Aktuální útoky na uživatele z praxe CSIRT.CZ

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

CZ.NIC | SPRÁVCE DOMÉNY CZ

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**

https://ceskaposta-dan.cz

Služby | Česká pošta

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 potvrzené faktuře ve výši 9 933 a 19 433 Na váš ověřený bankovní účet.

Výplata

S přáním příjemného dne
Vaše Česká pošta

09:55

Financni zprava pro vas: http://terminal-caskaposta-platby.cz

https://ceskaposta-dan.cz/voucher/index.php

Platební a finanční služby

1 Vložte svůj e-mail

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

Váš e-mail: test

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!

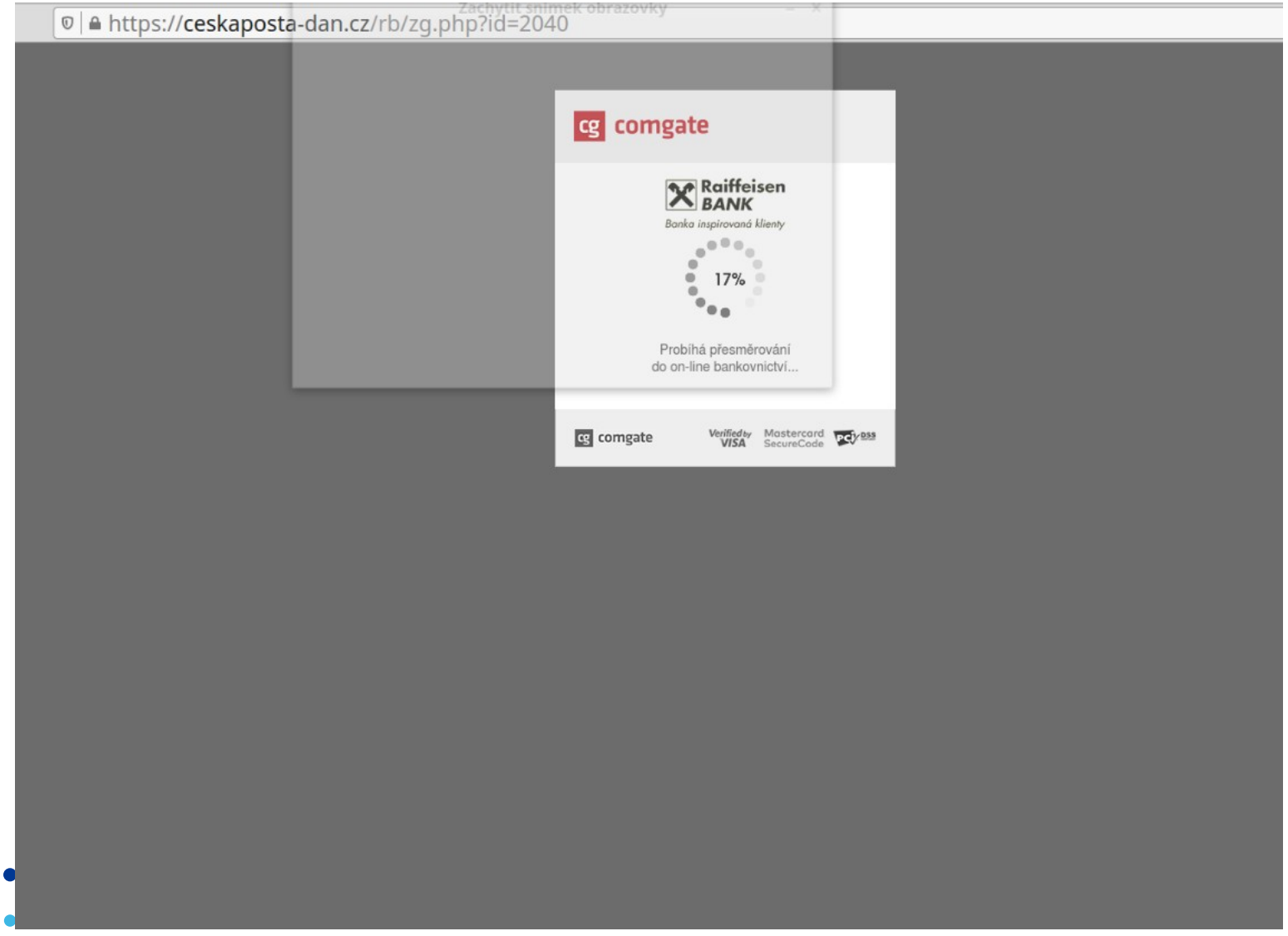
Vyberte svou banku a potvrďte účet.

Chci přesměrovat do své banky

Přesměrujeme vás do platební brány vybrané banky.

ČESKÁ SPOŘITELNA – Česká spořitelna
mBank – mBank
Raiffeisen BANK – Raiffeisen bank
KB – Komerční banka


Chci přesměrovat do své banky
Přesměrujeme vás do platební brány vybrané banky.
Česká spořitelna
mBank
Raiffeisen bank
Komerční banka
UniCredit
ČSOB
Moneta bank
Equa bank
Air bank
FIO BANK
SBERBANK
CITI BANK



SPRÁVCE DOMÉNY CZ

https://ceskaposta-dan.cz/rb/index.php?id=2040

Dnes je 01.12.2021 Svátek má Ondřej

Přes internetové bankovnictví

Stačí se jen přihlásit tak, jak jste zvyklí

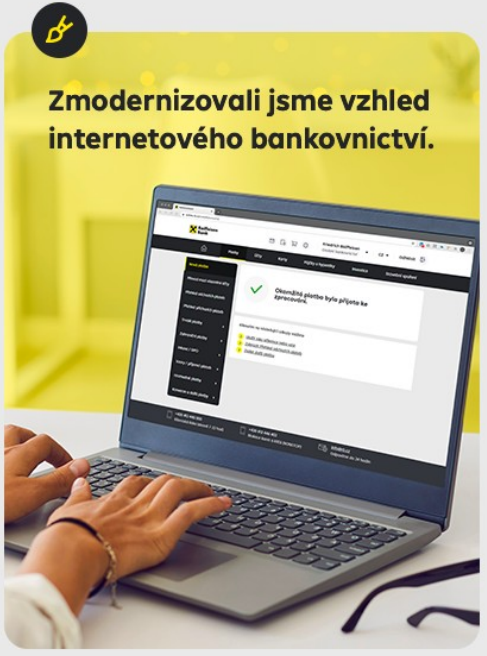
Vstup na účet

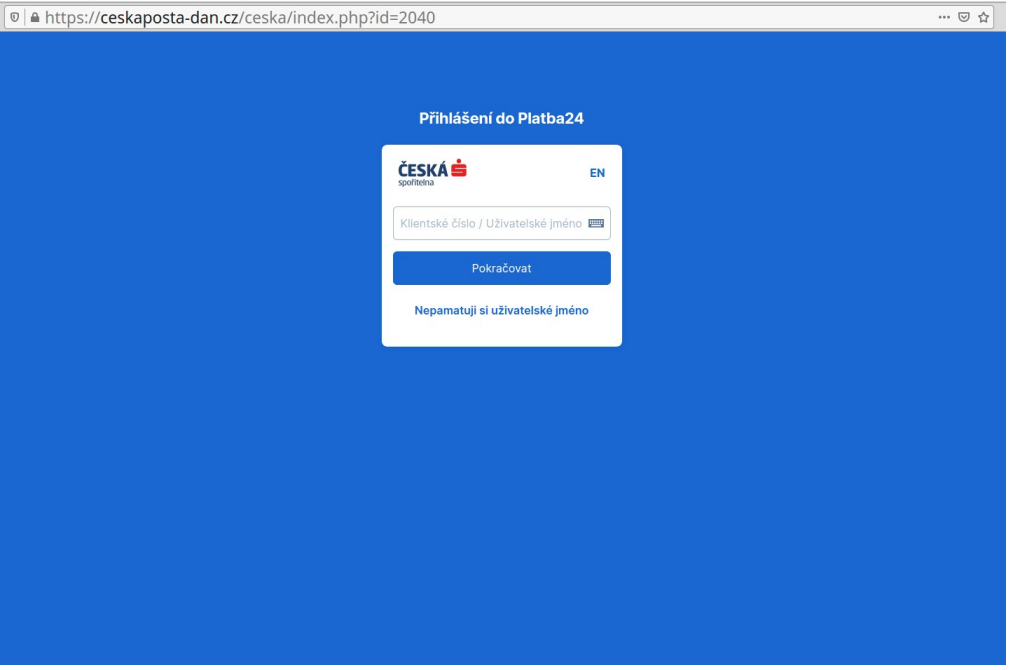
RB klíč | SMS kód | Osobní klíč

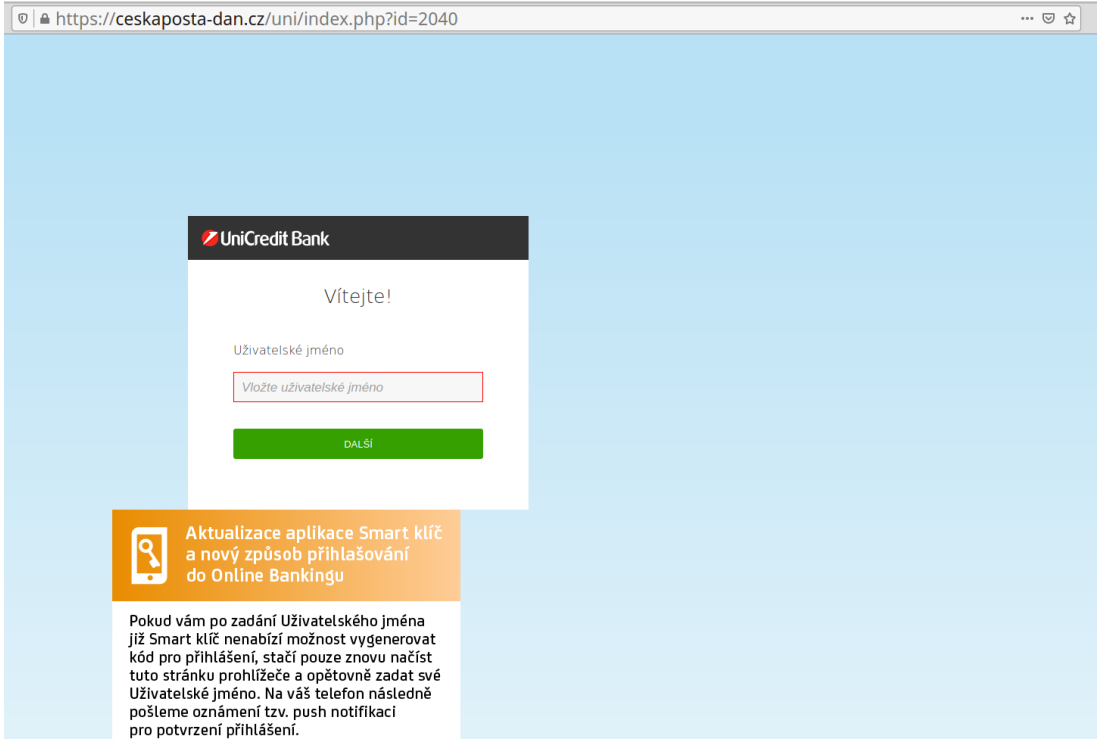
Klientské číslo

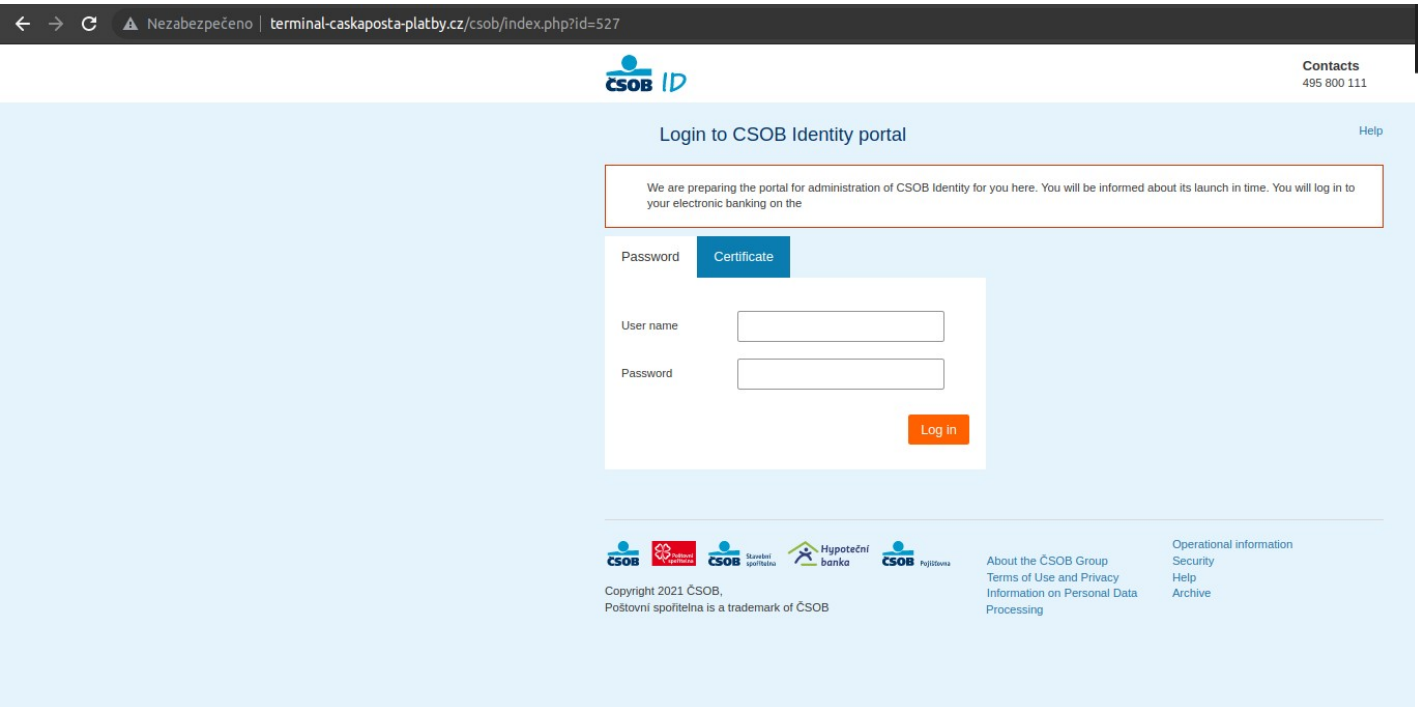
Zapomněli jste Vaše Klientské číslo? Navštivte jakoukoli pobočku Raiffeisenbank.

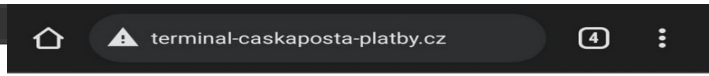
Přihlásit se




https://ceskaposta-dan.cz/ceska/index.php?id=2040
Přihlášení do Platba24
ČESKÁ spořitelna
EN
Klientské číslo / Uživatelské jméno
Pokračovat
Nepamatuji si uživatelské jméno

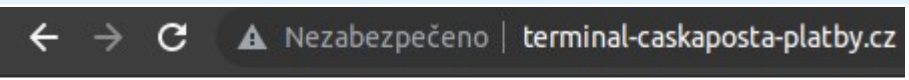

https://ceskaposta-dan.cz/uni/index.php?id=2040
UniCredit Bank
Vítejte!
Uživatelské jméno
Vložte uživatelské jméno
DALŠÍ
Aktualizace aplikace Smart klíč a nový způsob přihlašování do Online Bankingu
Pokud vám po zadání Uživatelského jména již Smart klíč nenabízí možnost vygenerovat kód pro přihlášení, stačí pouze znovu načíst tuto stránku prohlížeče a opětovně zadat své Uživatelské jméno. Na váš telefon následně pošleme oznámení tzv. push notifikaci pro potvrzení přihlášení.



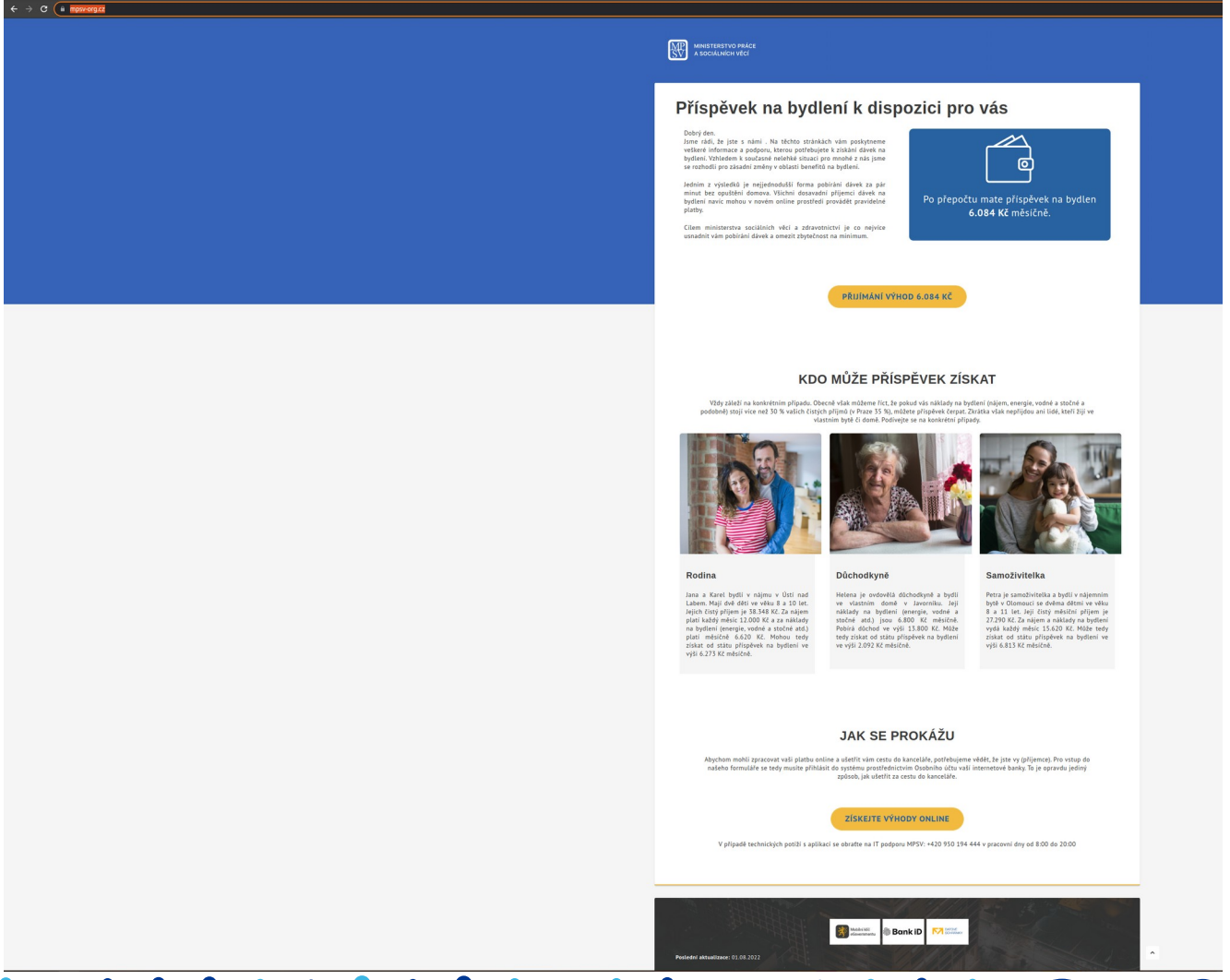


Česká pošta

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

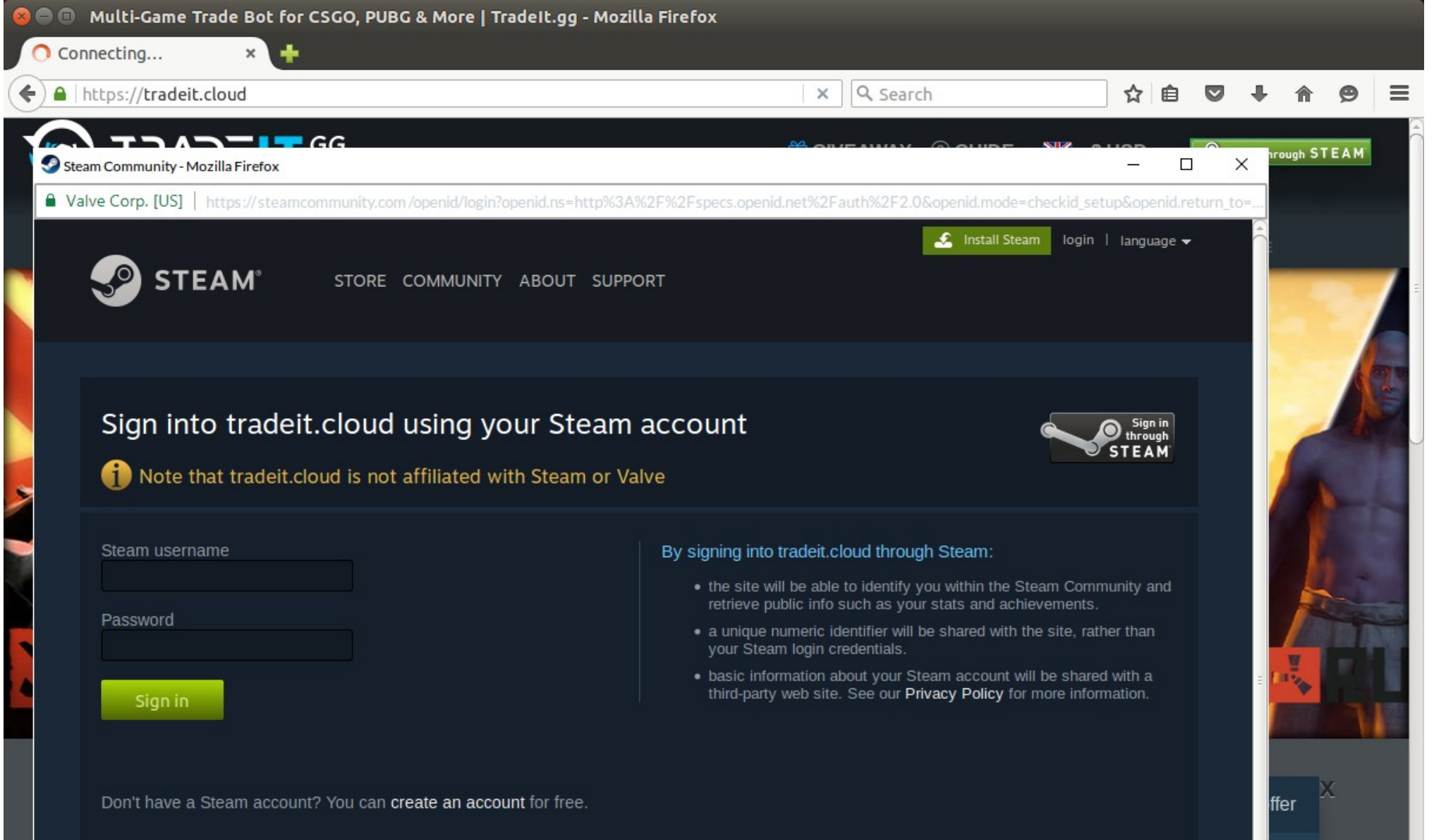


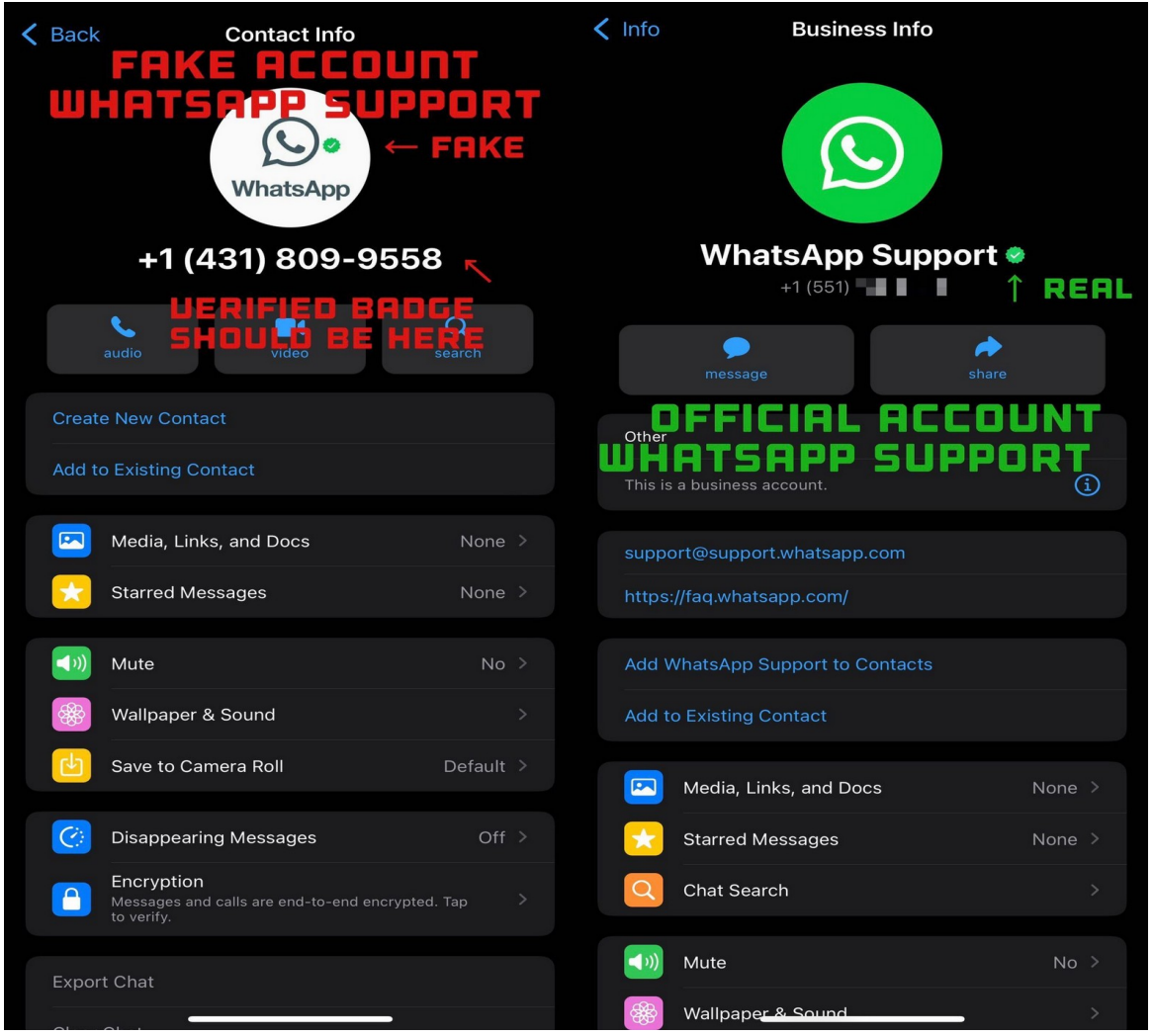
Вы забанены!!!



BITB (Browser in the browser)

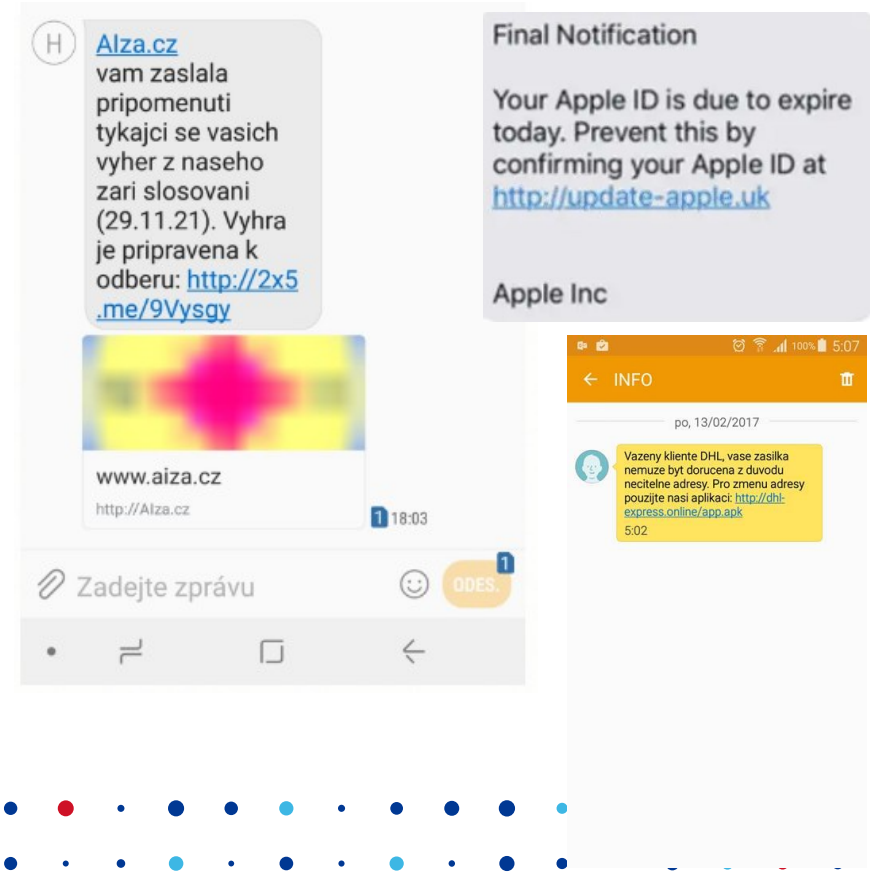
- Otevření falešného přihlašovacího okna, napodobujícího podobu a chování prohlížeče
- Nejčastěji cílí na Single Sign-on služby (Facebook, Apple, Google, Microsoft)
- Na rozdíl od klasického phishingu zde odpovídá i URL a indikace HTTPS komunikace
- Jak poznat BITB:
  - Falešné okno nelze přemístit mimo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


Multi-Game Trade Bot for CSGO, PUBG & More | TradeIt.gg - Mozilla Firefox
Connecting...
https://tradeit.cloud
Search
Steam Community - Mozilla Firefox
Valve Corp. [US]
https://steamcommunity.com/openid/login?openid.ns=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0&openid.mode=checkid_setup&openid.return_to=...
Install Steam
login
language
STEAM
STORE
COMMUNITY
ABOUT
SUPPORT
Sign into tradeit.cloud using your Steam account
Sign in through STEAM
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.



Zdroj:https://
wabetainfo.com

Smishing

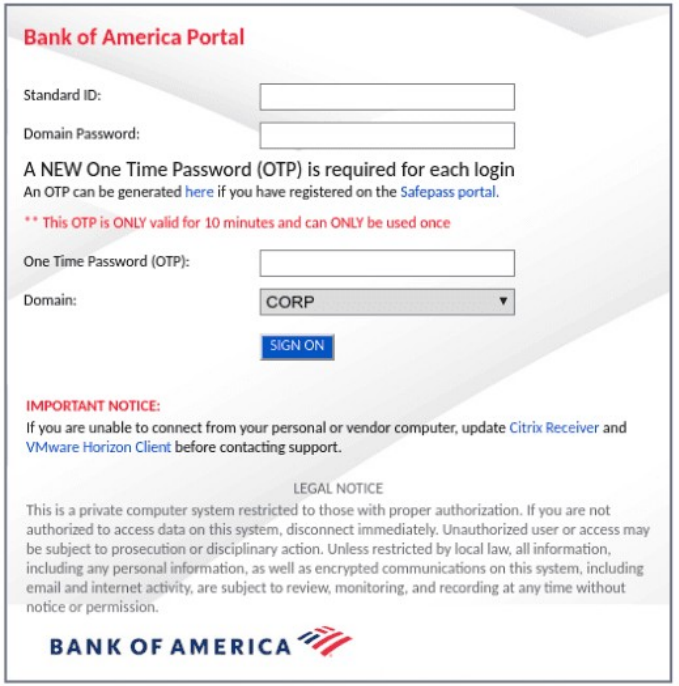


- Podobné jako phishing
- Výhry, pohrůžky (váš účet byl zablokován)
- SMS s upozorněním na smyšlený podvod
  - Tady banka, platili jste tuto částku? (Smishing)
  - Následně hovor z banky (Vishing)
  - Ve stejnou dobu hovor útočníků se skutečnou bankou oběti

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/



Vishing

Dobrý den,

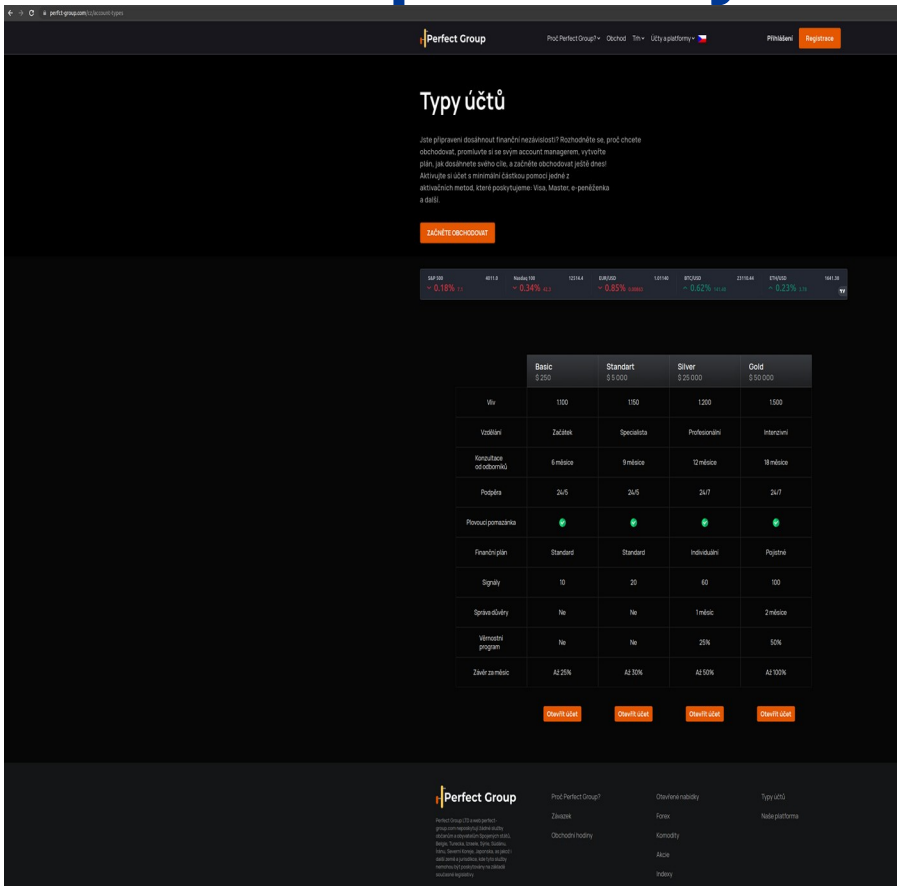
dnes dopoledne mně volala na pevnou linku žena. Mluvila lámanou angličtinou a
informovala mě, že můj soukromý počítač - přes který se propojuji přes VPN do zaměstnání - napadl hacker. V tu chvíli jsem na VPN do zaměstnání připojená nebyla
Nabízela, že za její asistence mě hackera, viru zbaví.

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



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 července 2022, 17:57

Ilustrační foto. | Foto: Shutte

ČEZ České Energetické Závody vyčlenily přes 129,3 milionu 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 společnosti 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 dál platit omezení elektrických vozítek segway, rozhodl Ústavní soud

před 41 minutami

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

Aktualizováno před 43 minutami

Akcionáři Monety 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 otevírací době obchodů je letos ještě větší chaos než jindy. Podívejte se, co platí

před 1 hodinou

Bylo to nedorozumění. Pcheng Šuaj ve videohovoru popřela sexuální napadení

DALŠÍ ZPRÁVY

CEZ GROUP

Vláda České republiky

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 ELEKTŘINY

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

Investice ve výši 7 000 korun

FOTOVOLTAIKA

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

Trh, 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

CEZ GROUP
ČEZ České Energetické Závody

Děkuji za pozornost

Pavel Bašta • pavel.basta@nic.cz