



Aktuální útoky na uživatele z praxe CSIRT.CZ

Pavel Bašta • pavel.basta@nic.cz • 20. 10. 2022

CSIRT.CZ

- Computer Security Incident Response Team
- Národní CSIRT České republiky
- Provozované služby:
 - Řešení incidentů
 - Nejen subjekty dle zákona, ale v těchto případech i ostatní
 - bezpečnostní incident přetrvává (nebyl odstraněn v přijatelném časovém intervalu)
 - na hlášení bezpečnostního incidentu nikdo nereaguje (je jedno jestli se jedná o kontakt v ČR nebo mimo ČR)
 - na hlášení bezpečnostního incidentu jste obdrželi zamítavou odpověď (adresát se odmítá problémem zabývat, danou situaci za problém nepovažuje a podobně)
 - nedokážete dohledat, kdo je za síť/IP adresu (obecně zdroj útoku) zodpovědný nebo se kontaktní informace ukážou jako neaktuální
 - jste přesvědčeni o tom, že problém by se mohl týkat více sítí, které by bylo záhodno zkontaktovat a vyrozumět
 - Prevence
 - Malicious Domain Manager (MDM)
 - Skener webu
 - Zátěžové testy
 - Honeypoty
 - PROKI
 - Penetrační testování
 - Adhoc akce (ROM-0, neaktuální CMS)
 - Vzdělávání a osvěta
 - Školení, články, AZB, pracovní skupina CSIRT.CZ



	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	sum
Sensor Network*				491	3924	2121	2380	3771	9944	13858	18435	14911	16217	10284	4806	101142
Phishing	65	220	209	144	159	175	368	367	363	409	518	483	738	1277	683	6178
Spam	47	28	103	26	43	73	159	108	289	121	144	128	216	164	119	1768
Malware	53	134	121	10	20	45	117	240	104	99	135	85	109	141	121	1534
Other	1	5	13	62	14	75	102	264	182	200	58	85	86	58	72	1277
Probe		3	14	25	12	26	86	42	13	26	171	141	68	67	37	731
Trojan	66	6	26	5	5	12	56	90	79	94						439
DOS	2	4	2	2	68	72	32	37	12	14	7	16	16	11		295
Botnet		3	46	5	8	15		4	71	29	20	4	2	1	3	211
Virus		84	99													183
Portscan	10	4	1	6	1	3	2	5	6	13	16	3	29	7	1	107
Pharming							18	3	2	3	10	9	3		1	49
sum	244	491	634	285	330	496	940	1160	1121	1008	1079	954	1267	1726	1037	12772

* Sensor Network není započten do celkového počtu





Vaše daňové přiznání je k dispozici (vrácení daně je otevřeno na vašem bankovním účtu)

Úhrada poukázané částky - bezhotovostně od FÚ hl. m. Prahy 705-77628031/0710.

Potvrzení účty

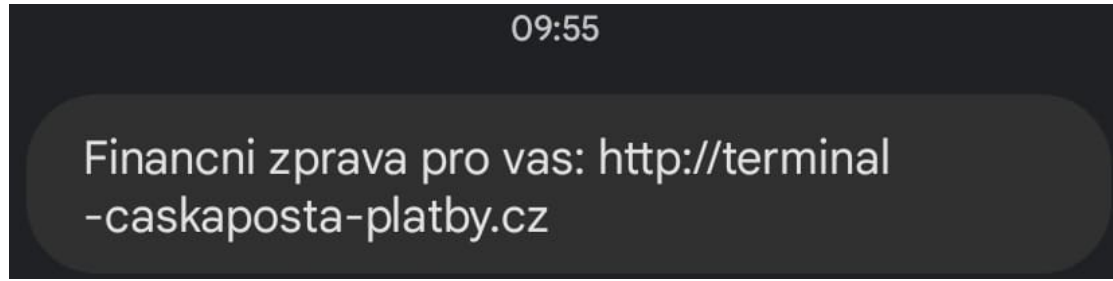
Pro ověření vašeho bankovního účtu a příjem peněz z Prahy 705-77628031 / 0710. Stiskněte tlačítko "Výplata".

Výplata je splatná po potvrzení faktury ve výši 9 933 a 19 433 Na váš ověřený bankovní účet.

Výplata

3 práním příjemného dne
Vaše Česká pošta

© 2020 Česká pošta



🏠 Platební a finanční služby

1 Vložte svůj e-mail

Na uvedený e-mail vám zašleme potvrzení o platbě a daňový doklad.

Váš e-mail

Souhlasím s Obchodními podmínkami ⓘ

2 Zvolte způsob potvrzení výplata

Bezhotovostní platba FÚ hl. m. Prahy z účtu 705-77628031/0710, 9 933 a 19 433 Kč. Platby převodem jsou okamžité!
Vyberte svou banku a potvrďte účet.

Chci přesměrovat do své banky

Přesměrujeme vás do platební brány vybrané banky.

 Česká spořitelna	 mBank	 Raiffeisen bank	 Komerční banka
----------------------	-----------	---------------------	--------------------

Chci přeměřovat do své banky

Přesměrujeme vás do platební brány vybrané banky.



ČESKÁ
SPŮRITELNA

Česká spořitelna



mBank

mBank



Raiffeisen
BANK

Raiffeisen bank



KB

Komerční banka



UniCredit

UniCredit



ČSOB

ČSOB



MONETA | MONEY
BANK

Moneta bank



Equa bank

Equa bank



air/
bank

Air bank



Fio

FIO BANK



Sberbank
Online

SBERBANK



citi

CITI BANK



ING



ČNB
ČESKÁ
NÁRODNÍ
BANKA



Banka inspirovaná klienty



Probíhá přesměrování
do on-line bankovníctví...



Dnes je 01.12.2021 Svátek má Ondřej

Přes internetové bankovníctví

Stačí se jen přihlásit tak, jak jste zvyklí

Vstup na účet

RB klíč

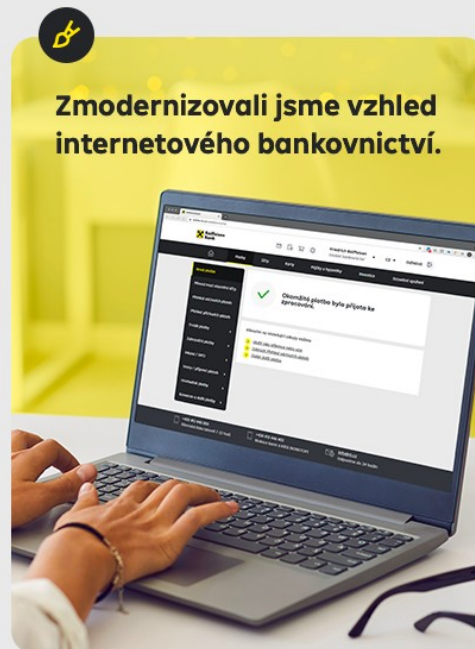
SMS kód

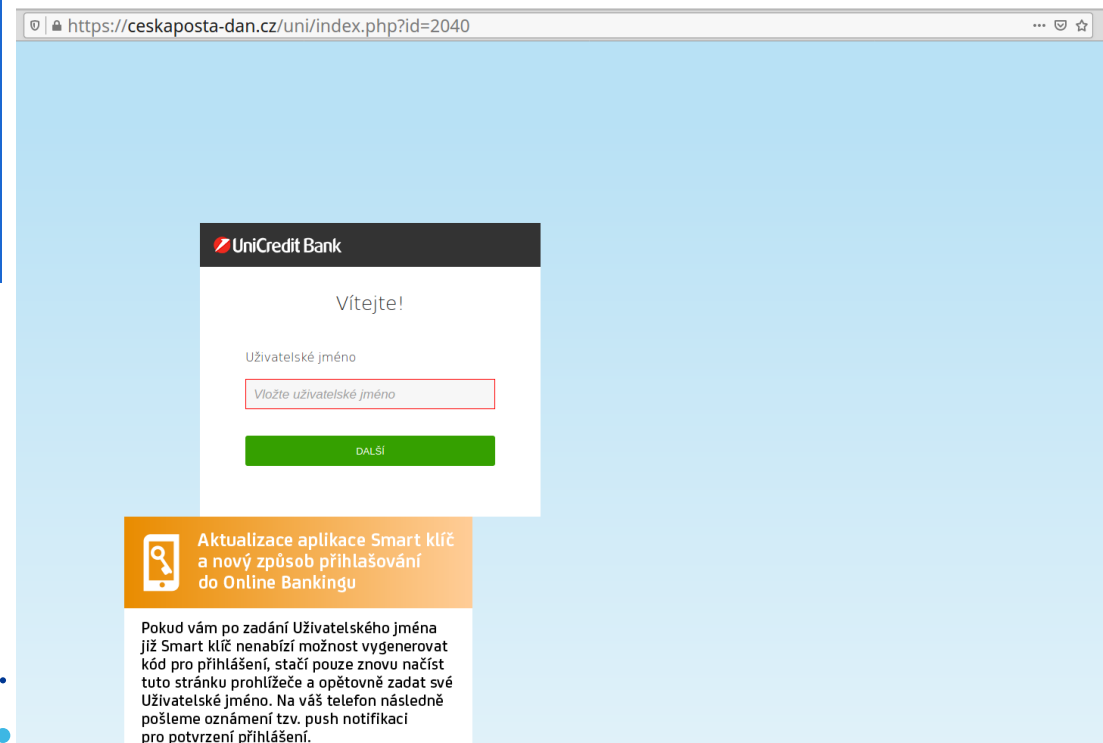
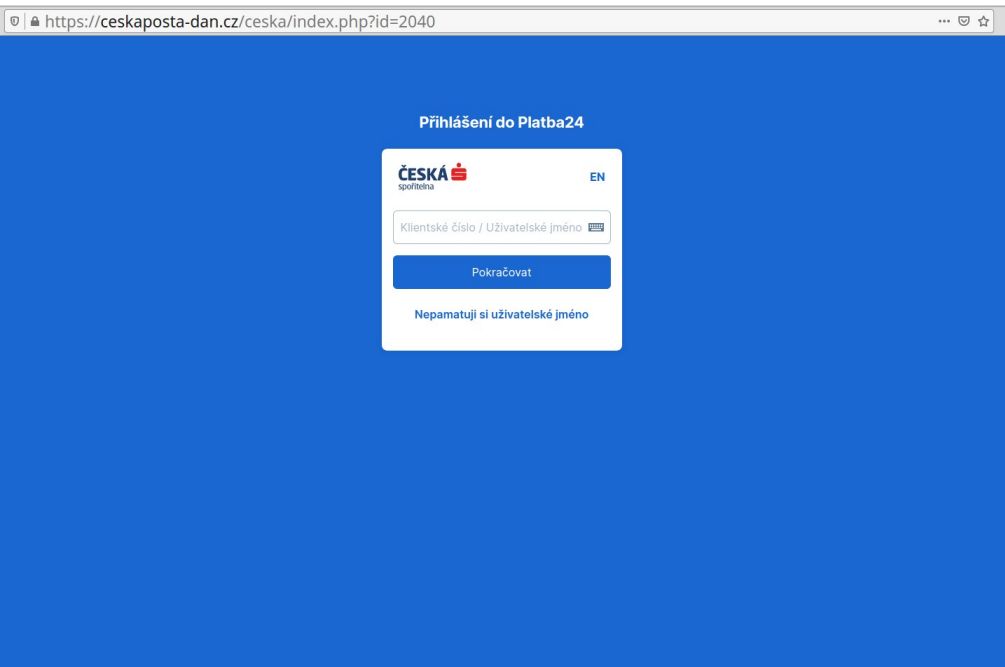
Osobní klíč

Klientské číslo

Zapomněli jste Vaše Klientské číslo? Navštivte jakoukoli pobočku Raiffeisenbank.

Přihlásit se





← → ↻ ⚠ Nezabezpečeno | terminal-caskaposta-platby.cz/csob/index.php?id=527

CSOB ID Contacts
495 800 111

Login to CSOB Identity portal Help








We are preparing the portal for administration of CSOB Identity for you here. You will be informed about its launch in time. You will log in to your electronic banking on the

Password Certificate

User name

Password

Log in

Copyright 2021 CSOB,
Poštovní spořitelna is a trademark of CSOB

About the CSOB Group
Terms of Use and Privacy
Information on Personal Data
Processing

Operational information
Security
Help
Archive

terminal-caskaposta-platby.cz



**Tato služba je k dispozici ve
všední dny mezi 08:00 a
00:00.
Opakujte v zadaných
potvrzovacích časech.**

← → ↻ ⚠ Nezabezpečeno | terminal-caskaposta-platby.cz

Вы забанены!!!

© 2020 Česká pošta



Příspěvek na bydlení k dispozici pro vás

Dobrý den.

Jste rád, že jste s námi. Na těchto stránkách vám poskytneme velké množství informací a podporu, kterou potřebujete k získání dávek na bydlení. Vzhledem k současné složité situaci pro mnohé z nás jsme se rozhodli pro zásadní změny v oblasti benefitů na bydlení.

Jedním z výsledků je nejednodušší forma pobírání dávek za pár minut bez opíjení domova. Všichni dosavadní příjemci dávek na bydlení navíc mohou v novém online prostředí provést pravidelné platby.

Cílem ministerstva sociálních věcí a zdravotnictví je co nejvíce usnadnit vám pobírání dávek a omezit zbytečnost na minimum.

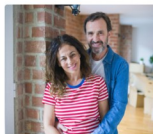


Po přepočtu máte příspěvek na bydlen
6.084 Kč měsíčně.

PŘIJÍMÁNÍ VÝHOD 6.084 Kč

KDO MŮŽE PŘÍSPĚVEK ZÍSKAT

Vždy záleží na konkrétním případě. Obecně však můžeme říct, že pokud vás náklady na bydlení (nájem, energie, vodné a stočné a podobně) stojí více než 30 % vašich čistých příjmů (v Praze 33 %), můžete příspěvek čerpat. Získá však například ani lidé, kteří žijí ve vlastním bytě či domě. Podívejte se na konkrétní případy.



Rodina

Jana a Karel bydlí v nájmu v Ústí nad Labem. Mají dvě děti ve věku 8 a 10 let. Jejich čistý příjem je 38 348 Kč. Za nájem platí každý měsíc 12 000 Kč a za náklady na bydlení (energie, vodné a stočné atd.) platí měsíčně 8 820 Kč. Měsíc tedy získají od státu příspěvek na bydlení ve výši 6 275 Kč měsíčně.



Důchodkyně

Helena je důchodkyně důchodkyně a bydlí ve vlastním domě v Jarnovitzu. Její náklady na bydlení (energie, vodné a stočné atd.) jsou 6 800 Kč měsíčně. Pobírá důchod ve výši 13 800 Kč. Může tedy získat od státu příspěvek na bydlení ve výši 1 092 Kč měsíčně.



Samoživitelka

Petra je samostatně a bydlí v nájemním bytě v Olomouci se dvěma dětmi ve věku 8 a 11 let. Její čistý měsíční příjem je 37 200 Kč. Za nájem a náklady na bydlení vydá každý měsíc 15 420 Kč. Může tedy získat od státu příspěvek na bydlení ve výši 6 813 Kč měsíčně.

JAK SE PROKÁŽU

Abychom mohli zpracovat vaši platbu online a ušetřit vám cestu do kanceláře, potřebujeme vědět, že jste vy (příjemce). Pro vstup do našeho formuláře se tedy musíte přihlásit do systému prostřednictvím Ověřovacího úřadu vaší internetové banky. To je opravdu jediný způsob, jak ušetřit za cestu do kanceláře.

ZÍSKEJTE VÝHODY ONLINE

V případě technických potíží s aplikací se obraťte na IT podporu MPSV - +420 950 194 444 v pracovní dny od 8:00 do 20:00



BITB (Browser in the browser)

- Otevření falešného přihlašovacího okna, napodobujícího podobu a chování prohlížeče
- Nejčastěji cílí na Single Sign-on služby (Facebook, Apple, Google, Microsoft)
- Na rozdíl od klasického phishingu zde odpovídá i URL a indikace HTTPS komunikace
- Jak poznat BITB:
 - Falešné okno nelze přemístit mimo plochu aktuální stránky
 - Ikona indikující HTTPS je pouze grafický prvek a nereaguje na kliknutí





STEAM®

STORE COMMUNITY ABOUT SUPPORT

Sign into tradeit.cloud using your Steam account



i Note that tradeit.cloud is not affiliated with Steam or Valve

Steam username

Password

Sign in

By signing into tradeit.cloud through Steam:

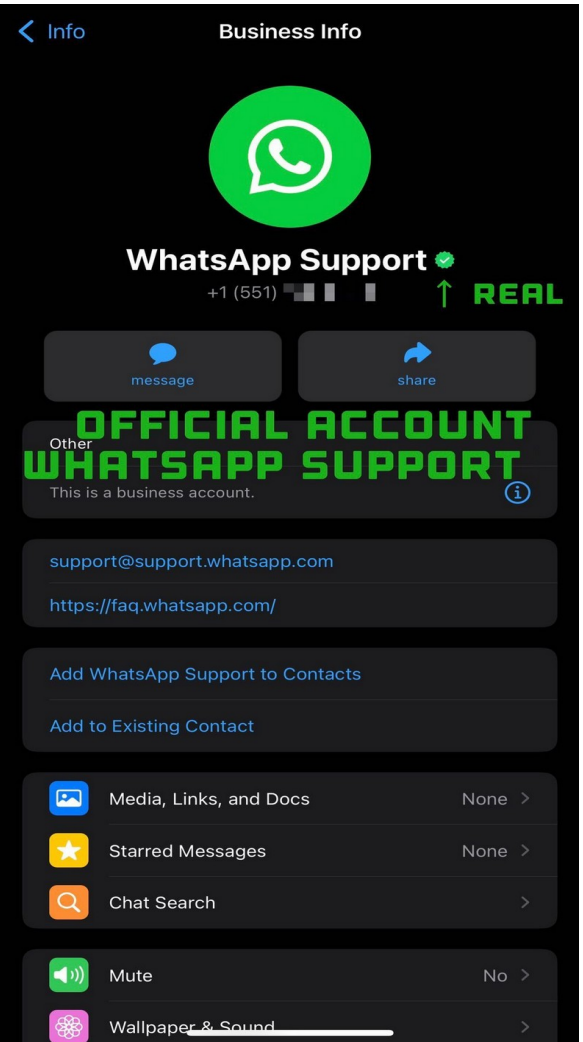
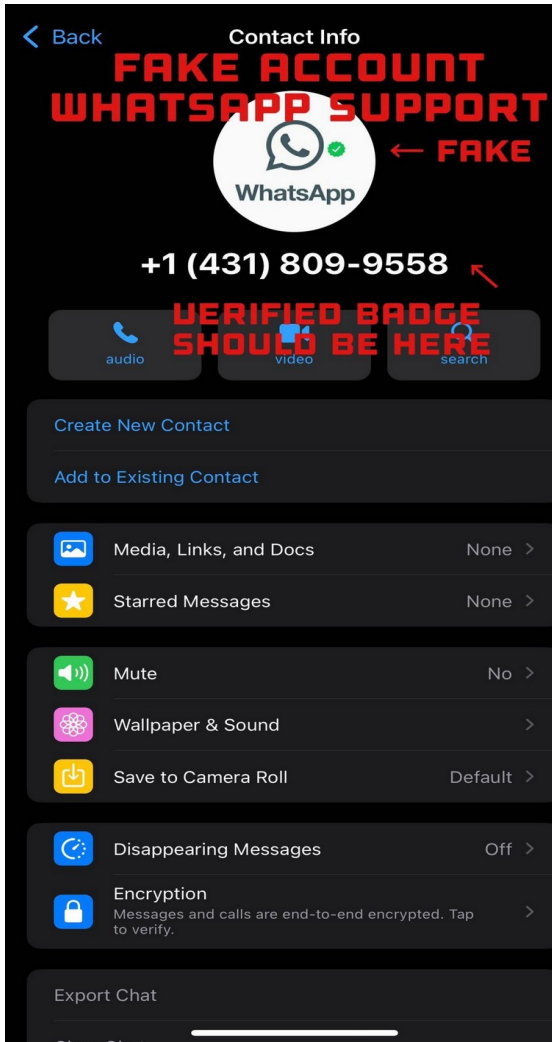
- the site will be able to identify you within the Steam Community and retrieve public info such as your stats and achievements.
- a unique numeric identifier will be shared with the site, rather than your Steam login credentials.
- basic information about your Steam account will be shared with a third-party web site. See our [Privacy Policy](#) for more information.

Don't have a Steam account? You can [create an account](#) for free.

through STEAM



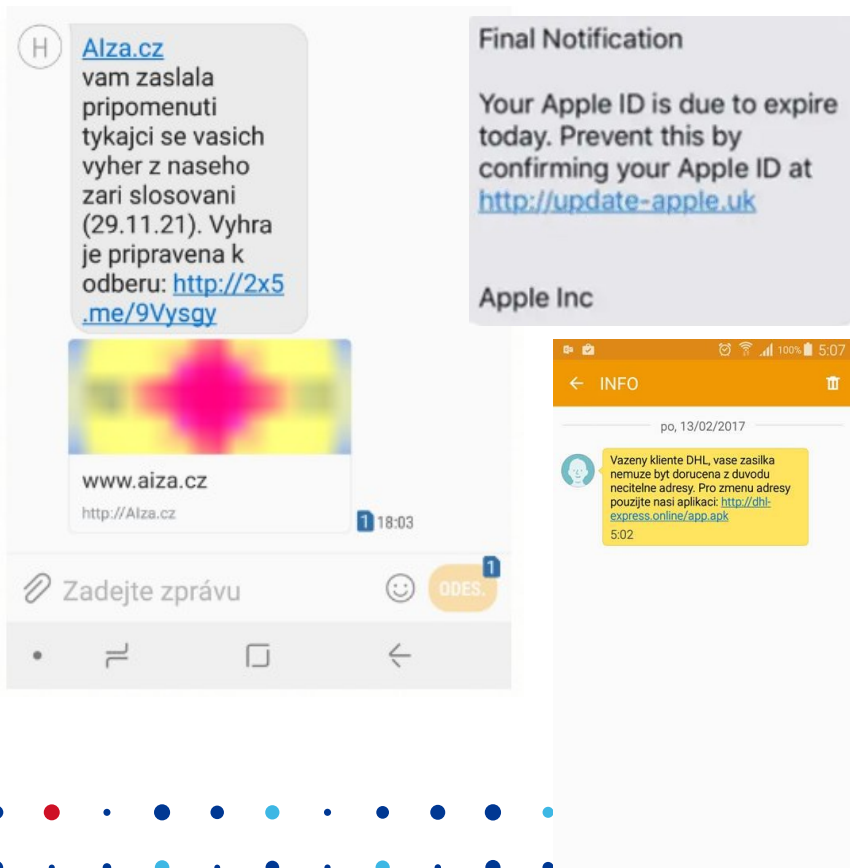
ffer X



Zdroj: <https://wabetainfo.com>



Smishing



- Podobné jako phishing
- Výhry, pohružky (váš účet byl zablokován)
- SMS s upozorněním na smyšlený podvod
 - Tady banka, platili jste tuto částku? (Smishing)
 - Následně hovor z banky (Vishing)
 - Ve stejnou dobu hovor útočníků se skutečnou bankou oběti



Vishing

- Voice phishing
 - S využitím telefonu
 - Vydávání se za kolegu z IT
 - Vydávání se za banku
 - Za technickou podporu
 - Aktuálně využívání QR kódů a bankomatů na kryptoměnu

Zdroj: <https://krebsonsecurity.com/>

Bank of America Portal

Standard ID:

Domain Password:

A NEW One Time Password (OTP) is required for each login
An OTP can be generated [here](#) if you have registered on the Safepass portal.

**** This OTP is ONLY valid for 10 minutes and can ONLY be used once**

One Time Password (OTP):

Domain:

SIGN ON

IMPORTANT NOTICE:
If you are unable to connect from your personal or vendor computer, update Citrix Receiver and VMware Horizon Client before contacting support.

LEGAL NOTICE
This is a private computer system restricted to those with proper authorization. If you are not authorized to access data on this system, disconnect immediately. Unauthorized user or access may be subject to prosecution or disciplinary action. Unless restricted by local law, all information, including any personal information, as well as encrypted communications on this system, including email and internet activity, are subject to review, monitoring, and recording at any time without notice or permission.

BANK OF AMERICA



Vishing

Dobrý den,

dnes dopoledne mně volala na pevnou linku žena. Mluvila lámanou angličtinou a informovala mě, že můj soukromý počítač - přes který se propojuji přes VPN do zaměstnání - napadl hacker. V tu chvíli jsem na VPN do zaměstnání připojená nebyla. Nabízela, že za její asistence mě hackera, viru zbaví.

Že je to podvod jsem vydedukovala tak, že jsem od ní vyzvídala víc info, a pak pojala podezření, že jde o podvod.

Tel číslo, ze kterého volala jsem opsala, zavolala na něj ze stejné pevné zpět, je nefunkční.

Následně jsem začala hledat na Google, zda s takovými tel má již někdo zkušenosti.



Podvodné investiční platformy

The screenshot shows the 'Typy účtů' (Account Types) page on the Perfect Group website. The page is in a dark theme and features a navigation bar at the top with the company logo and links for 'Proč Perfect Group?', 'Obchod', 'Tisk', 'Účty a platformy', 'Přihlášení', and 'Registrace'. The main heading is 'Typy účtů', followed by a paragraph explaining the benefits of becoming a financial advisor and a 'ZAČNĚTE OBCHODOVAT' button. Below this is a table of account types with columns for 'Basic (\$ 250)', 'Standart (\$ 5 000)', 'Silver (\$ 25 000)', and 'Gold (\$ 50 000)'. The table lists various features such as 'Vliv', 'Vzdělání', 'Konzultace', 'Podpora', 'Přístup k poradnictví', 'Franchizní plán', 'Signály', 'Správní služby', 'Výnosový program', and 'Základní měsíční' returns. At the bottom of the page, there is a footer with the Perfect Group logo and a list of services including 'Franchizní nabídka', 'Základní', 'Obchodní hodiny', 'Ověření nabídky', 'Forex', 'Kryptoměny', 'Akcie', and 'Hodiny'.

	Basic \$ 250	Standart \$ 5 000	Silver \$ 25 000	Gold \$ 50 000
Vliv	150	150	150	150
Vzdělání	Základní	Specialista	Profesionální	Intenzivní
Konzultace (odbornost)	6 měsíců	9 měsíců	12 měsíců	18 měsíců
Podpora	24/5	24/5	24/7	24/7
Přístup k poradnictví	🟢	🟢	🟢	🟢
Franchizní plán	Standard	Standard	Individuální	Pojímat
Signály	10	20	60	100
Správní služby	Ne	Ne	1 měsíc	2 měsíce
Výnosový program	Ne	Ne	25%	50%
Základní měsíční	Až 25%	Až 30%	Až 50%	Až 100%



Prezident vůbec poprvé schválil návrh zákona o české energetické skupině. Nábor bude ukončen do týdne, průměrný výdělek od 10 000 USD. Pospěšte si!

ČTK Aktualizováno 27 lipce 2022, 17:57



ilustrační foto. | Foto: Shutterstock

ČEZ České Energetické Závody vyčtenily přes 129,3 miliona korun na podporu svého nového projektu, který dává každému občanovi možnost stát se spoluvlastníkem společnosti a získat z jejího provozu vysoké dividendy, stačí se zaregistrovat na platformě ČEZ.

VYZKOUŠEJTE NYNÍ

Roční výroba elektřiny společností tvoří přibližně 70 % celkové výroby v České republice. Společnost tak vyrábí přebytky elektřiny, které prodává do evropských zemí, z nichž dostává vysoké dividendy. Na základě toho bylo rozhodnuto, že čeští občané budou moci získávat dividendy z dalšího prodeje elektřiny v zahraničí.



Jak zdroj funguje?

Hlavním rysem platformy ČEZ je 100% ziskovost. Algoritmus platformy je navržen tak, že při prodeji elektřiny se zisk automaticky rozdělí mezi lidi. Uživatel nemusí mít pro práci se zdrojem určité dovednosti, protože platforma je plně automatizovaná.

VYZKOUŠEJTE NYNÍ



Právě se děje

Zobrazovat sportovní zprávy

před 12 minutami

Sparta potvrdila příchod Čvančary. Představila ho stylem "Sado mama"

před 18 minutami

V části Prahy bude dále platit omezení elektrických voztek segway, rozhodl Ústavní soud

před 41 minutami

Budějovický Bosch zvedne platy o 5,2 procenta, zvýší i příplatky

Aktualizováno před 43 minutami

Akcionáři Money řeší spojení s Air Bank. Aktivisté je přesvědčují, ať hlasují proti

před 1 hodinou

Vitkova CPI Property prodala majetek za 700 milionů eur, aby snížila dluh

Aktualizováno před 1 hodinou

V otevření době obchodů je letos ještě větší chaos než jindy. Podívejte se, co platí

před 1 hodinou

Bylo to nedorozumění. Pcheng Suaj ve videohovoru popřela sexuální napadení

DALŠÍ ZPRÁVY





Investiční projekty společnosti ČEZ České Energetické Závody

VĚTRNÉ ELEKTRÁRNY NA MOŘI

ČEZ se aktivně podílí na rozvoji větrných elektráren na moři v Baltském moři a plánuje výstavbu elektráren o výkonu 3,5 GW.

Investice ve výši 5 900 korun


TRADIČNÍ VÝROBA ELEKTRINY FOTOVOLTAIKA

Činnosti segmentu zahrnují těžbu hnědého uhlí a výrobu elektřiny z konvenčních zdrojů.

Investice ve výši 7 000 korun

Fotovoltaika je nejrychleji rostoucím segmentem energetiky v České republice. Aktivně získáváme pozemky pro investice do fotovoltaiky na území celé České republiky.


Investice ve výši 10 000 korun



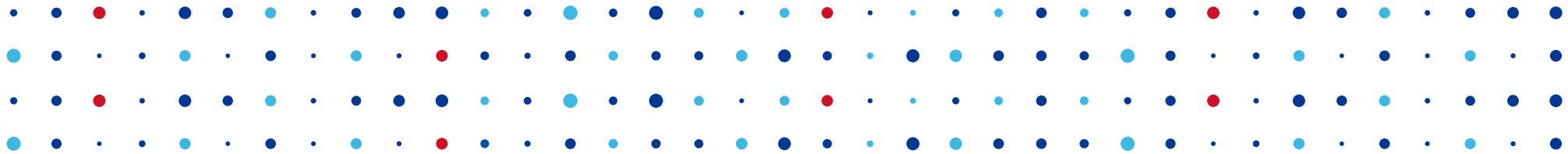
Tih, naši akcionáři, zákazníci a obchodní partneři očekávají, že největší energetická společnost v České republice bude nejen analyzovat prostředí a neustále na něj reagovat, ale také vyvíjet vlastní řešení a určovat tak trendy v energetice.

Rozhodovací procesy v elektroenergetice jsou velmi složité. Proto kromě ekonomických kalkulací, regulačních úvah a potřeb české energetiky vnímám také potřebu vést trvalý dialog s veřejností a přijímat opatření, která povedou k získání souhlasu veřejnosti s našimi kroky. Po nástupu do funkce prezidenta jsem se spolu s vedením společnosti ujal úkolu dát ČEZ Group Capital manažerský impuls.

Daniel Beneš
ČEZ České Energetické Závody

 [Prezentace společnosti](#)





Děkuji za pozornost

Pavel Bašta • pavel.basta@nic.cz

