limitovaná edice
březen 2024
59,- Kč

CYBER GUARD

PRŮVODCE OCHRANOU A DIGITÁLNÍ BEZPEČNOSTÍ

NENECHME SE POHLTIT KYBERNETICKÝMI ÚTOKY!

SPOLEČNĚ TO ZVLÁDNEME

foto: canva

OBSAH

Kybernetické podvody se stávají čím dál tím větší společnostním problémem. Zrušení tohoto cyklu není v našich rukou, avšak tu přece jen jsou cesty jak ho obejít či alespoň minimálně zmírnit. Společně vás provedeme časopisem Cyberguard a pokusíme se vám ulehčit život.

Digitální podvody

Co jsou digitální podvody?

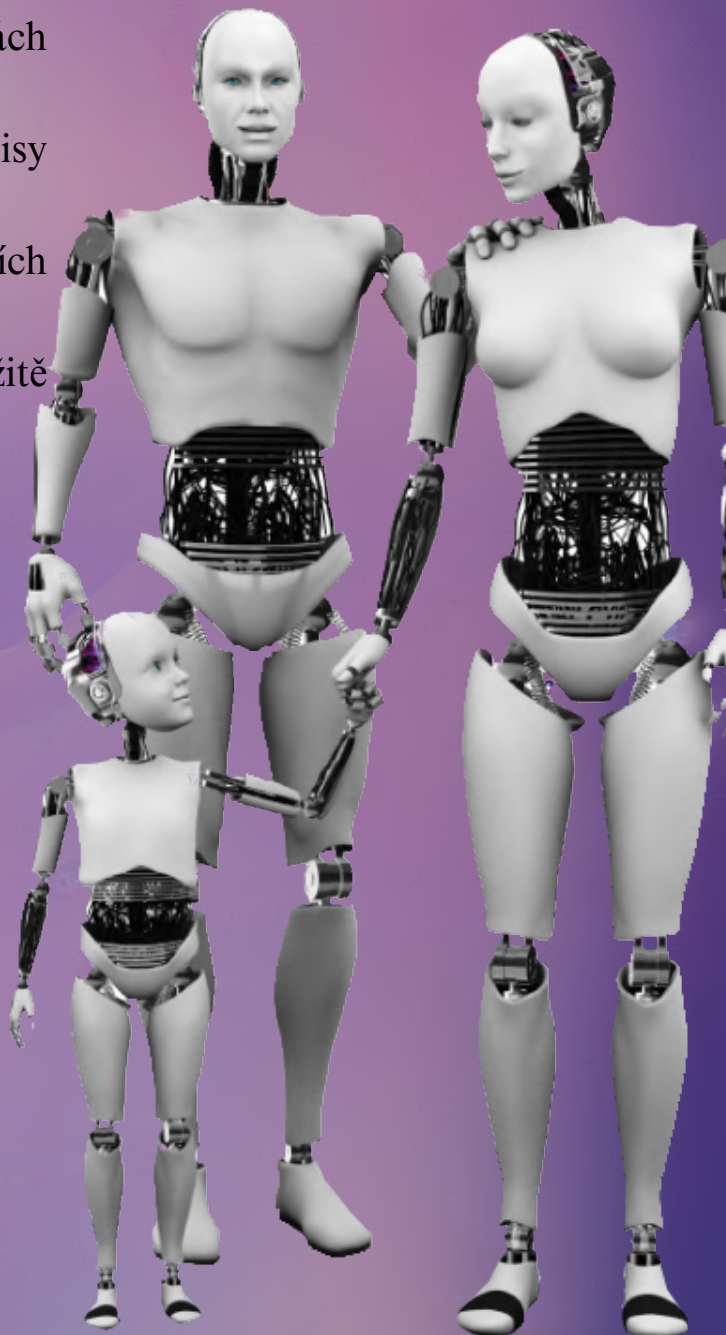
Digitální podvody představují nečestné a často ilegální praktiky, které se odehrávají prostřednictvím internetu nebo jiných digitálních technologií. Jsou zaměřeny na získání citlivých informací, finančních prostředků nebo jiných cenných aktiv od obětí. Tyto podvody mohou zahrnovat různé techniky, jako je phishing, ransomware, identitní krádež a další. Jejich cílem je často manipulace s důvěrou uživatelů nebo vytvoření zdání legitimnosti s cílem oklamat a získat neoprávněný přístup k účtům, údajům nebo finančním prostředkům.

Podvody jsou různého druhu, mění se v čase i na základě lokality. Podvodníky mohou být v dané zemi občané daného státu, ale i cizinci. Nejvíce online podvodníků neboli scammerů pochází z Brazílie, Pákistánu, Jižní Afriky či Rumunska. V Česku jsou aktivní Kazaši či Rusi.

https://chat.openai.com/auth/login

OPATŘENÍ K OCHRANĚ PŘED DIGITÁLNÍMI PODVODY

1. Vzdělávejte se: Poznejte různé typy podvodů a naučte se je rozpoznávat.
2. Opatrnost s e-maily a odkazy: Buďte obezřetní při klikání na odkazy a otevírání příloh v e-mailech.
3. Používejte silná hesla a povolte dvoufaktorovou autentizaci.
4. Udržujte aktualizovaný operační systém a antivirový software.
5. Provádějte online transakce pouze na důvěryhodných webových stránkách se zabezpečeným připojením.
6. Pravidelně kontrolujte své bankovní výpisy a transakce.
7. Sdílejte osobní informace opatrně na sociálních médiích.
8. Pokud se stane obětí podvodu, okamžitě kontaktujte svou banku a příslušné orgány.



Dodržování těchto opatření vám a vaši rodině pomůže minimalizovat riziko stát se obětí digitálních podvodů.

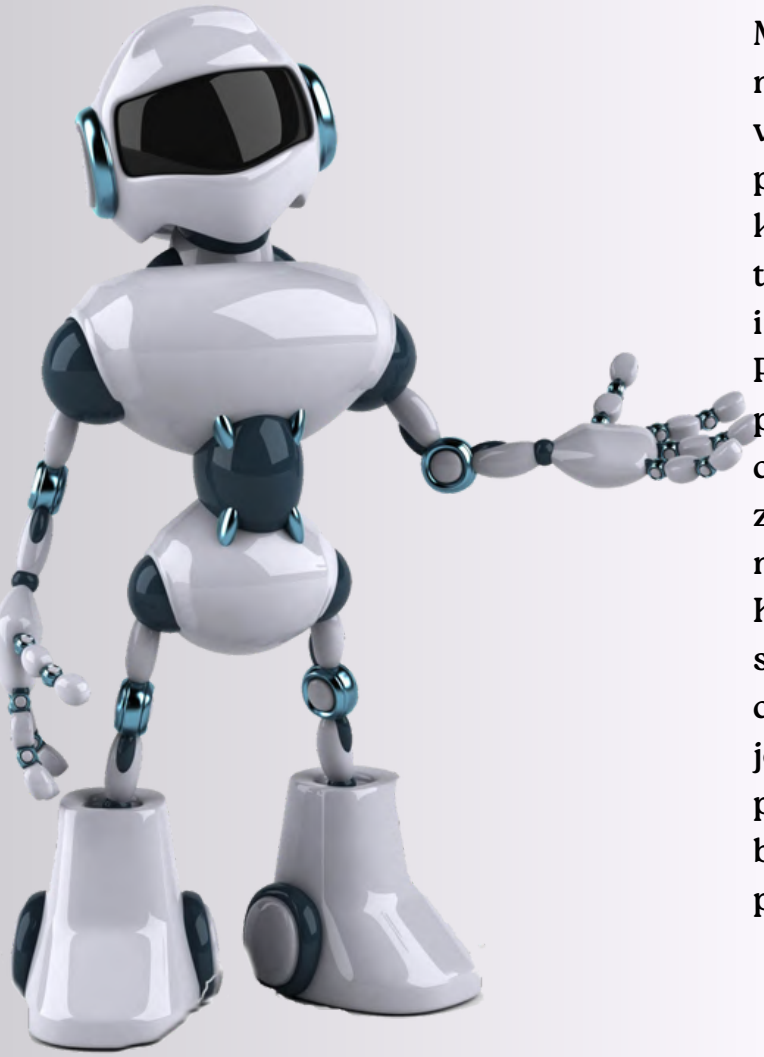
https://chat.openai.com/auth/login

Podvody na internetu stále rostou

Češi ročně přijdou až o

2 MILIARDY KORUN

Podle České bankovní asociace (ČBA) je průměrná škoda jednoho poškozeného při internetových podvodech 161 500 korun. Klienti tak loni přišli dohromady téměř o dvě miliardy korun. I policie potvrzuje rapidní nárůst on-line podvodů a varuje, že obětí se může stát každý.



Mezi momentálně nejčastější problémy v českém on-line prostředí, které kriminalisté řeší, patří takzvané reverzní inzertní podvody. Podvodník se v těchto případech staví do role falešného zájemce o koupi nabízeného zboží. Když se s prodávajícím domluví, navrhne, aby jeho platba proběhla pomocí platební brány, na kterou pošle odkaz.

V Česku vzrostl počet kyberútoků o 660 procent. Lukáš Benzl z České asociace umělé inteligence uvedl, že v Evropě vzrostla míra takzvaných deepfake útoků o 781 procent, v Česku pak prý o 660 procent. Je to neuvěřitelné číslo. Pokud nebudeme nic dělat, statistiky se mohou změnit k horšímu, to bylo uvedeno před odborníky a poslanci.

Typy internetových podvodů

Phishing: Podvodníci se vydávají za legitimní organizace nebo osoby a snaží se získat citlivé informace od obětí, jako jsou hesla, bankovní údaje nebo osobní identifikační údaje, často prostřednictvím falešných e-mailů, webových stránek nebo zpráv.

Smishing: Smishing je taktika podobná phishingu, ale místo e-mailů nebo webových stránek používá podvodné SMS zprávy, které lákají oběti k otevření odkazu nebo stáhnutí škodlivé aplikace.

Ransomware: Tento typ podvodu se zaměřuje na infikování počítačů nebo sítí škodlivým softwarem, který šifruje data oběti a požaduje výkupné za jejich obnovení.

Identitní krádež: Podvodníci kradeží osobní údaje obětí, jako jsou jména, adresy, čísla sociálního zabezpečení nebo bankovní údaje, aby je poté zneužili k provádění finančních transakcí nebo dalších nelegálních aktivit.

Sociální sítě: Útočník se vydává za kamaráda, který ztratil přístup k původnímu účtu. Požaduje peníze, přeposlání ověřovací SMS zprávy (s výmluvou na účast v soutěži) a podobně.

BEZPEČNÉ NÁKUPY ONLINE

Jak chránit své peníze a osobní údaje

S rostoucím trendem online nákupů je důležitější než kdy jindy zabezpečit své finanční prostředky a osobní údaje. Přestože internet nabízí pohodlí, skýtá také potenciální rizika. Připojte se k nám na naší cestě za bezpečnými online nákupy a objevte tipy, triky a nejnovější trendy v ochraně spotřebitelů. Naší prioritou je zajistit, abyste mohli využívat výhody on-line nakupování bez obav.

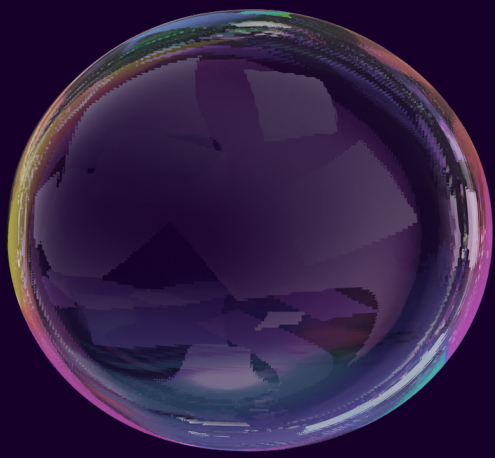
Podvodné transakce
Můžete se stát obětí podvodného prodejce, který vám po obdržení platby nepošle zboží nebo poskytne vadný produkt.

Zneužití osobních údajů
Pokud zadáte citlivé osobní údaje na nezabezpečené webové stránce, mohou být tyto údaje zneužity k identitní krádeži nebo dalším podvodným aktivitám.

Narušení bezpečnosti platebních informací
Pokud použijete nezabezpečenou platební metodu nebo zadáte platební údaje na falešné webové stránce, mohou být Vaše platební informace ohroženy a mohou být zneužity k neoprávněným transakcím.

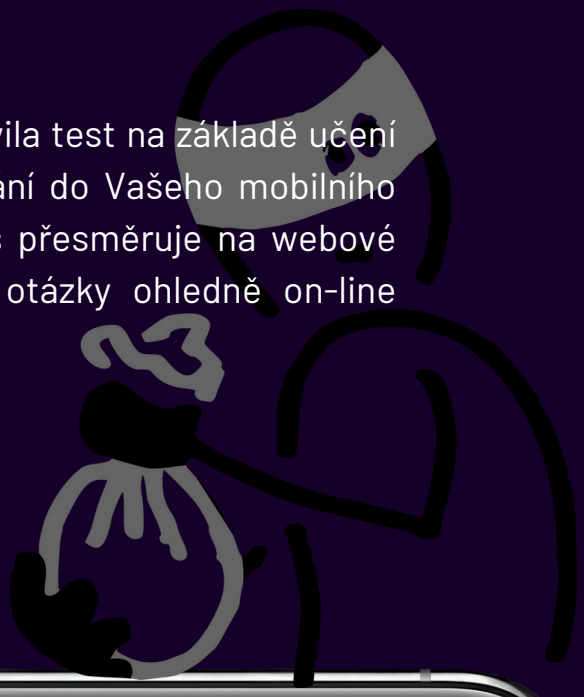
Ztráta peněz
V nejhorším případě můžete přijít o peníze, které jste investovali do nákupu online, pokud jste padli za oběť podvodnému prodejci nebo jste provedli neopatrnou transakci.

Nekvalitní produkty
Někdy můžete obdržet zboží, které neodpovídá popisu nebo není kvalitní. Pokud neexistuje možnost vrácení zboží nebo získání refundace, můžete ztratit peníze



NAUČTE SE NENALETĚT!

Společnost České bankovní asociace si pro Vás připravila test na základě učení se nenaletět. Níže uvedený QR kód Vás po naskenování do Vašeho mobilního telefonu či navštívení stránky www.kybertest.cz, Vás přesměruje na webové stránky, kde si sami můžete vyzkoušet připravené otázky ohledně on-line podvodů.



Dokázali byste nenaletět? Zkuste si on-line test!

https://chat.openai.com/auth/login

VÝHODY ON-LINE NAKUPOVÁNÍ

EKOLOGIE

Méně fyzických cest k obchodům znamená nižší emise CO2 a menší zátěž pro životní prostředí.

VRÁCENÍ ZBOŽÍ

Většina online obchodů nabízí flexibilní politiky vrácení zboží a záruky, což poskytuje zákazníkům větší klid a jistotu při nákupu.

PLATEBNÍ MOŽNOSTI

Moderní platební brány poskytují bezpečné a snadné platební možnosti. Zákazníci mohou platit kreditními kartami, bankovními převody nebo využít platebních bran, což zajišťuje bezpečnost jejich finančních údajů.

AKČNÍ NABÍDKY, SLEVY

Online obchody často nabízejí akční nabídky, slevy a propagační akce. Zákazníci mohou využít různé nabídky a ušetřit peníze při nakupování online.

DORUČENÍ

Mnoho online obchodů nabízí různé možnosti doručení, včetně expresního doručení a možnosti odběru zboží na blízkém místě. To zvyšuje pohodlí a šetří čas zákazníků.

ŠIROKÝ VÝBĚR

Online obchody mají obvykle obrovský sortiment zboží. Spotřebitelé mají možnost vybírat z produktů, které by jinak nebyly v dostupné ve fyzických prodejnách nebo k světovým značkám, které by nemusely být dostupné v místních prodejnách.

POHODLÍ

Nakupování online umožňuje spotřebitelům nakupovat kdykoliv a odkudkoliv. Bez ohledu na to, zda je to večer z domova nebo během pracovní přestávky, online nakupování poskytuje flexibilitu a pohodlí.

RECENZE

Spotřebitelé mohou snadno porovnávat ceny různých produktů a číst recenze od ostatních zákazníků. To jim umožňuje udělat informované rozhodnutí a najít nejlepší nabídky.

nemějte strach! online nakupování může být zábava a ulehčit spoustu práce

https://chat.openai.com/auth/login

BEZPEČNÉ STRÁNKY

dají se vůbec poznat?

Zde jsou některé kroky a znaky, které vám mohou pomoci určit, zda je online obchod bezpečný:

webovoá adresa (URL)

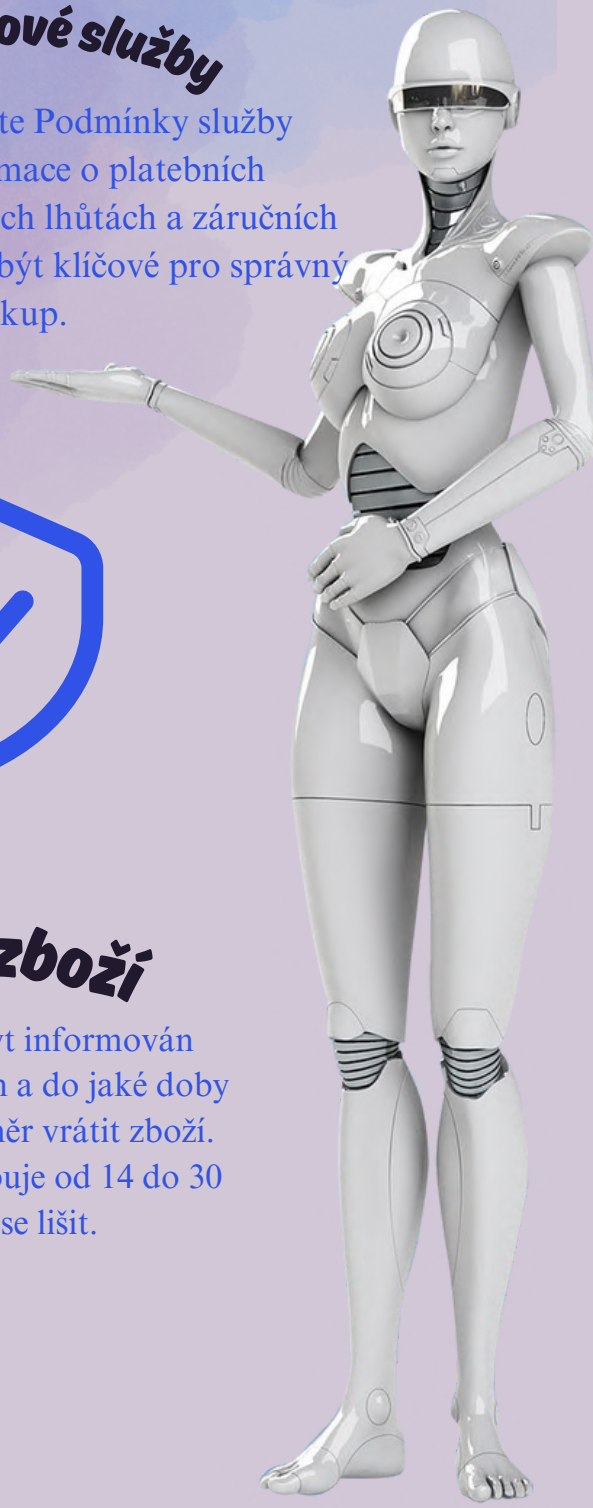
Bezpečné webové stránky začínají "https://" namísto "http://" Písmeno "s" označuje šifrovanou připojení, což je důležitý bezpečnostní prvek

recenze a diskuse

Hledejte recenze a zkušenosti ostatních zákazníků na recenzních portálech nebo diskusních fórech. To vám může poskytnout představu o pověsti obchodu.

podmínkové služby

Detailně si přečtěte Podmínky služby obchodu. Informace o platebních podmínkách, dodacích lhůtách a záručních podmínkách mohou být klíčové pro správný nákup.



kontaktní informace

Zkontrolujte, zda jsou na webové stránce uvedeny správné kontaktní informace, jako jsou adresa, telefonní číslo a e-mail. Seriózní obchody mají obvykle jasné kontaktní údaje

vrácení zboží

Spotřebitel by měl být informován o tom, jakým způsobem a do jaké doby musí oznámit svůj záměr vrátit zboží. lhůta se obvykle pohybuje od 14 do 30 dnů, ale může se lišit.

Pokud máte stále pochybnosti, mějte vždy na paměti, že je lepší vyhnout se podezřelým obchodům a nakupovat u důvěryhodných a známých prodejců.

https://chat.openai.com/auth/login

STAŇ SE CYBERMANEM

1. **Jaký typ hesla je nejlepší pro bezpečné online nakupování?**

a) 12345
b) nakupovani
c) ShoppingQueen83
d) 6Xrd6K9t

2. **Měli bychom brát ohled na recenze?**

a) ano, můžeme předejít podvodnému nákupu
b) ne, lidé na internetu si vymýšlí
c) ne, protože jsou automaticky generovány
d) ne, přeci máme vlastní názor

3. **Co dělat, když váš internetový obchod vám posílá denně e-maily s nabídkami a vám se to nelíbí?**

a) budu jim na maily odpovídat a oni přestanou
b) ignorovat e-maily
c) v nastavení souhlasů vypnu možnost zasílání obchodních sdělení
d) nahlásím podnik na policii

4. **Co je "malware"?**

a) zkratka pro moderní umění.
b) zkratka pro škodlivý software, který může poškodit nebo získat neautorizovaný přístup k počítači nebo síti.
c) válka, která se konala v online světě
d) internetový prohlížeč

5. **Kam si poznamenat heslo k telefonu?**

a) dát si lísteček za kryt telefonu
b) napsat si heslo do poznámek telefonu
c) nedávat si heslo, když si ho nepamatuju
d) heslo si nikam nezapisuji, zvolím si takové, které nezapomenu

6. **Proč je nutné dělat průběžné aktualizace softwaru?**

a) aktualizace zahrnují opravy chyb a zlepšení bezpečnosti, což chrání před potenciálními hrozbami
b) vždy mi to zlepší výkon foťáku
c) když aktualizaci neprovedu, dostanu pokutu
d) pro zlepšení výkonu hardware

správné odpovědi naleznete v příštím vydání!

BYL JSEM OKRADEN

Zbavte se pocitu bezradnosti:
Co dělat, když Vás někdo okrade

Okradli Vás někdy?
Máme pro vás několik klíčových tipů, jak rychle a efektivně jednat.

Změna Hesla:

- Okamžitě změňte heslo ke všem svým online účtům, včetně těch, které byly zasaženy.

Kontakt na banku:

- Pokud byla zasažena finanční transakce, okamžitě kontaktujte svou banku nebo vydavatele kreditní karty a informujte je o situaci.

Oznamování podvodu:

- Oznámit podvodní pokusy na online platformě, kde k nákupu došlo. Mnoho obchodů a platebních bran má mechanismy pro oznamování podvodů.

Nahlášení na Policii:

- Pokud jste obětí kriminální činnosti, včetně online podvodu, měli byste tuto situaci nahlásit místní policii. Poskytněte jim co nejvíce informací.

Aktualizace antivirového a antimalwarového software:

- Ujistěte se, že máte nainstalovaný aktualizovaný antivirový a antimalwarový software na svém zařízení a provedete úplný sken pro potenciální škodlivý software.

Monitorování bankovních výpisů a transakcí:

- Pravidelně sledujte své bankovní výpisy a monitorujte všechny transakce, aby bylo možné okamžitě identifikovat další podezřelé aktivity.

Získání pomoci od odborníka na kybernetickou bezpečnost:

- Pokud máte podezření, že vaše zařízení bylo kompromitováno, nebojte se požádat o pomoc odborníka na kybernetickou bezpečnost pro důkladné vyšetření.

Podvod na internetu vynesl dvěma mladíkům 1,5 milionu korun. Teď půjdou do vězení

Mladíci podvedli 651 lidí, hrozí jim vězení až 8 let! Z falešných profilů na FB a Marketplacu prodávali herní konzole, telefony a chytré hodinky

Platba předem se nevyplatila. E-shop s levnou elektronikou byl podvod

Podvodník na internetové stránce top-elektro.cz prodával elektrospotřebiče a vydával se za ověřeného prodejce

Podvodnice nabízela štěňata i elektroniku, zájemce připravila o 270 tisíc!

Kriminalisté dopadli mladou ženu z Prahy, která si nechávala předem zaplatit, ale zákazníkům nikdy nic neposlala. Zakládala si různé účty a telefonní čísla, aby bylo složité ji vystopovat.

Policie řeší podvodné e-shopy s elektrem. Neznámý pachatel od lidí vylákal téměř půl milionu korun

Za sedm dní fungování portálu Hurá elektro vylákal uprostřed léta od 28 zájemců více než 200 tisíc korun. Skoro stejný počet zákazníků internetového obchodu Prostě elektro přišel v listopadu stejným způsobem během čtyř dnů fungování portálu skoro o 250 tisíc korun.

Podvodník prodával značkovou elektroniku, za inkasované peníze zboží ale nedodal

Ne e-mailové adresy lidem rozposílal nabídky s elektronikou. Mladíka dopadli hradečtí policisté a nyní mu hrozí až 8 let vězení.

zdroj informací:
https://www.idnes.cz/
https://www.chip.cz/
https://www.irozhlas.cz/
https://hradecky.denik.cz/

Časopis CyberGuard vypracovali studenti 3. ročníku Veřejné správy v Hradci Králové

NetGuard minulé vydání Průvodce influencerství a sociálními sítěmi

CyberGuard

FitGuard příští vydání Průvodce zdravým životním stylem

Na závěr Vám s radostí představujeme svět Ochrany a Digitální Bezpečnosti.
Jsme Natálie, Adéla a Dennis, studenti Obchodní Akademie se zaměřením na Veřejnou správu. V tomto čísle časopisu jsme se s Vámi podělili o inspirativní průvodce, které Vás provedly klíčovými aspekty digitální bezpečnosti. Doufáme, že Vás naše články nejen zaujaly, ale také vám poskytly užitečné nástroje pro bezpečné pohybování se online světem. Děkujeme vám za Váš zájem a těšíme se, že nás budete sledovat i v následujících číslech našeho časopisu.

Natálie Tokárová
Adéla Radáková
Dennis Poul

zdroj obrázků robotů: https://www.pngwing.com/en/search?q=ROBOT