. Dodržování uvedených bezpečnostních opatření vám může pomoci minimalizovat riziko úspěšného útoku a poskytnout vám větší klid v mysli při používání online bankovnictví. Tento článek byl vytvořen s cílem informovat a osvětlovat o důležitosti bezpečnosti při používání online bankovnictví a poskytnout praktické tipy k zajištění bezpečnosti jejich finančních účtů.

1

Používání bezpečné sítě pro přístup k vašemu bankovnímu účtu je dalším klíčovým opatřením. Vyhněte se připojení k veřejným Wi-Fi sítím nebo neznámým sítím, které mohou být zranitelné vůči útokům. Pokud je to možné, používejte síť VPN pro zajištění dodatečného šifrování vašeho internetového provozu.

2

Druhým klíčovým opatřením je aktivace dvoufaktorové autentizace (2FA). 2FA zahrnuje ověřování vaší identity pomocí dvou nezávislých faktorů, jako je heslo a jednorázový kód zaslaný na váš mobilní telefon. Tento dodatečný krok přidává vrstvu bezpečnosti, která ztěžuje hackeřům přístup k vašemu účtu.

3

Opatrnost při klikání na odkazy v e-mailech je další důležitým pravidlem pro zajištění bezpečnosti vašeho online bankovnictví. Hackeři často využívají phishingové útoky k získání citlivých informací od uživatelů. Buďte obezřetní při klikání na odkazy obsažené v podezřelých e-mailech a vyhněte se poskytování citlivých informací na neznámých webových stránkách.

4

Nikdy neposílejte osobní informace, jako jsou číslo účtu, PIN kódy nebo hesla e-mailem nebo prostřednictvím nezabezpečených kanálů komunikace. Buďte obezřetní při sdílení svých bankovních informací na sociálních sítích a online platformách.

Poznáváme nebezpečné signály: Jak identifikovat příznaky možného kybernetického útoku

V digitálním věku, kde jsme neustále propojeni s online světem, je důležité být obezřetní a pozorně sledovat různé signály, které naznačují možný kybernetický útok. Tyto signály mohou být klíčovými indikátory, že něco není v pořádku se zabezpečením našich zařízení a účtů. Zde je několik nejčastějších příznaků, na které byste měli být pozorní,

Pokud zjistíte neobvyklé transakce na vašem bankovním účtu nebo podezřelé změny v aktivitě na vašich online účtech, mohlo by to být znamení, že byl váš účet kompromitován.

Neočekávaný pokles výkonu vašeho počítače, zvýšená spotřeba energie nebo neobvyklé chování aplikací mohou být známkami toho, že by váš systém mohl být infikován malwarem.

Neobvykle pomalé internetové připojení, zejména pokud je to způsobeno několika zařízeními v síti, může naznačovat, že některé z nich mohou být zapojeny do kybernetického útoku, například do distribuce spamu nebo DoS (Denial of Service) útoku.

Systémové chyby, neočekávané restarty, nezvyklé výzvy k zadání hesla nebo změny v nastavení systému bez vašeho svolení mohou být příznaky toho, že by mohl být váš systém kompromitován.

Pokud najednou zjistíte, že nejsou dostupné některé důležité soubory, nebo pokud se zobrazí výzva k zaplacení výkupného za jejich obnovení, mohlo by to být znamení ransomwarového útoku.

Pokud zaznamenáte neobvyklé e-maily od známých nebo neznámých odesílatelů, zejména s požadavky na zaslání citlivých informací nebo otevření podezřelých příloh, mohlo by to naznačovat phishingový útok.

Proč banka vypadá jako přátelské místo?
Protože má vždy úsměv na tváři, když vidí vklad!

Je důležité být pozorný na tyto signály a jednat rychle, pokud se některý z nich objeví. Pokud máte podezření, že jste se stali obětí kybernetického útoku, okamžitě kontaktujte svou banku nebo poskytovatele služeb a sledujte další kroky k zabezpečení vašich účtů a zařízení.

Pamatujte, že prevence je vždy lepší než léčba, a že nejlepší způsob, jak se chránit před kybernetickými útoky, je pravidelně aktualizovat své znalosti o bezpečnosti a uplatňovat nejlepší postupy v oblasti kybernetické bezpečnosti.

Digitální Detox: Jak najít rovnováhu ve světě online

V dnešní době jsme neustále spojeni s digitálním světem prostřednictvím chytrých telefonů, tabletů a počítačů. Zatímco moderní technologie nám přinášejí mnoho výhod a možností, může být neustálý digitální proud také vyčerpávající a způsobovat stres. Jak najít rovnováhu mezi online a offline světem? To je otázka, kterou si mnozí z nás klade. V tomto článku prozkoumáme koncept "digitálního detoxu"
a poskytneme tipy, jak si najít zdravou rovnováhu ve světě online. Tento článek by mohl poskytnout inspiraci a návody, jak najít rovnováhu a zvýšit kvalitu svého života prostřednictvím digitálního detoxu.

Co je to digitální detox?

Digitální detox se stává stále populárnější alternativou v dnešním světě plném technologie. Jedná se o dočasné omezení nebo úplné odpojení od digitálních zařízení
a online aktivit, s cílem obnovit mentální a emocionální zdraví.

Důvody pro digitální detox.

Existuje mnoho důvodů, proč se lidé rozhodují podstoupit digitální detox. Někteří cítí, že jsou příliš závislí na sociálních médiích a ztrácejí kontakt
s reálným světem. Jiní trpí nedostatkem spánku kvůli neustálému sledování obrazovek. Další mají pocit, že jejich produktivita klesá kvůli neustálému rušení online notifikacemi. Digitální detox může být řešením pro tyto problémy
a mnoho dalších.

Jak na to?

Pokud se rozhodnete pro digitální detox, je důležité si stanovit jasné cíle
a plán, jak je dosáhnout. To může zahrnovat omezení času stráveného
na sociálních médiích, vyhrazení určitých časových okamžiků bez použití chytrých telefonů nebo pravidelné digitální pauzy během dne. Může také zahrnovat například pobyt v přírodě, cvičení, čtení nebo trávení času s rodinou a přáteli.

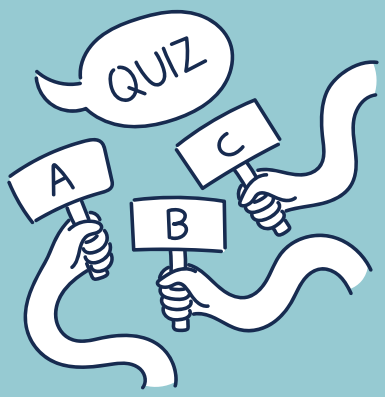
Benefity digitálního detoxu.

Existuje mnoho potenciálních benefitů spojených s digitálním detoxem. Mezi ně patří zlepšený spánek, zvýšená produktivita, lepší koncentrace, zlepšení mezilidských vztahů a celkové zvýšení duševního blahobytu.

Facebook je jediné místo, kde můžete koukat do zdi a nejste za blázna.

Umíte brouzdat internetem bezpečně

Otestujte si Vaše znalosti bezpečného chování na internetu pomocí kvízu, který jsme pro Vás připravily.



1. Co znamená zkratka VPN?
   a) Veřejné připojení
   b) Platba bez přítomnosti karty
   c) Virtuální privátní síť

2. Jaké heslo je nejvhodnější použít?

   a) David
   b) 1JfmuV2Ba
   c) 13prosince1989

3. Jakou zkratku má protokol, který označuje zabezpečenou komunikaci v internetové síti?

   a) Https
   b) Hippopotamus
   c) Http

4. Jaké jsou nejčastější formy kybernetických útoků?

   a) Malware
   b) Phishing
   c) Vandalismus

5. Co je to phishing?

   a) Ochrana proti malwaru
   b) Metoda útoku, která využívá falešné e-maily nebo webové stránky k získání citlivých informací
   c) Je to přeci anglicky lovení ryb

6. Jaká je doporučená frekvence změny hesla?

a) Podle potřeby
b) Každý měsíc
c) Každých 6 měsíců

7. Jak se nejlépe ochránit před phishingem?

a) Otevřít podezřelý odkaz
b) Nikdy nesdílet osobní informace na neověřených webových stránkách
c) Nebuď ryba!

8. Co je to firewall?

a) Přece hořící facebooková zeď
b) Bezpečnostní opatření, které kontroluje a filtruje sítový provoz
c) Ochrana proti požáru

0-3
Jste loser!

Je důležité si uvědomit, že každý má své slabé momenty a neúspěchy. Důležité je se z nich poučit a jít dál. Nikdo není dokonalý a všichni máme prostor k růstu a zlepšení.

4-6
Totální průměr

Skvělý postoj! Stavět na průměrných znalostech a pracovat na nich, aby se přiblížily dokonalosti, je cesta k úspěchu a neustálému zlepšování. Držíme palce na vaší cestě k dalšímu rozvoji.

7-8
Jste mistr

To je skvělý výkon! Získat plný počet bodů a ovládat internet levou zadní je úspěch. Pokračujete v tomto směru a využívejte své schopnosti k dosažení ještě větších cílů. Gratuluji!

správné odpovědi: 1.c), 2.b), 3.a), 4.a), 5.b), 6.a), 7.b), 8.b)

Milí čtenáři,
rády bychom Vám touto cestou poděkovaly za Váš zájem a podporu při čtení prvního čísla našeho časopisu. Vaše pozornost a zájem jsou pro nás velkou motivací a potvrzením toho, že naše úsilí má smysl.
Vaše podněty, názory a komentáře jsou pro nás neocenitelné a pomáhají nám neustále zlepšovat naše články a přinášet vám obsah, který vás zaujme a přinese vám užitečné informace.
Děkujeme Vám za Vaši důvěru a přízeň, a těšíme se na setkání v dalších číslech našeho časopisu.
S přátelskými pozdravy,
Markéta, Julie a Klára

KONTAKTY:

Autoři: Markéta Sůrová, Julie Lukášková, Klára Řeháková
Koordinátorka: Mgr. Lenka Homoláčová

E-MAIL
hradeckralovemagazin@redakce.cz

TELEFON
+420 123 456 789

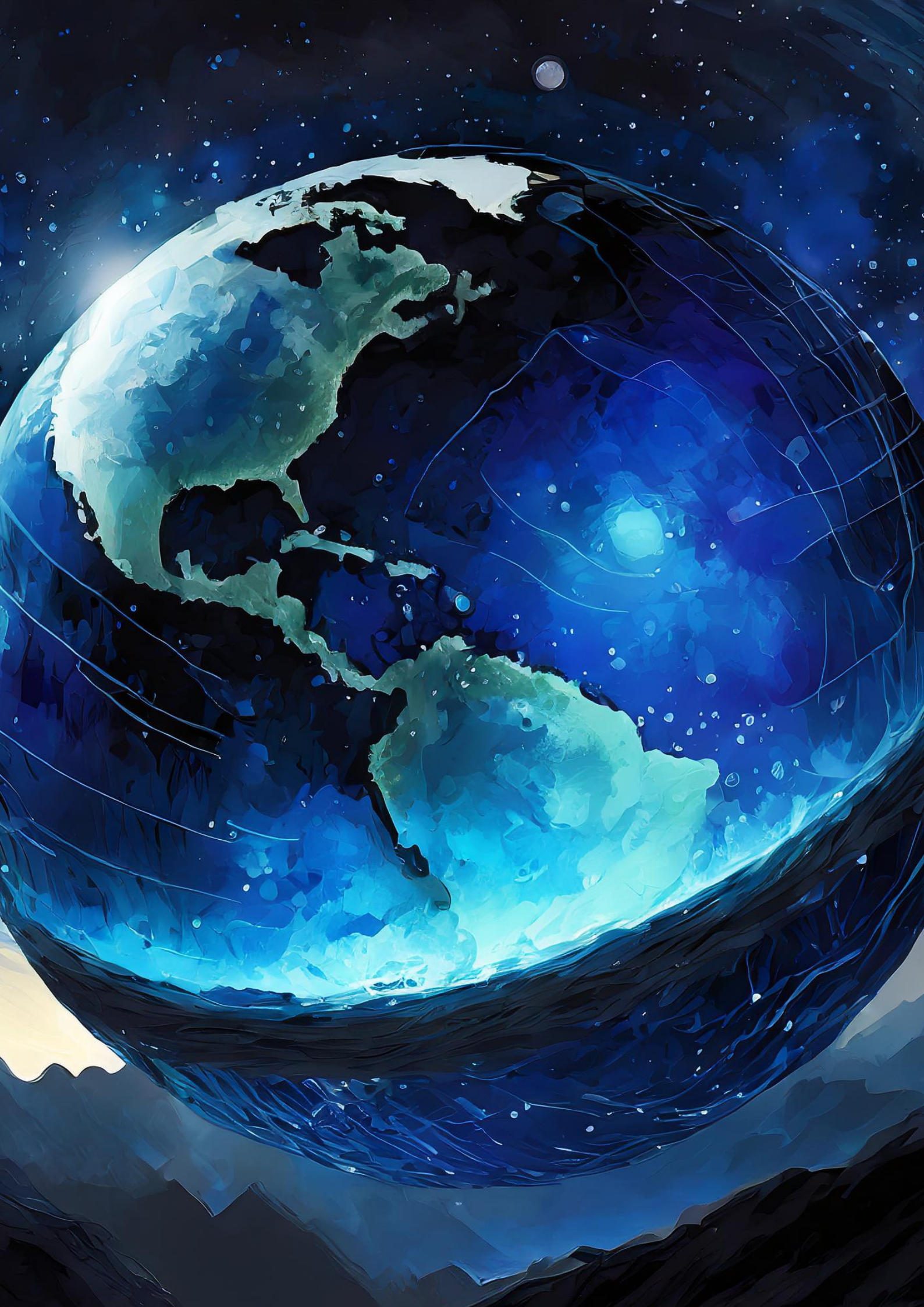
MOBIL
+ 420 987 654 321

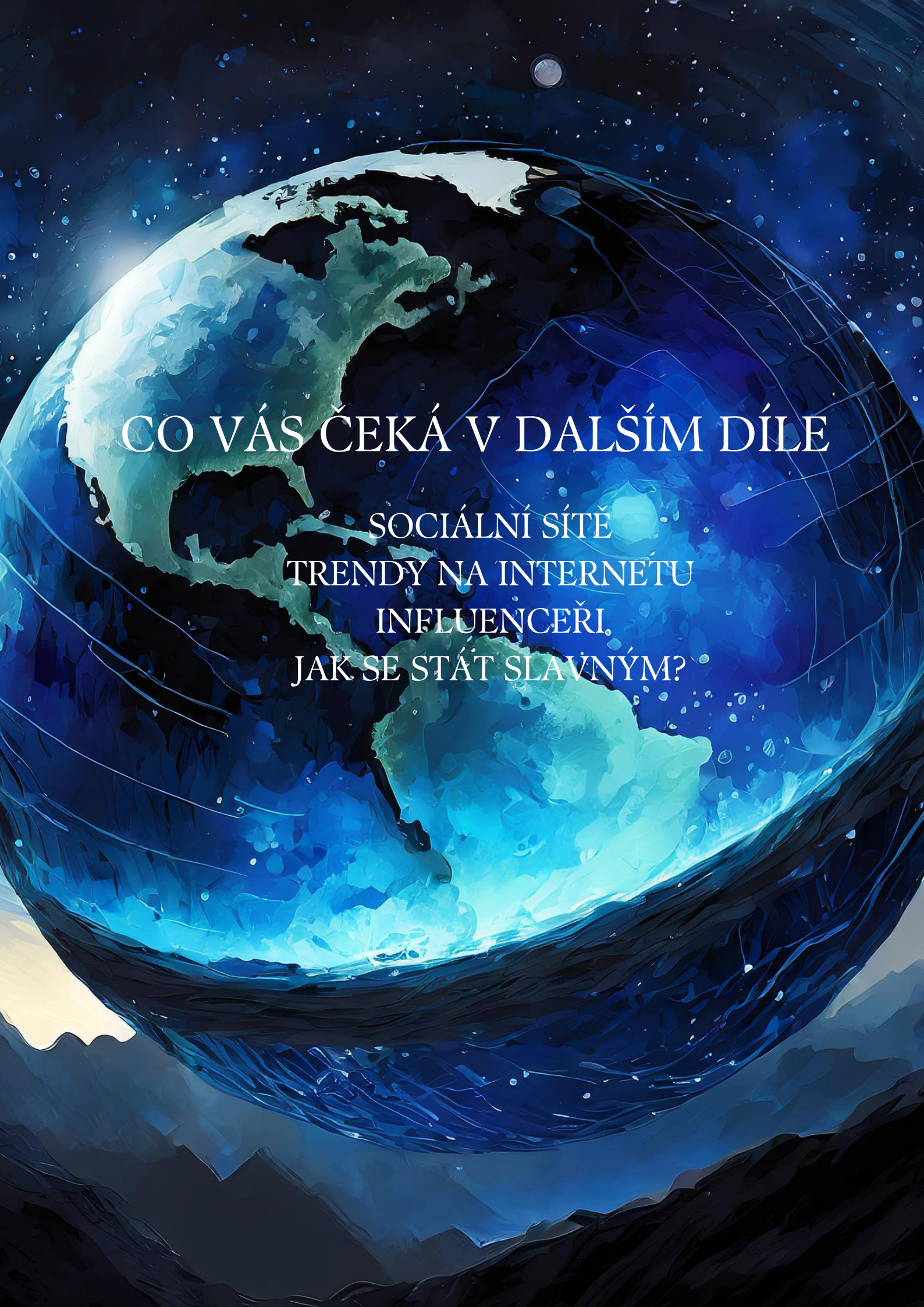
SÍDLO
Obchodní akademie, Střední odborná škola a Jazyková škola
Pospíšilová 365, 500 03 Hradec Králové

KDE NÁS NAJDETE?
digit_redakcehk

ZDROJE:

- Obrázky jsou generované AI, grafika Canva
- Vtipy jsou generované AI
- Hacking. [online]. [cit. 2024-02-25]. Dostupné z: https://www.dcit.cz/papers/eTime_Miko.pdf
- Motivace hackerů. [online]. [cit. 2024-02-25]. Dostupné z: https://is.muni.cz/th/cmtgj/BC_prace_Motivace_a_agresivita_hackeru_v2o.pdf
- Mobilní a Internetové bankovnictví [online]. [cit. 2024-02-25]. Dostupné z: https://slideplayer.cz/slide/2441968/
- Digitální desatero [online]. [cit. 2024-02-25]. Dostupné z: https://docs.google.com/presentation/u/0/d/1e-fZ04mjwZtQpM_rpENxpzgU_C5PuInlMJMpLvHNdao/htmlpresent?hl=cs&pli=1
- Digitální desatero [online]. [cit. 2024-02-25]. Dostupné z: https://www.kb.cz/cs/podpora/bezpecnost/desatero-bezpecnosti
- Digitální detox [online]. [cit. 2024-02-25]. Dostupné z: https://digitalnidetox.cz/





CO VÁS ČEKÁ V DALŠÍM DÍLE

SOCIÁLNÍ SÍTĚ
TRENDY NA INTERNETU
INFLUENCEŘI
JAK SE STÁT SLAVNÝM?