12. Bezpečnost na Internetu a počítačová kriminalita

Ing. Jana Varnušková, Ph.D.
janavar@kiv.zcu.cz

Obsah

- HOAX, SPAM a **phishing**
- Podvodné e-shopy a e-bazary
- Dobré rady pro uživatele
- Dobré praktiky (dobrých) společností
- Podvodné telefonní hovory
- Kopírování platebních karet
- Ransomware
- Dobré rady od antivirové společnosti ESET
- Odkazy na další materiály
- Ukázky phishingu

HOAX

- Význam - žert, výmysl, poplašná zpráva, mystifikace.
- Příklad - injekční stříkačky zapíchané v sedadlech v metru, recyklované mléko, zpoplatnění Facebooku, pomeranče nakažené HIV aj.
- Někdy neškodné, jindy vyvolávají paniku a strach.
- Vybízejí k přeposílání; Často šířeny jako SPAM.
- Příklad - *POMENANČE Z LIBIE JSOU POSTŘÍKANÉ HIV KRVÍ, celní služba v chorvatsku to zjistila !!!!! posílejte dál hlavně kdo má malé děti!!!!!!!!!!!!!!!!*

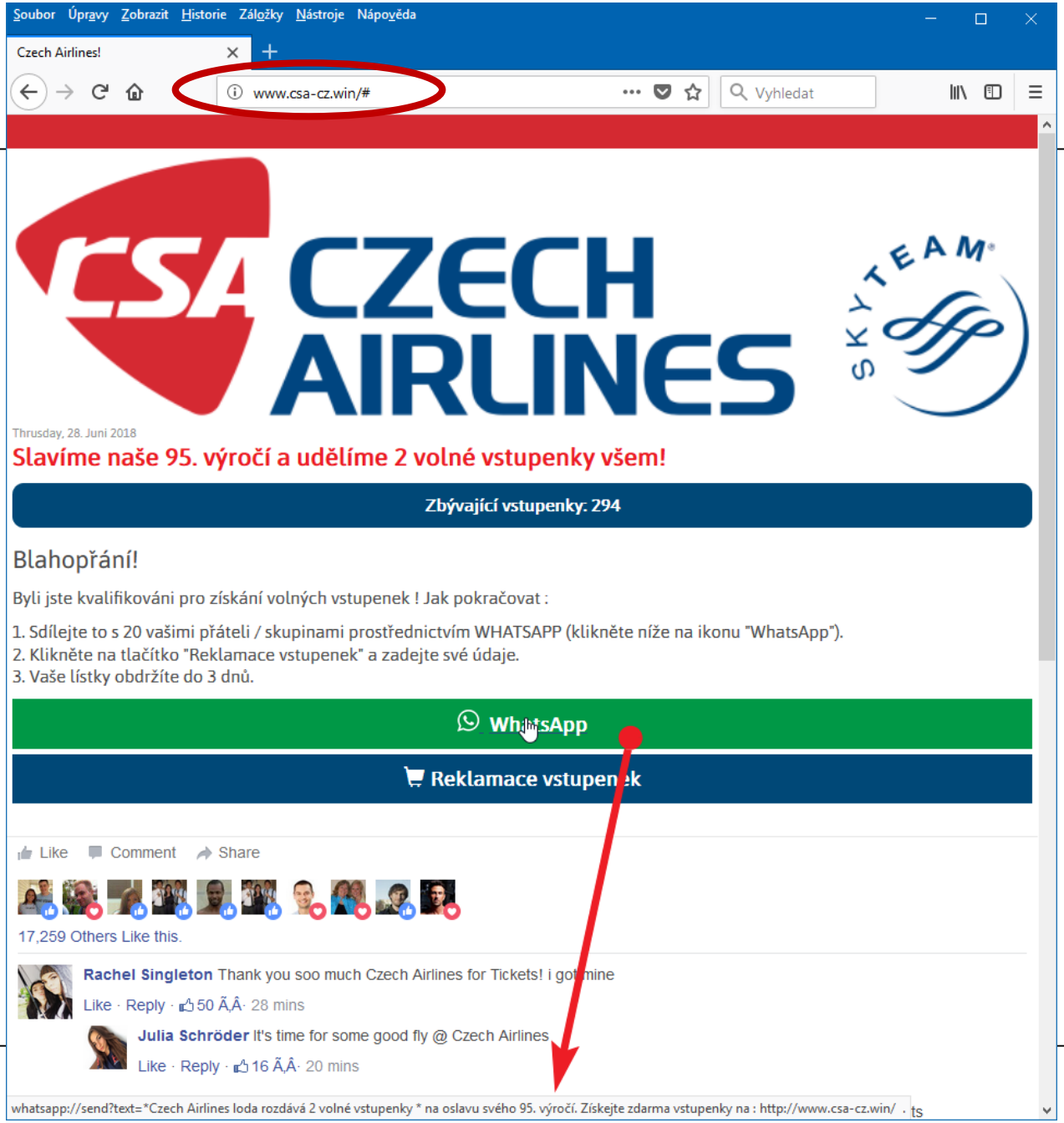
- Zdroje:
  - https://www.hoax.cz
  - https://www.mbank.cz/informace-k-produktum/info/bezpecnost/zasady-bezpecnosti.html

SPAM

- Hromadně rozesílaný e-mail či zpráva.
  - Obvykle není cílen na konkrétní skupinu osob.
- Většinou reklama, ale také přílohy s viry či odkazy na stránky obsahující malware.
- **Spamem nejsou obchodní sdělení**, **k jejichž zasílání jste dali souhlas**, například při nákupu v e-shopu. Nicméně ta se od spamu liší tím, že dle zákona 480/2004 Sb. **musí obsahovat odkaz s možností odhlášení odběru těchto e-mailů**.

Phishing (rybaření)

- Obdoba SPAMu – obvykle email, ale dnes často také SMS nebo telefonní hovor.
- Snaha získat od uživatele peníze či přístup do jeho bankovnictví.
  - Snaha o získání obchodních tajemství apod. je nazývána *spear-phishing*.
- Často odkazují na podvodné stránky – vypadají jako uživateli dobře známý web.
- SMS mohou nabádat k instalaci aplikací či k potvrzení autorizačních zpráv např. z banky.



Zdroj:
https://www.hoax.cz

Zdroj:
https://www.hoax.cz

Phishing – využití sociálního inženýrství

- Často cílí na lidi „s nižším vzděláním “
  - Záměrné chyby v textu apod.
  - Nabídky finančního zisku, loterie atd.
  - Známé celebrity a lákavé titulky.
  - Reklamy na zázračné produkty (léky, doplňky).
  - Přísliby trestu či trestu z prodlení.
  - Varování před nebezpečím (např. *máte v PC virus*)

- Typický příklad sociálního inženýrství:
  - **Útočník:** *… žiji s malými dětmi na Ukrajině a je nám zima … pošli mi kamna, prosím …*
  - **Napadený:** *… poslání kamen je příliš drahé a komplikované … raději ti pošlu peníze a kamna si kup …*

Co mohou útočníci požadovat?

- uživatelská jména a hesla,
- rodná čísla,
- čísla bankovních účtů,
- kódy PIN,
- čísla platebních karet,
- jméno vaší matky za svobodna,
- datum narození, adresy,
- potvrzení ověřovací SMS

Zdroj: https://support.google.com/websearch/answer/106318?hl=cs

Zdroj a další příklady:

https://bezpecnejsi.ostrava.cz/situace/internet/ phishing-utoky-pres-zpravy/

Ministerstvo spravedlnosti České republiky

GENERÁLNÍ ŘEDITELSTVÍ KRIMINÁLNÍ POLICIE

PŘEDVOLÁNÍ K SOUDU

Pro průzkum
(článek 331-1-22 trestního řádu)

Jsem Jan Švejdar, ředitel Úřadu pro vyšetřování zločinů.
Ve spolupráci s Evropským policejním úřadem (EUROPOL) se na Vás obracím krátce po zadržení kybernetické infiltrace (autorizované, zejména v oblasti dětské pornografie, pornografických stránek, kyberpornografie), abych Vás informoval, že jste předmětem několika probíhajících soudních řízení:

*** KYBERPORNOGRAFIE**
*** PORNOGRAFICKÉ STRÁNKY**
*** DĚTSKÁ PornografIE**

Prosíme vás, abyste se vyjádřili e-mailem a napsali nám své zdůvodnění, abychom mohli a zkontrolovány za účelem vyhnutí se sankcí; to za přísných podmínek Přísných 48 hodin.

Po uplynutí této doby budeme muset naši zprávu předat státnímu zástupci Richardu Krpacovi, specialistovi na kyberkriminalitu, aby na vás vydal zatykač a zařadil vás na seznam sexuálních delikventů.
Váš případ bude rovněž zveřejněn v médiích, aby byla informována široká veřejnost.
Vaše rodina, komunita a přátelé budou vědět, co na počítači děláte.

Nyní jste upozorněni.

Jan Švejdar
ředitel Úřadu kriminální policie
a vyšetřování Policejního prezidia.
Otevřeno 24 hodin denně, 7 dní v týdnu

HOAX

Zdroj:
https://www.hoax.cz/scam419/policejni-

Podvodné e-shopy

Seznam rizikových e-shopů:
https://www.coi.cz/pro-spotrebitele /rizikove-e-shopy/
- je i jako doplněk pro vyhledávače

- Kdy si začít dávat pozor?
  - Neobvyklé možnosti platby.
  - Špatný design webových stránek.
  - Podezřelá doménová jména.
  - Nadstandartní slevy.
  - Podezřelé nebo neexistující kontaktní údaje.
  - Negativní recenze.

- Byli jste podvedeni?
  - Při platbě kartou lze banku požádat o tzv. *chargeback transakci* (nicméně ten nemusí být zaručen).
  - *Česká obchodní inspekce* (ČOI) pro české obchodníky.
  - *Evropské spotřebitelské centrum* pro ostatní.
  - *Policie ČR.*

Zdroj: https://www.bluepartners.cz/blog/clanek/6-zpusobu-jak-identifikovat-podvodne-nakupni-webove-stranky

Podvody v e-bazarech

- Časté triky:
  - Prodávající vám zaplacené zboží vůbec **nepošle.**
  - Při platbě na dobírku vám **nedojde zakoupené zboží** ale např. cihla.
  - Prodávající vám pro zaplacení za zboží pošle **odkaz na falešnou platební bránu**, přes kterou získá údaje o vaší kartě.
- Dobré rady:
  - Vždy kontrolujte hodnocení/recenze prodávajícího.
  - Platťe ideálně hotově při osobním převzetí a zkontrolování zboží.
  - Pro převod peněz na váš účet potřebuje kupující znát pouze číslo vašeho účtu.
  - Nikdy neklikejte na odkazy pro přihlášení do internetového bankovnictví či platební brány, které vám někdo pošle e-mailem nebo na sociálních sítích.

Zdroj: https://www.mbank.cz/o-nas/bezpecnost/klient/nakupovani-na-e-shopech/

Dobré rady (obecně)

- Obezřetnost na prvním místě.
- Neklikejte na neověřené odkazy.
- Nikdy neposkytujte své osobní údaje neznámému člověku.
- Neplaťte předem (pokud si nejste obchodem jisti).
- Sledujte recenze a zkušenosti ostatních.
- Aplikace a nástroje stahujte pouze z oficiálních obchodů.
- Udržujte svá zařízení aktualizovaná.
- Chraňte svá zařízení antivirem.

Zdroj: https://www.dvojklik.cz/4-nejcastejsi-podvody-na-ceskem-internetu/

Dobré rady (viz Google)

- Berte to s klidem
  - *Podvody jsou často navrženy tak, aby vyvolávaly dojem naléhavosti. Nespěchejte a vše si důkladně promyslete.*
- Ďábel se skrývá v detailu
  - *Dejte si práci s pečlivým ověřením všech informaci, které dostanete. Dává vám vše smysl?*
- **Stop!** Nic neodesílejte
  - *Žádná důvěryhodná osoba ani organizace nebudou požadovat platbu nebo osobní údaje ihned.*

Zdroj: https://support.google.com/faqs/answer/2952493

Dobré rady při práci s emaily (viz mBank)

- Neotevírejte podezřelé e-maily a přílohy (např. *převod.pdf.zip*).
- V e-mailu najetím kurzoru na odkaz zkontrolujte, zda odkazuje opravdu na vámi očekávanou stránku.
- Věnujte pozornost důvěryhodnosti odesílatele a způsobu, jakým s vámi komunikuje.
- Nikdy se nepřihlašujte do banky z odkazu, který obdržíte v e-mailu.
- Nevěřte e-mailům oznamujícím výhru v soutěži, do které jste se nepřihlásili.

Zdroj: https://www.mbank.cz/o-nas/bezpecnost/klient/phishing/#opatrne

Dobré rady, osobní údaje (viz mBank)

- Nikdy na sociálních sítích nesdílejte fotky svých průkazů - **rodné číslo, číslo občanského** či **řidičského průkazu** nebo **pasu, číslo platební karty** včetně 3místného **CVC/CVV kódu** na zadní straně karty, datum platnosti karty, adresu, **adresu trvalého bydliště** a vlastnoruční **podpis**.
- Nenechávejte své doklady bez dozoru.
- Pozor při pořizování kopií dokladů.

- Jste-li na dovolené a váš dům je bez dozoru, tak zvažte, zda je vhodné sdílet fotografie z dovolené v reálném čase.

Zdroj: https://www.mbank.cz/o-nas/bezpecnost/klient/osobni-udaje

Dobré rady, další nástrahy (viz mBank)

- Zabezpečení telefonu: https://www.mbank.cz/o-nas/bezpecnost/klient/telefon/
- Nástrahy na Wi-Fi: https://www.mbank.cz/o-nas/bezpecnost/klient/wi-fi/
- Zabezpečení počítače: https://www.mbank.cz/o-nas/bezpecnost/klient/pocitac/

Varování ve webovém prohlížeči

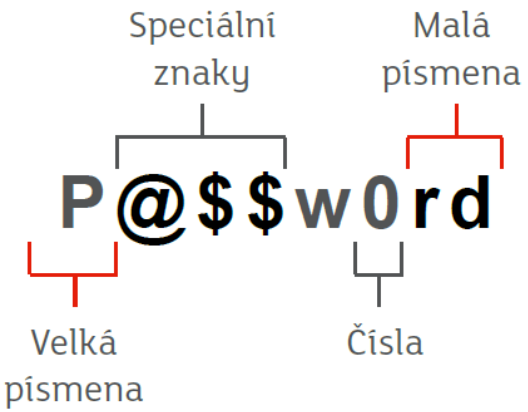
- Samotný webový prohlížeč dokáže upozornit na problémové stránky či stránky, které by problémové mohly být.

- Varování v *Google Chrome*:
  - Webové stránky, které chcete otevřít, obsahují malware.
  - Chystáte se navštívit podvodné webové stránky.
  - Podezřelý web.
  - Web, na který se chystáte přejít, obsahuje škodlivé programy.
  - Tato stránka se pokouší načíst skripty z neověřených zdrojů.

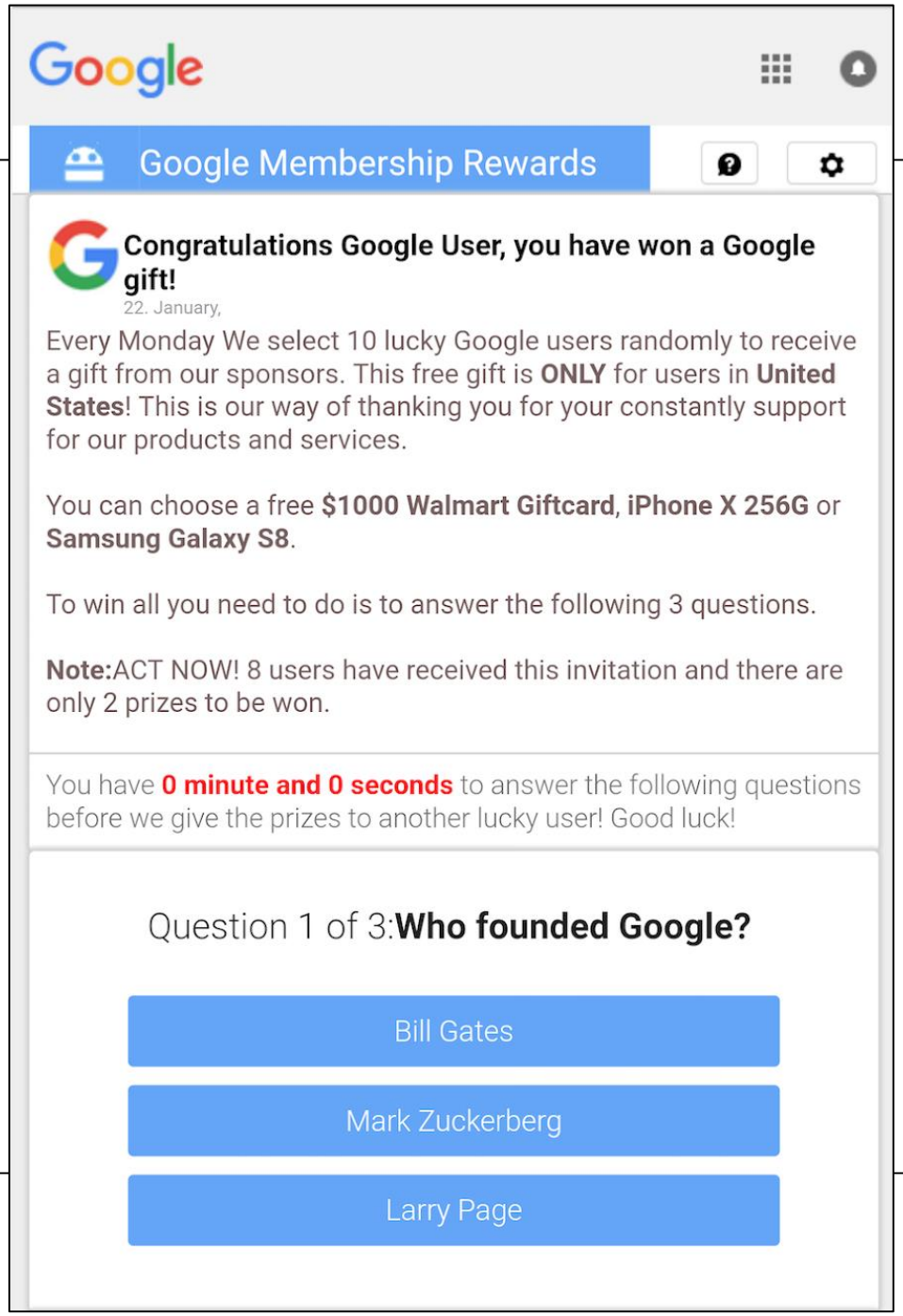
Zdroj: https://support.google.com/chrome/answer/99020

Hesla

- Jakmile nabydete dojmu, že heslo bylo někým zneužito/odcizeno, okamžitě ho změňte.
- Používejte silná hesla
  - min. 8 znaků
  - kombinace malých/velkých písmen, čísel a speciálních znaků.



Zdroj: https://www.mbank.cz/o-nas/bezpecnost/klient/hesla/



Zdroj: https://support.google.com/faqs/answer/10122682

Dobré praktiky - *obecně*

- Platný certifikát webu.
- Zabezpečený protokol HTTP**S** (ne pouze HTTP).
- Správná URL adresa.
- Nevyžadování hesel (ani emailem, ani tel. hovor).
- Nevyžadování osobních údajů (max. ověření ano/ne).

Zdroj: https://support.google.com/faqs/answer/10123201

Dobré praktiky - *Google*

- Google **nepoužívá** automatické hovory.
- Google vás **nebude** po telefonu vyzývat k aktualizaci zápisu na titulní stránce ani k nárokování bezplatného webu.
- Google vám **nebude** účtovat poplatek za zařazení do Vyhledávání nebo služby Moje firma na Googlu.

- Příklady podvodů zneužívajících společnost Google: https://support.google.com/faqs/answer/2952493

Zdroj: https://support.google.com/faqs/answer/10123201

Dobré praktiky – *mBank (1)*

- mBank po vás nikdy nebude vyžadovat abyste převedl své prostředky na účty jiných zákazníků, ani vás nebudeme vybízet k zadávání údajů k platebním kartám apod.
- Pokud jste vyzýváni k zadání citlivých údajů, **ověřte si, že jste na skutečných stránkách banky** (tj. https://www.mbank.cz).
- Do internetového bankovnictví **se přihlašujte pouze přes oficiální www** stránky mBank.
- **Adresu stránky do prohlížeče pište ručně**, nevyhledávejte internetové bankovnictví mBank na Seznamu či Googlu.
- Žádosti o produkty a schůzky vyplňujte pouze přes oficiální www stránky či v internetovém bankovnictví mBank.
- Pokud Vám někdo tvrdí, že si svou autorizační SMS (k IB) nechal zaslat na Váš mobil, odmítněte ho a neprodleně nás kontaktujte.

Zdroje:
https://www.mbank.cz/informace-k-produktum/info/bezpecnost/zasady-bezpecnosti.html

Dobré praktiky – *mBank (2)*

- Operátor mLinky **nikdy nevyžaduje heslo do internetového bankovnictví** ani celé heslo pro mLinku.
- Operátor mLinky při aktivaci kanálu požaduje 3 náhodně vybraná čísla z hesla pro mLinku.
- mBank **nikdy nevyžaduje údaje k vašemu mobilnímu telefonu**, např.
  tel. číslo, model atd., při přihlašování do internetového bankovnictví.
- mBank **nikdy nezasílá na váš mobilní telefon žádné bezpečnostní ani jiné certifikáty**, které byste museli instalovat.
- mBank **nikdy nežádá o instalaci certifikátů nebo bezpečnostních aplikací** v mobilních telefonech.

Zdroje:
https://www.mbank.cz/informace-k-produktum/info/bezpecnost/zasady-bezpecnosti.html

Podvodné telefonní hovory

- Falešní „vnuci" a „doktoři" okrádají seniory o úspory, viz ukázka:
  - https://bezpecnejsi.ostrava.cz/falesni-vnuci-okradaji-seniory/
  - Zajímavé část: ***Jak se nestát obětí telefonického podvodu***
  - Policie provádí osvětu seniorů využitím telefonního automatu.

Příklad: *V nočních hodinách telefonuje seniorovi muž, který tvrdí, že je lékař, který právě operoval seniorova vnuka. Vysvětlí, že vnuk zavinil autonehodu a sám byl zraněn, takže nemůže mluvit. Požádal proto „lékaře", aby vyřídil mimosoudní vyrovnání, a prosí jeho prostřednictvím prarodiče, aby mu poslali peníze na účet…*

Podvodné telefonní hovory

- Příklad SMS:
  Zpráva Google č. 42132: Váš Gmail byl napaden hackery. Google vám musí zavolat a ověřit vaši totožnost. Až budete připraveni přijmout hovor, v odpovědi na tuto SMS napište „READY" *(Připraven(a)).*
  - Následuje hovor s automatem.
  - Mohou být účtovány dodatečné poplatky.
- Podvodníci, kteří vám zavolají a vydávají se za banku a policii – ukázka manipulace viz video (18min): https://youtu.be/rB0x09uAyyE

Zdroje:
https://support.google.com/faqs/answer/10122683
https://www.hoax.cz/aktuality/podvodnici-kteri-vam-zavolaji-a-vydavaji-se-za-banku-a-policii_689

Skimming – kopírování platební karty

- Možnosti ochrany:
  - **zakrývat klávesnici bankomatu** při zadávání PIN kódu.
  - před použitím bankomatu **hledat podezřelé prvky.**
  - **využívat možnosti bezkontaktního výběru peněz,** tj. nevkládat kartu přímo do bankomatu.
  - mít **rozumně nastavené limity na kartě.**
  - **preventivně deaktivovat platby magnetickým proužkem** vaší karty (v ČR se magnetickým proužkem již neplatí, ale bývá aktivní kvůli zahraničí; návod viz zdroj).
  - mít na účtu spojeném s kartou pouze minimální obnos financí.

Zdroj: https://www.mbank.cz/o-nas/bezpecnost/klient/bankomat/

Ransomware

- Složení anglických slov *ransom* „výkupné“ a *software.*
- Škodlivý kód, který zamyká přístup k infikovanému zařízení nebo šifruje jeho obsah a za obnovení dat požaduje poplatek.

- ESET popisují:
  - Platba nejčastěji v **bitcoinech** nebo jiné virtuální měně. Po zaplacení by následně mělo dojít k odšifrování dat nebo obnovení přístupu do infikovaného zařízení.
  - Útočnici však nic negarantují, proto **nedoporučujeme výpalné platit**. V praxi se setkáváme spíše s případy, kdy se po zaplacení nic nedělo, než naopak.

Zdroj: https://www.eset.com/cz/ransomware/

Ransomware

- Typy:
  - **Diskcoder** šifruje celý pevný disk a brání uživateli v přístupu do operačního systému.
  - **Screen locker** blokuje přístup na obrazovku zařízení.
  - **Crypto ransomware** šifruje data na disku.
  - **PIN locker** cílí na zařízení s Androidem a mění (případně vytvoří) přístupový PIN k odemčení mobilu nebo tabletu.
- Obrana:
  - **Pravidelně zálohujte data** a udržujte aktuální aspoň jednu plnou offline zálohu.
  - **Pravidelně aktualizujte** všechny používané aplikace včetně operačního systému.
  - **Používejte kvalitní bezpečnostní řešení**, které obsahuje nejen antivirovou ochranu, ale také další vrstvy ochrany proti škodlivému kódu.

Zdroj: https://www.eset.com/cz/ransomware/

Dobré rady (viz *antivirus ESET)*

- Vytvořte u uživatelských účtů politiku na **používání silného hesla**.
- Omezte nebo úplně **zakažte používání RDP** (*Remote Desktop Protocol*) **mimo firemní síť**, případně používejte autorizaci na úrovni sítě (*Network Level Authentication*).
- Používejte **VPN** (*Virtual Private Network*).
- Pravidelně **kontrolujte nastavení firewallu** a politik pro komunikaci mezi vnitřní a vnější sítí.
- Přístup do **nastavení bezpečnostního řešení chraňte** silným heslem.
- Používejte **dvoufaktorovou autentizaci** přístupu do sítě.
- Pravidelně **pořádejte školení zaměstnanců**, aby znali potenciální rizika a dokázali je poznat.
- Riziko napadení můžete snížit i odinstalací nepoužívaných služeb a softwaru.

Zdroj: https://www.eset.com/cz/ransomware/

Další materiály

- Aktuální dění v oblasti HOAX, Phishing apod.: https://www.hoax.cz
- *SecFest* na ZČU: https://secfest.zcu.cz
- Kraje pro bezpečný internet: https://www.kpbi.cz
  - Po registraci dostupná spousta materiálů (děti, učitelé, senioři, aj.).
  - Obsažena i témata: kyberšikana, kyberstalking, kybergrooming, sexting aj.
- Osvětové materiály kybernetické bezpečnosti: https://secfest.zcu.cz/SecFest2021/prezentace/2021-11-15-Osvetove-materialy-kyberbezpecnosti-Cepak.pdf
- NÚKIB (národní úřad pro kybernetickou a informační bezpečnost): https://osveta.nukib.cz/local/dashboard/
- Bezpečnostní kvíz (*mBank*): https://www.mbank.cz/o-nas/bezpecnost/kviz/
- Ochrana na FaceBooku: https://www.youtube.com/playlist?list=PLrT6AA3DsRDDCtiMnd9gAHsK9ZxZgWffg
- Konference NCBI se spoustou materiálů k bezpečnosti na internetu: http://konference.ncbi.cz/index.php?option=com_content&view=article&id=45&Itemid=224

Reálné příklady Phishingu apod.

Mikulášský dárek - Perspektiva 05.12.2022

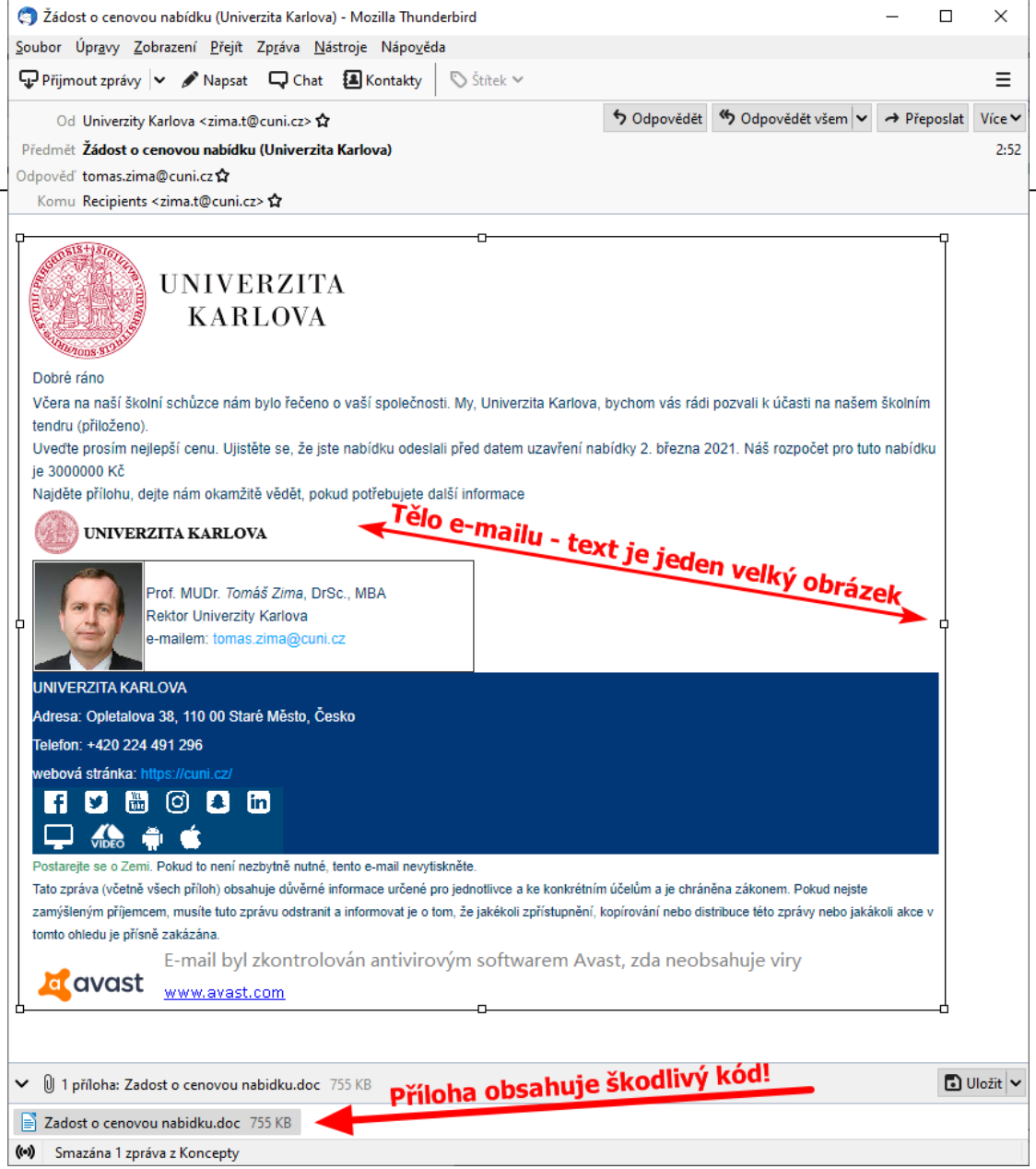
Perspektiva, o významu tohoto slova si můžeme přečíst ve slovníku cizích slov, že značí:

- zobrazení pohledu do vzdáleného prostoru do roviny, kdy se zobrazované předměty zdánlivě zmenšují a sbíhají
- pohled do dálky
- vyhlídky do budoucnosti
- hledisko, stanovisko

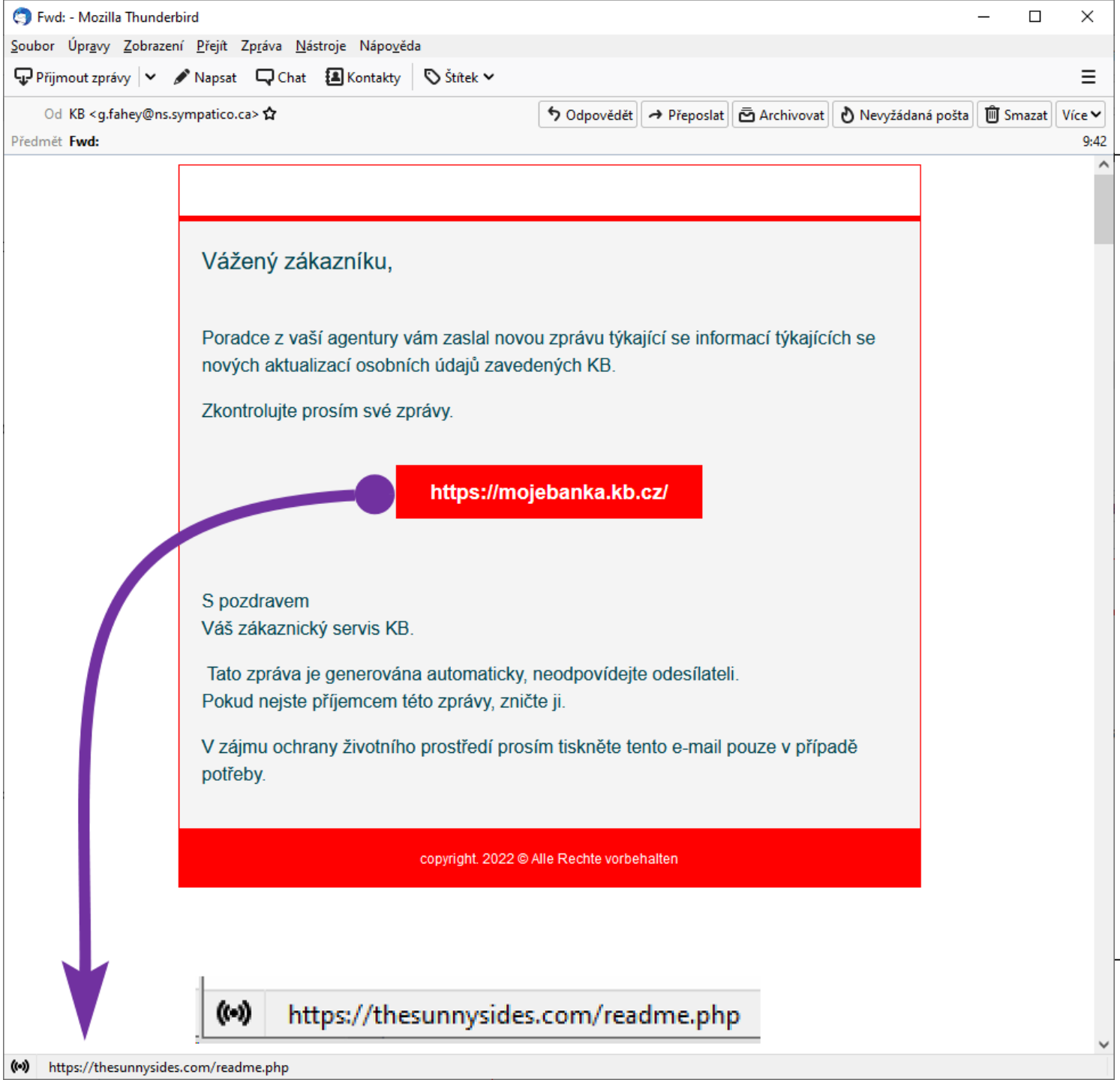
Ale **Perspektiva** je také název nové **knihy Josefa Dubna**. Jak se stalo v posledních letech tradici, je pro čtenáře našeho serveru k dispozici zdarma ke stažení.
A komu se knížka líbila, má volnou ruku ji poslat dál, tedy ji mohou takto obdržet i další čtenáři, „z druhé ruky".

Přehled e-knih ke stažení je níže v detailu zprávy.

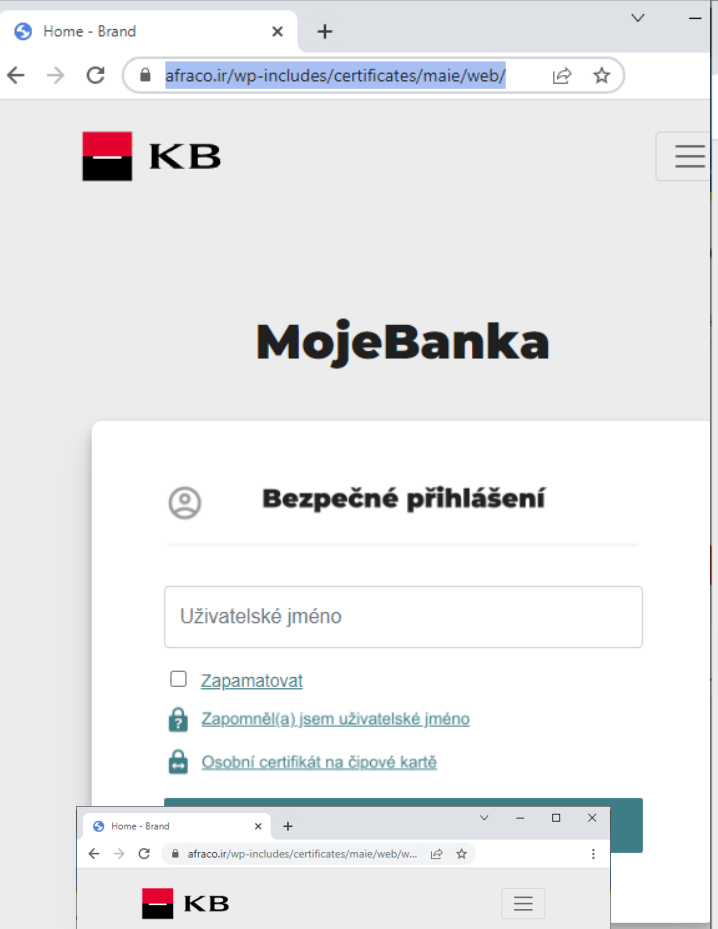
Zdroj: https://www.hoax.cz/aktuality/mikulassky-darek---perspektiva_693

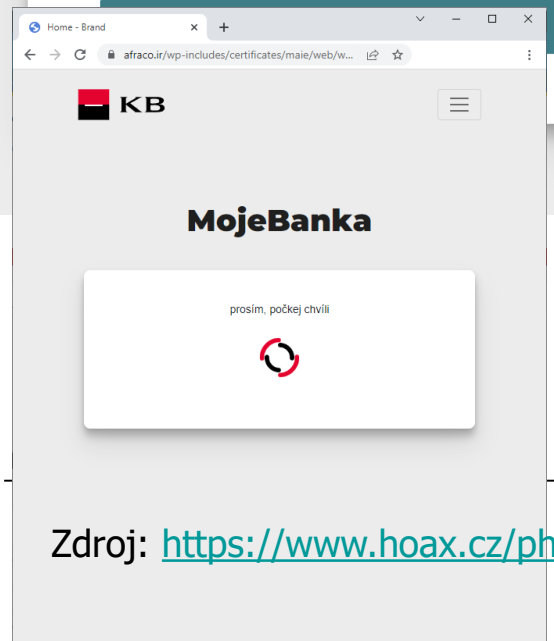


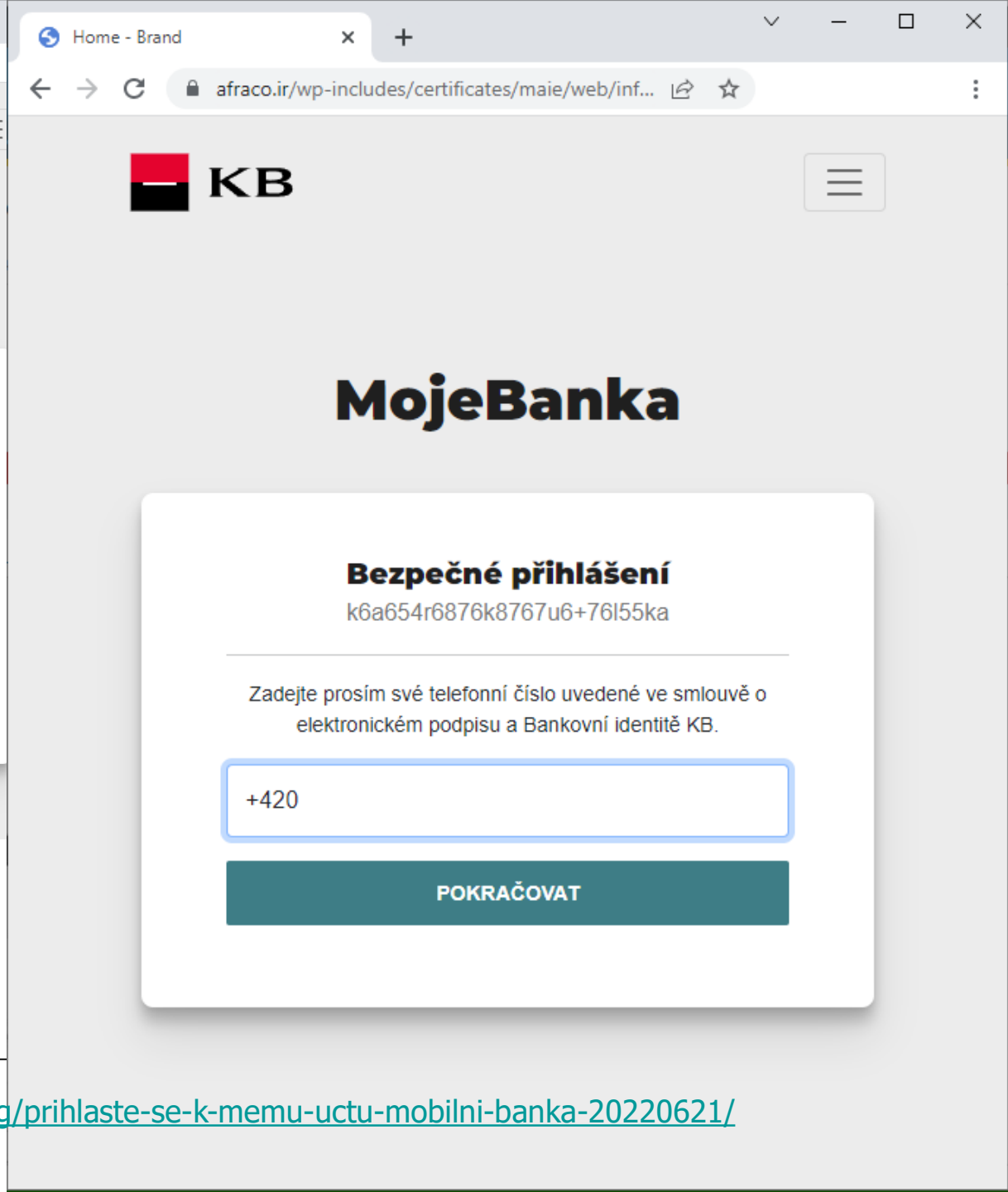
Zdroj: https://www.hoax.cz/malware/zadost-o-cenovou-nabidku-univerzita-karlova-20200326/



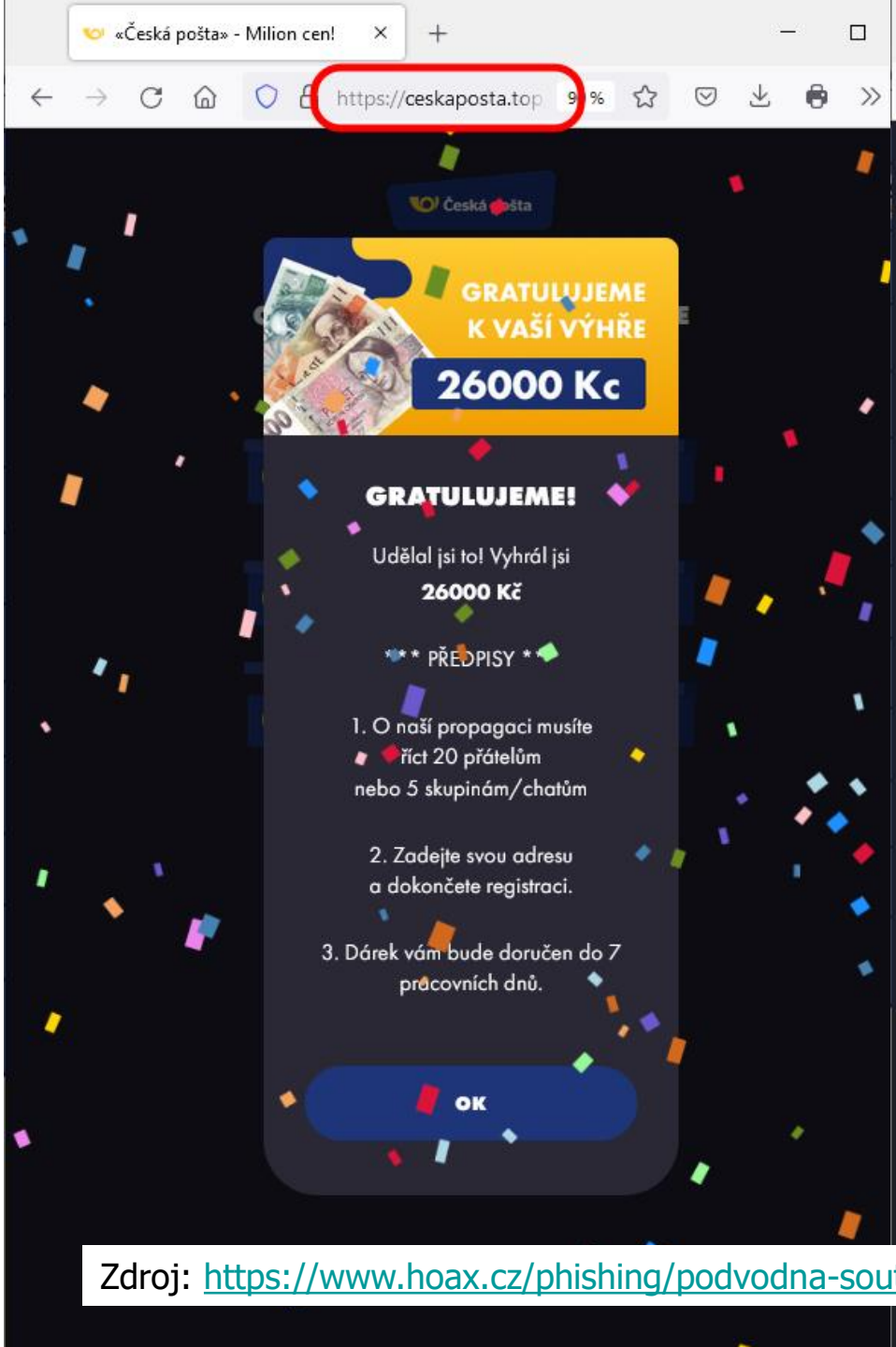
Zdroj: https://www.hoax.cz/phishing/prihlaste-se-k-memu-uctu-mobilni-banka-20220621/

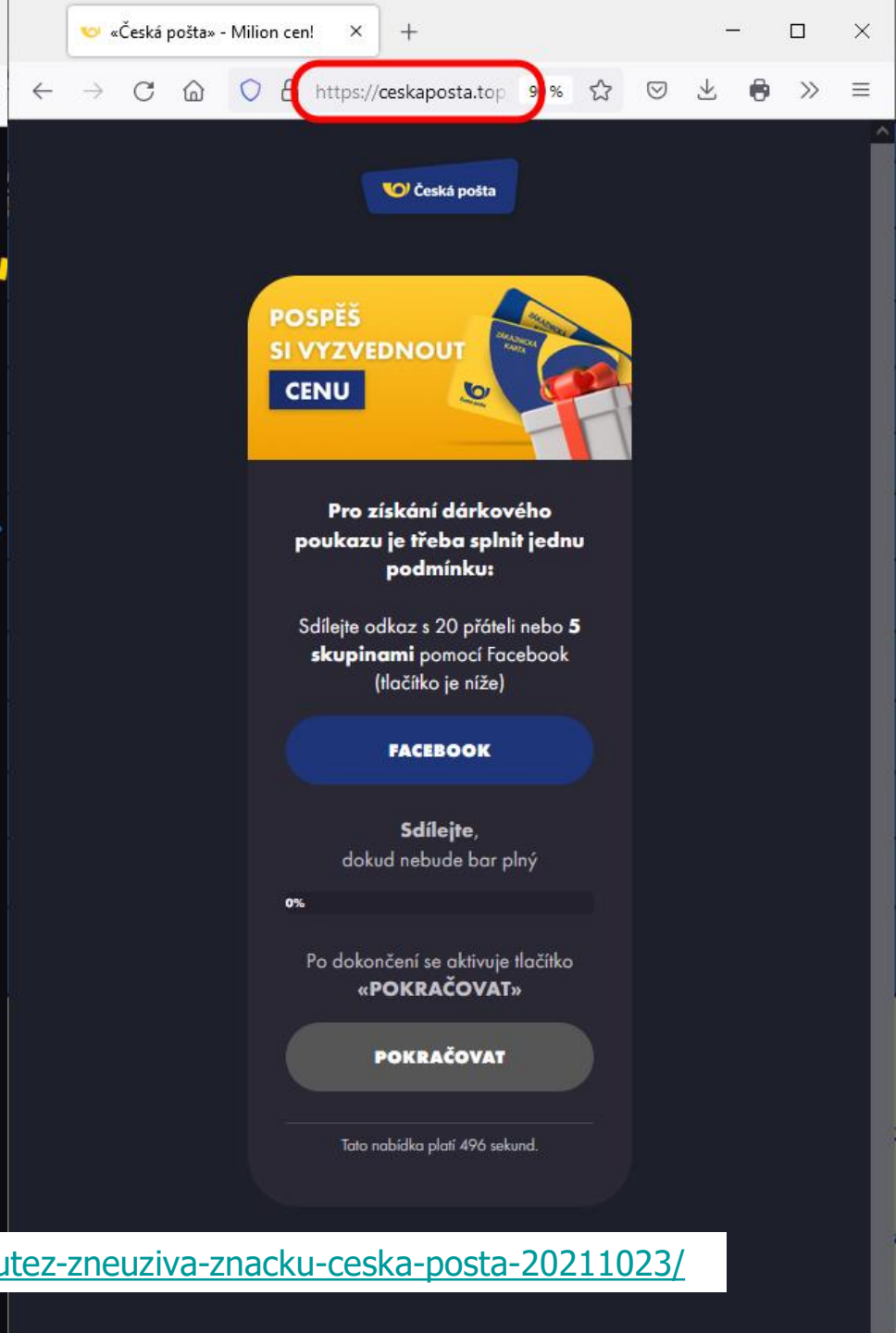




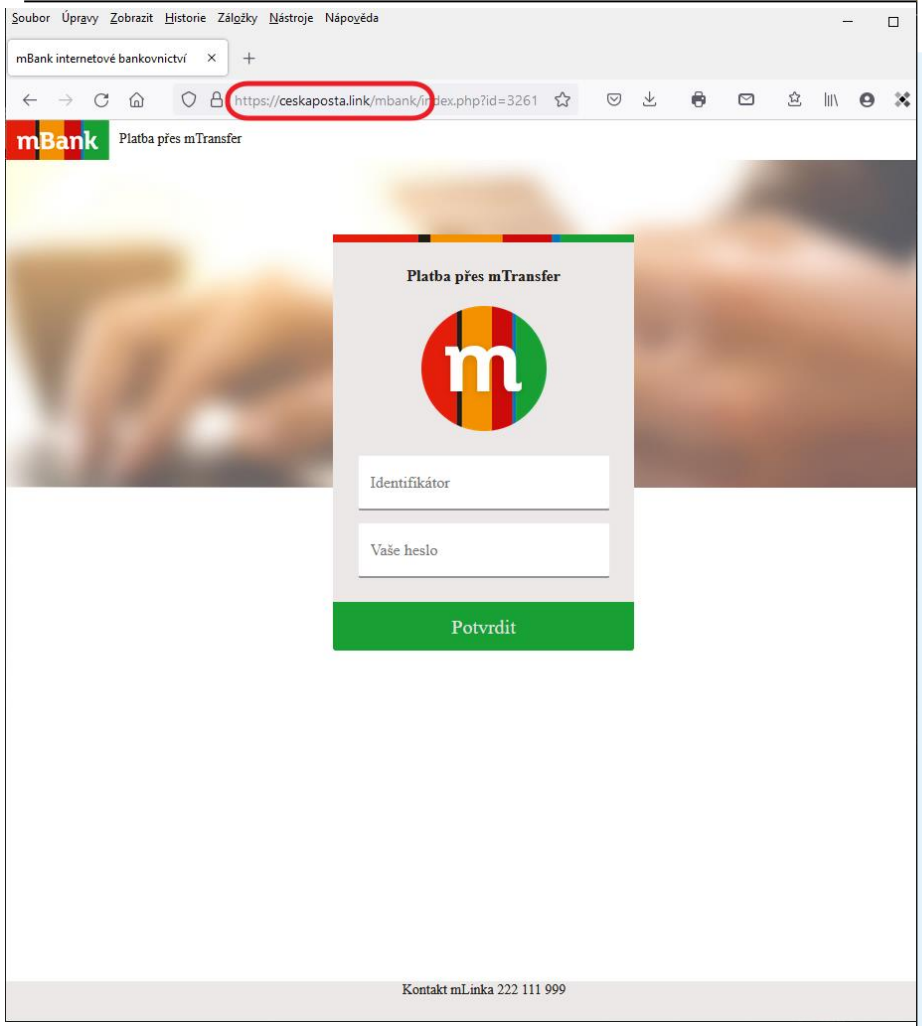


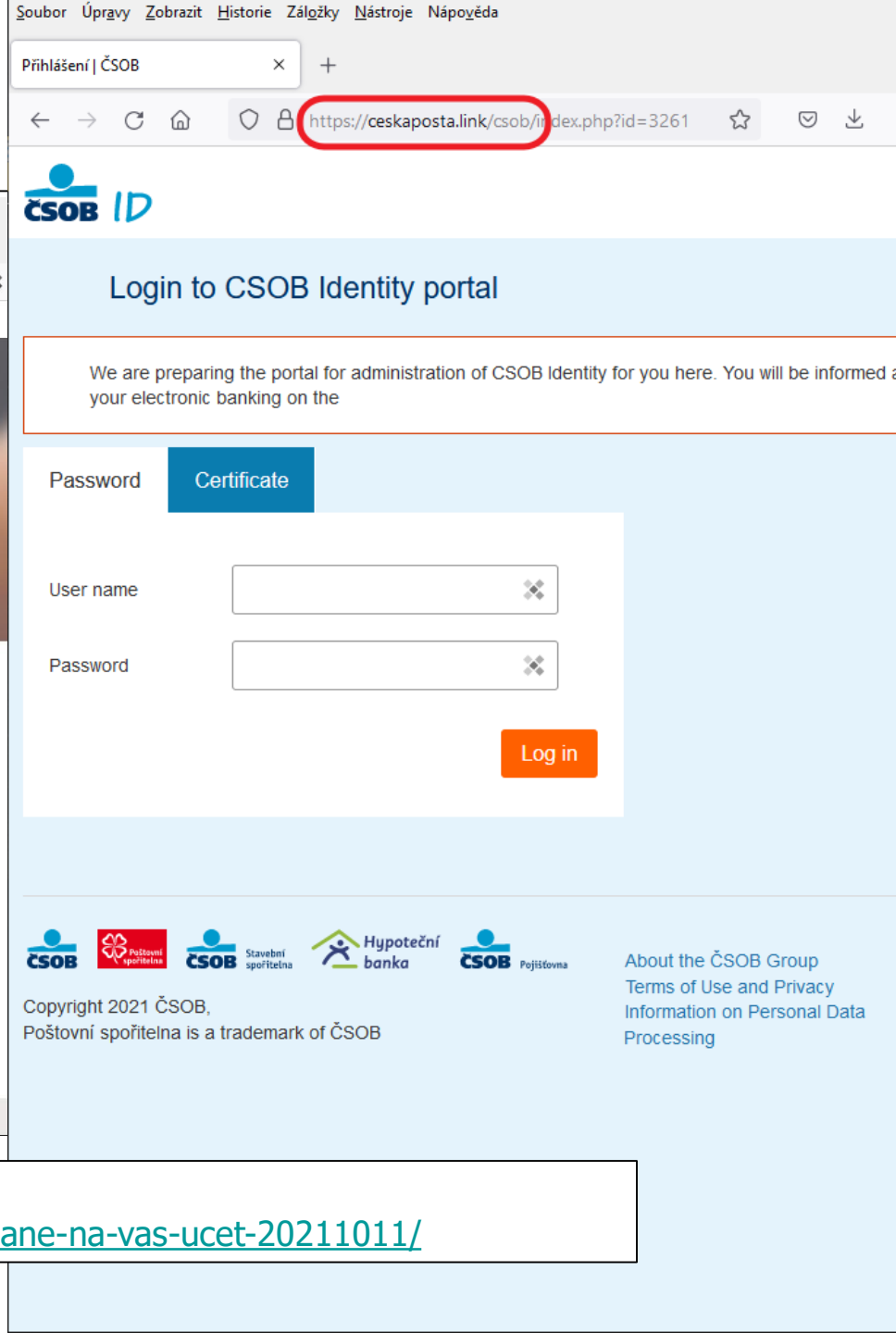
Zdroj: https://www.hoax.cz/phishing/prihlaste-se-k-memu-uctu-mobilni-banka-20220621/



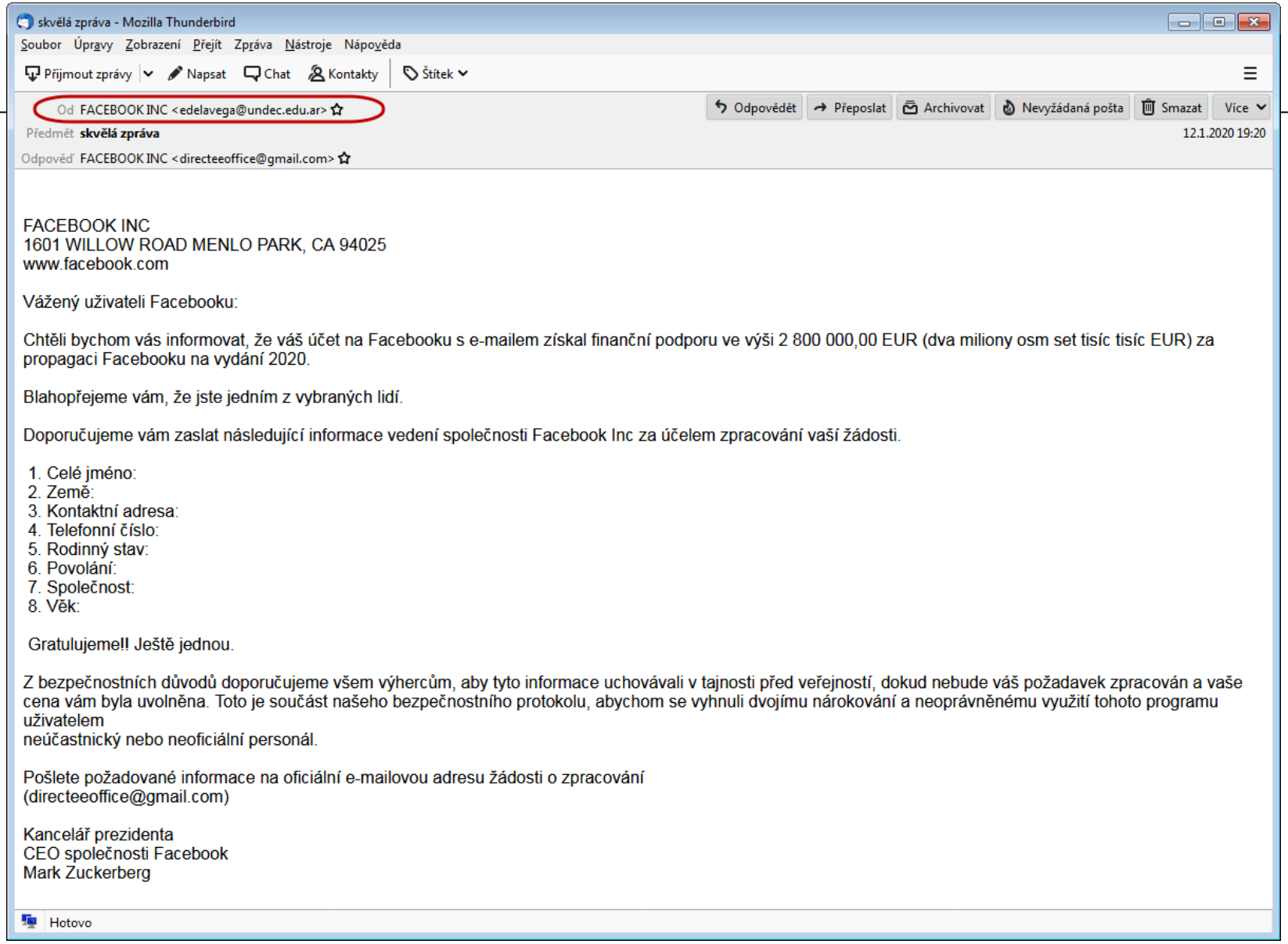


Zdroj: https://www.hoax.cz/phishing/podvodna-soutez-zneuziva-znacku-ceska-posta-20211023/





Zdroj a další příklady pro snad všechny banky v ČR:
https://www.hoax.cz/phishing/oznameni-o-vraceni-dane-na-vas-ucet-20211011/



skvělá zpráva - Mozilla Thunderbird

Soubor Úpravy Zobrazení Přejít Zpráva Nástroje Nápověda

Přijmout zprávy | Napsat | Chat | Kontakty | Štítek

Od FACEBOOK INC <edelavega@undec.edu.ar>

Odpovědět | Přeposlat | Archivovat | Nevyžádaná pošta | Smazat | Více

Předmět **skvělá zpráva**

12.1.2020 19:20

Odpověď FACEBOOK INC <directeeoffice@gmail.com>

FACEBOOK INC
1601 WILLOW ROAD MENLO PARK, CA 94025
www.facebook.com

Vážený uživateli Facebooku:

Chtěli bychom vás informovat, že váš účet na Facebooku s e-mailem získal finanční podporu ve výši 2 800 000,00 EUR (dva miliony osm set tisíc tisíc EUR) za propagaci Facebooku na vydání 2020.

Blahopřejeme vám, že jste jedním z vybraných lidí.

Doporučujeme vám zaslat následující informace vedení společnosti Facebook Inc za účelem zpracování vaší žádosti.

1. Celé jméno:
2. Země:
3. Kontaktní adresa:
4. Telefonní číslo:
5. Rodinný stav:
6. Povolání:
7. Společnost:
8. Věk:

Gratulujeme!! Ještě jednou.

Z bezpečnostních důvodů doporučujeme všem výhercům, aby tyto informace uchovávali v tajnosti před veřejností, dokud nebude váš požadavek zpracován a vaše cena vám byla uvolněna. Toto je součást našeho bezpečnostního protokolu, abychom se vyhnuli dvojímu nárokování a neoprávněnému využití tohoto programu uživatelem
neúčastnický nebo neoficiální personál.

Pošlete požadované informace na oficiální e-mailovou adresu žádosti o zpracování
(directeeoffice@gmail.com)

Kancelář prezidenta
CEO společnosti Facebook
Mark Zuckerberg

Hotovo

Zdroj: https://www.hoax.cz/loterie/facebook-skvela-zprava-20200112/

FACEBOOK INC
1601 WILLOW ROAD MENLO PARK, CA 94025
www.facebook.com

Vážený uživateli Facebooku:

Chtěli bychom vás informovat, že váš účet na Facebooku s e-mailem získal finanční podporu ve výši **2 800 000,00 EUR** (dva miliony osm set tisíc tisíc EUR) za propagaci Facebooku na vydání 2020.

Blahopřejeme vám, že jste jedním z vybraných lidí.

Doporučujeme vám zaslat následující informace vedení společnosti Facebook Inc za účelem zpracování vaší žádosti.

1. Celé jméno:
2. Země:
3. Kontaktní adresa:
4. Telefonní číslo:
5. Rodinný stav:
6. Povolání:
7. Společnost:
8. Věk:

Gratulujeme!! Ještě jednou.

Z bezpečnostních důvodů doporučujeme všem výhercům, aby tyto informace uchovávali v tajnosti před veřejností, dokud nebude váš požadavek zpracován a vaše
cena vám byla uvolněna. Toto je součást našeho bezpečnostního protokolu, abychom se vyhnuli dvojímu nárokování a neoprávněnému využití tohoto programu uživatelem
neúčastnický nebo neoficiální personál.

Pošlete požadované informace na oficiální e-mailovou adresu žádosti o zpracování (directeeoffice@gmail.com)

Kancelář prezidenta
CEO společnosti Facebook
Mark Zuckerberg

Zdroj: https://www.hoax.cz/loterie/facebook-skvela-zprava-20200112/

Dobrý den,
Váš balíček dorazil do našeho skladu 23. ledna 2020 roku v 12:15 ráno. Číslo sledování zásilky-0619095 Náš kurýr bohužel nemohl doručit zásilku na vaši adresu kvůli nesprávným nebo neúplným informacím v adrese. Zdá se, že v celním prohlášení došlo k chybě. Informovali jsme odesílatele a on nám předal vaši e-mailovou adresu, abychom mohli tento problém vyřešit co nejdříve. Abychom mohli doručit váš balíček, musíte potvrdit adresu. Za tímto účelem si **stáhněte dokument připojený k tomuto dopisu**, vyplňte ho a pošlete nám ho.

S úctou,
Kamila Jurčíková

Soubor přílohy s názvem např. fa0026913446.doc obsahuje trojského koně.

Zdroj: https://www.hoax.cz/malware/vznikli-potize-s-dorucenim-vaseho-balicku-20200124/

Zdroj: https://www.hoax.cz/scam419/policejni-predvolani---soubor-nr-966-cglt-20220819/

EVROPSKÁ POLICIE (EUROPOL)
Vytvořeno 1. července 1999
Sídlo: Eisenhowerlaan 73
Vlajka: Nizozemsko Haag
Souřadnice 52° 05' 34'' N, 4°16'53E
Zaměstnanci 1065(prosinec 2016)
Roční rozpočet 116,4 milionů EUR (2017)
Odpovědný ministr Vlajka Belgie Jean Philippe LECOUFFE (Zástupce výkonného ředitele)
Eisenhowerlaan 73 Vlajka: Nizozemsko Haag

SVOLÁNÍ

HOAX

Na žádost pana Jean Philippe LECOUFFE.

Jednající v rámci písemných pokynů pana Jean-Philippe LECOUFFE, zástupce výkonného ředitele kanceláře Europolu a vedoucího brigády pro ochranu nezletilých, číslo 160422900879.

Na základě analýz a prací provedených naší brigádou pro ochranu nezletilých (BPM) v počítačové síti byly identifikovány určité stopy vašich identifikačních údajů a jste předmětem několika obvinění:

- **ONLINE SEXUÁLNÍ NABÍZENÍ A VYDÍRÁNÍ**
- **PORNO STRÁNKY**
- **KYBERPORNOGRAFIE**
- **PEDOFILIE**
- **EXHIBITIONISMUS**

Pro vaši informaci, zákon z března 2007 zvyšuje tresty za pokusy o nezletilé osoby, sexuální napadení nebo znásilnění pomocí internetu, žádáme vás, abyste se ozvali e-mailem: officeeuropol05@gmail.com
tím, že nám napíšete svá odůvodnění, abychom je prověřili a ověřili za účelem posouzení sankcí; to v přísném termínu 72 hodin.
Po uplynutí této doby budeme povinni naši zprávu odeslat.

Paní Myriam QUEMENEROVÉ, soudkyni v trestní službě Odvolacího soudu ve Versailles, expertce Rady Evropy v oblasti kybernetické kriminality, aby na vás vypracovala zatykač, zašlete jej nejbližšímu četnictvu v místě vašeho bydliště k zatčení a označte vás jako sexuálního delikventa, odešlete svůj záznam několika národním televizním zpravodajským kanálům k vysílání, kde vaše rodina, příbuzní a všichni ostatní uvidí, co děláte před vaším počítačem.

Nyní jste varováni.

LEGALIZACE DOKUMENTŮ

Pana JEAN-PHILIPPE LECOUFFE
ZÁSTUPCE VÝKONNÉHO ŘEDITELE KANCELÁŘE EUROPOL
VEDOUCÍ BRIGÁDY PRO OCHRANU NEZLETILÝCH

Zdroj: https://www.hoax.cz/scam419/stanovisko-soudu-ze-dne-n-3589-20221013/

?