10. Počítačová síť, zálohování, archivace a bezpečnost dat, etické aspekty ICT, kyberbezpečnost

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

Počítačová síť – co to vlastně je?

- až dosud – 1 počítač (pravděpodobně připojený k Internetu)

- propojení více počítačů → počítačová síť
  - co propojujeme (zařízení)
  - čím (přenosová média)
  - jak může být počítačová síť velká
  - jaká je rychlost
  - konkrétně (domácí síť)
  - bezpečnost – přednáška 12

- archivace a zálohování dat

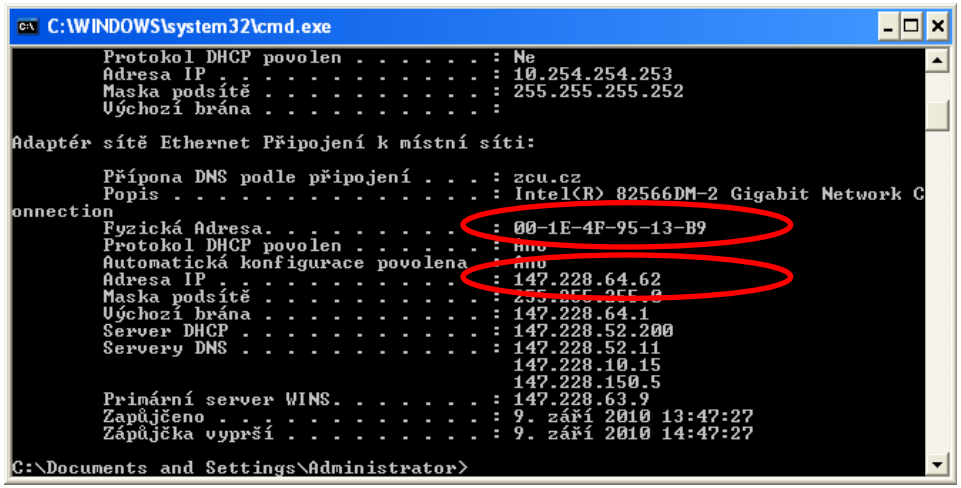
Proč počítačové sítě?

- komunikace, přenos a sdílení dat
- jednodušší využití prostředků
  - tiskárny, datová úložiště, ...
- paralelní výpočty
  - vědecké výpočty rozsáhlých dat
  - distribuované výpočty
    - např. projekt SETI@home – univerzita v Berkeley, hledání mimozemské civilizace
- počítačové hry
  - multiplayer hry – lokálně mezi několika počítači
  - massive multiplayer – servery spravované vydavateli hry
- uložení a archivace dat

Zařízení připojitelná do počítačové sítě

- síťový uzel
  - osobní počítač (síťová karta), server
  - mobilní telefon, PDA
  - tiskárna, webkamera, …
  - datové úložiště
  - aktivní síťová zařízení, ...

- MAC adresa (fyzická adresa)
  - např. 01:23:45:67:89:AB
  - přidělena již při výrobě



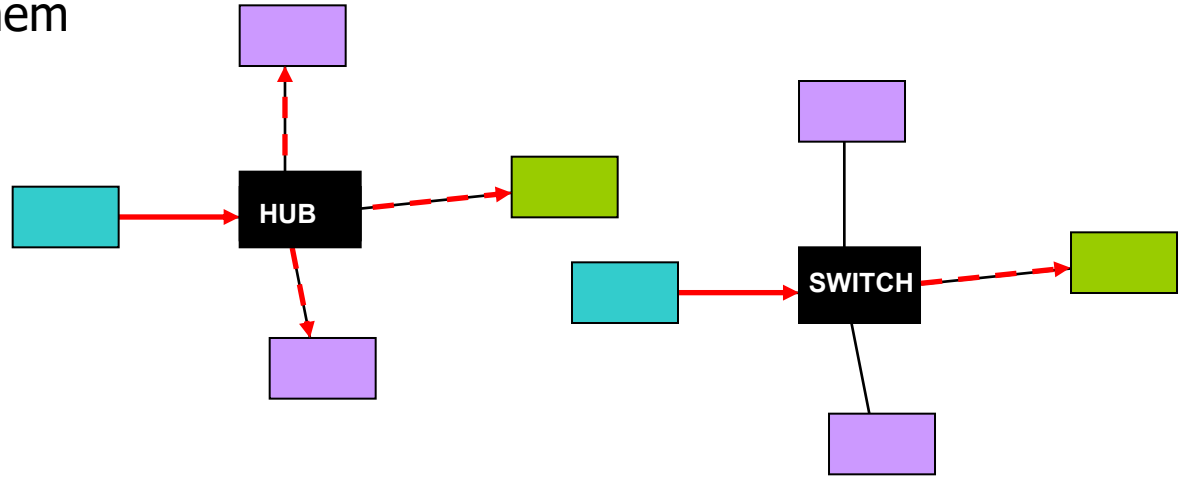
IP adresa

- IP adresa (logická)
  - např. 147.228.64.1 (každá část – rozsah 0-255)
  - omezený počet – 4 294 967 296 = 2^{32}
  - veřejná – celosvětově jedinečná
  - privátní
    - řeší problém nedostatku adres (např. podnikové sítě)
    - musí být skryty za překladačem síťových adres
  - speciální
    - 127.0.0.1 – lokální přístup
    - 255.255.255.255 – broadcast
- zjištění adres (Windows)
  - Start → Spustit… → cmd (příkazový řádek)
    - příkaz ipconfig /all
  - detaily všech síťových adaptérů včetně jejich MAC adres

Síťová zařízení 1

- přijímají a odesílají data z/do počítačové sítě

- hub (rozbočovač)
  - umožňuje větvení počítačové sítě
  - přijatý signál kopíruje všem připojeným zařízením
  - použití v hvězdicové topologii
  - nahrazován switchem



- switch (přepínač)
  - jako hub
  - přijatý signál kopíruje pouze na port zařízení, pro který je určeno

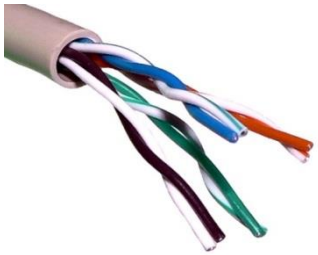
Síťová zařízení 2

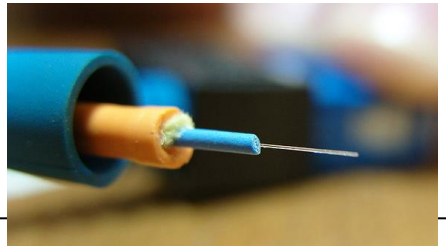
- repeater (opakovač)
  - přijímá zkreslený, zašuměný nebo jinak poškozený signál a opravený, zesílený a správně časovaný ho vysílá dále
  - zvyšuje dosah média bez ztráty kvality a obsahu signálu
- router (směrovač)
  - spojuje dvě nebo více sítí a přenáší mezi nimi efektivně data
- AP (Access Point)
  - umožňuje bezdrátové připojení

- zařízení kombinují funkce + různé možnosti konfigurace

Způsoby přenosu

- přenosová média
  - metalické kabely
    - kroucená dvoulinka
    - koaxiální kabely
  - optické kabely
    - odolné vůči elektro-magnetickému rušení





- bezdrátová spojení
  - rádiové spoje
    - bezdrátové sítě Wi-Fi
    - Bluetooth (10-100m ve volném prostoru)
    - ZigBee (do 75m)
    - mikrovlnné spoje (použití pro WAN)
  - optické spoje
    - infračervené spoje – televizní ovladač, mobilní telefon (do 1m)

Wi-Fi

- standard pro lokální bezdrátové sítě (Wireless LAN, WLAN)
- notebooky, tablety, PDA, mobilní telefony, tiskárny, …
- různé způsoby zabezpečení (kontrola IP adresy, WEP, WPA, WPA2, …)
- je-li síť k dispozici, zařízení se může připojit
  - zabezpečená síť – heslo, certifikát

- hotspot – místo, v němž je dostupné bezdrátové připojení do sítě Internet (kavárny, restaurace, …)
  - zabezpečený (heslo, certifikát)
  - nezabezpečený – připojit se může kdokoliv

Rychlost

- download × upload
- možnost změření – např. http://rychlost.cz
- konkrétní příklad
  - rychlost 12 036,17 kb/s (= 1 504,52 kB/s = 1,47 MB/s)
  - za 1 hodinu: 5 416,28 MB
  - za 1 den: 129,99 GB
  - film (DVD): 4GB → 46 minut

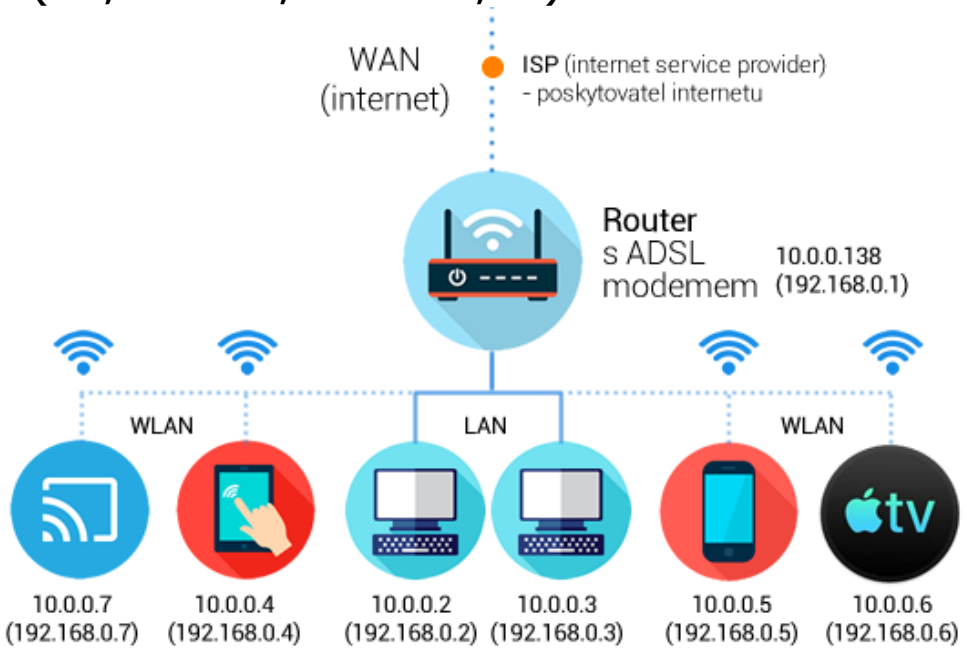
- *optika* *... Gb/s a víc*
- *lokální sítě* *... 100 Mb/s - Gb/s*
- *ADSL* *... do 10 Mb/s*

- *wifi* *... 54 Mb/s*
- *modem* *... 54 kb/s*
  (tel. linka)

Počítačová síť doma

- připojení k Internetu
  - modem, ADSL, Pilsfree, …
  - mobilní operátoři
- přímé připojení 1 počítače
  nebo
- switch + AP (zabezpečený, zaheslovaný)
  - připojení potřebných zařízení (PC, telefon, tiskárna, …)
  - kabel
  - Wi-FI

- zabezpečené počítače
  - antivir, firewall



Archivace a zálohování dat

- zálohování
  - záloha
    - „pojistka“, abychom o data nepřišli, kopie
    - životnost – několik dní, měsíců
  - vytváření bezpečnostní kopie dat / operačního systému
  - v případě ztráty dat obnovení stavu před vznikem poruchy
- archivace
  - archiv
    - data uložená na bezpečném místě, která jsou určena k pozdějšímu použití
    - životnost – desítky let
  - shromažďování informací pro případné pozdější použití
  - rychlé vyhledávání a třídění výsledků (důležité uspořádání, dlouhodobá spolehlivost a vysoká trvanlivost)

Zálohování

- zálohovat dřív, než bude pozdě
- zálohování by mělo probíhat automaticky a pravidelně
- důležitá data – ve 3 kopiích
  - jedna mimo vaši domácnost, například na cloudovém úložišti
- u fotografií nespoléhat pouze na Facebook nebo Instagram
  - ukládají fotografie v nízké kvalitě
- manuální × automatické
  - na manuální musíme něj myslet
  - automatické – nastavíme SW na určitý čas (např. každý den 12:00)
    - vestavěné nástroje MS Windows
    - bezplatný nebo placený zálohovací SW

Zálohování – kam?

- nespoléhat pouze na jeden typ, ale využívat více možností současně
- CD/DVD
  - \+ jednoduché, levné
  - – nedostatečná kapacita (4,7 GB nebo 8,5 GB), nízká životnost (několik let), nedostupnost mechaniky na moderních PC
- externí pevný disk, NAS
  - \+ cenově dostupný, spolehlivý, rychlý (některé)
  - – možnost ztráty nebo poškození
- USB flash disk
  - \+ jednoduchý, více variant (kapacita 2 GB až 4 TB), cenově dostupný
  - – snadná ztráta kvůli velikosti, těžká obnova poškozených dat, malá kapacita na uložení videa

- síťový disk (externí disk připojený přes LAN)
  - \+ dostupný z více zařízení současně, vysoká kapacita (TB), rychlý
  - – drahý, připojení kabelem, nutná pravidelná kontrola dat
- NAS (network access storage)/ NAS server
  - – server může obsahovat více disků v RAID poli – zrcadlení dat
  - \+ velká kapacita, možnost napojení na cloud, bezpečný přístup z internetu, další funkce (FTP, galerie, media server, …)
  - – vysoká cena, složitější nastavení, větší velikost a potřeba ho někde umístit, nutná pravidelná kontrola disků
- Cloud
  - – Kapacita 2-7 GB (volně), TB (po zaplacení)
  - \+ Přístup ze všech zařízení, data duplikovaná na různých místech po celém světě
  - – rychlost závisí na dostupnosti internetu, možné zneužití dat

Etické aspekty ICT

- ICT = informační a komunikační technologie
- etika
  - filozofická disciplína
  - určuje a rozlišuje co je špatné a dobré chování

- je třeba rozdíly mezi tím, co je:
  - správné
  - špatné
  - přijatelné
  - trestné

- svoboda projevu a právo na informace

Informační etika 1

- oblast morálky uplatňované při vzniku, šíření, transformací, ukládání, vyhledávání, využívání a organizaci informací
- určení a zdůvodnění morálních povinností lidí při předávání informací

- způsob nakládání s informacemi (např. zpřístupňování informací, odpovědnost za publikované informace)

- obecné zásady informační etiky:
  - informace by měly být volně šířeny
  - šíření informací by nemělo znamenat pro nikoho újmu
  - nepravdivé informace by neměly být šířeny
  - generovat nové informace je žádoucí
  - každý je odpovědný za důsledky svého jednání v informační oblasti

Informační etika 2

- řídí se stávajícími normami, tj. právním řádem, firemním etickým kodexem či společenským standardy

- problémové oblasti:
  - požadavek na ochranu soukromí x zajištění bezpečnosti občanů
  - právo na informace x ochrana soukromí
  - kontrola zaměstnavatelem x ochrana soukromí
  - obchodní tajemství x právo na informace
  - obchodování s osobními údaji
  - soukromí u veřejně činných osob
  - zabezpečení institucí a veřejných míst pomocí kamer apod.

GDPR (General Data Protection Regulation)

- obecné nařízení o ochraně osobních údajů
- kontroluje Úřad pro ochranu osobních údajů
- 99 bodů
- cíl – chránit osobní údaje občanů EU
- nařízením se musí řídit kdokoli, kdo působí v EU nebo zpracovává data občanů EU
- data musí být aktuální, uložená po nezbytnou dobu a za konkrétním účelem, zabezpečená, zpracovávaná zákonným způsobem
- ke zpracování dat musí být dán souhlas (ten může být odvolán)
- právo na informaci, která data jsou zpracovávaná, povinnost upravit, případně smazat z databáze
- data nesmí být bez zásahu člověka dostupná komukoliv

GDPR – kdo (fyzická nebo právnická osoba) s čím?

- osobní údaje
  - informace o konkrétní osobě, podle kterých ji lze identifikovat
  - *jméno, e-mailová adresa, telefonní číslo, rodné číslo, IP adresa, …*
- správce
  - sám nebo společně s jinými zpracovává osobní údaje
  - *každý, kdo má ve firmě zaměstnance, má databázi zákazníků, eviduje zájemce o své služby, má e-mailovou databázi nebo jinou evidenci*
- zpracovatel
  - zpracovává osobní údaje pro správce
  - *dodavatel mailového serveru, Google, …*
- třetí strana
  - není Správcem ani Zpracovatelem, ale je oprávněna osobní údaje zpracovávat
  - *obchodní partner, který využívá stejnou databázi*

GDPR – co?

- zpracování
  - jakákoliv operace s OÚ prováděná buď automaticky nebo ručně
  - operace související s kontaktem – od jeho získání až po vymazání
  - *shromažďování, ukládání do databáze, uspořádání, strukturování, mailování, úpravy, vyhledávání, …*
- profilování
  - automatické zpracování OÚ, na základě kterého je možné hodnotit skutečnosti o preferencích a chování člověka
  - *web/e-shop ukládá informace o tom, na kterých stránkách se člověk pohyboval, jak dlouho, zda objednal a podle toho upravuje nabídku*
- pseudonymizace
  - OÚ jsou zpracovávány tak, že není možné je přiřadit ke konkrétnímu člověku bez dodatečných informací, ty jsou ale zpracovávány odděleně
  - *data zašifrována pomocí speciálního klíče a tento klíč je uchováván odděleně (data nelze bez klíče přečíst)*

Počítačová etika

- počítačová etika
  - věnuje se společenským dopadům moderních počítačových technologií

- zákony týkající se počítačové etiky:
  - Zákon o ochraně osobních údajů v informačních systémech; č. 256/92 Sb.
  - Zákon o právu autorském; č. 121/2000 Sb.
  - Zákon o svobodném přístupu k informacím; č. 106/1999 Sb

- etické kodexy, které se tématikou zabývají
  - desatero počítačové etiky (formulováno The Computer Ethics Institute)
  - Netiquette (Netiketa) - sestavila Virginia Shea ve své knize Netiquette

Desatero počítačové etiky

- apel na mravní cítění člověka, který pracuje s počítačem, informacemi a informačními či komunikačními technologiemi
- soubor norem, žádné sankce při nedodržení
- zaměřují se na autorské právo

1. Nepoužiješ počítače ke škodě jiného.
2. Nebudeš ničivě zasahovat do práce druhých lidí.
3. Nebudeš slídit v souborech jiných lidí.
4. Nepoužiješ počítače ke krádeži.
5. Nepoužiješ počítače pro křivé svědectví.
6. Nepoužiješ nebo nepořídíš kopii softwaru, který jsi nezaplatil(a).
7. Nepoužiješ neoprávněně počítačového zdroje jiných lidí.
8. Nepřivlastníš si intelektuální dílo jiného.
9. Budeš přemýšlet o společenských následcích programu, který jsi stvořil(a).
10. Budeš používat počítače ohleduplně a s úctou.

Netiketa = etika na internetu

- = etika na internetu
- zabývá se především slušností, ohleduplností, respektování soukromí, ale nezdůrazňuje oblast autorských práv

1. Pamatuj na člověka
2. Drž se stejných standardů chování, jaké používáš v reálném životě
3. Měl bys vědět, kde se nacházíš
4. Respektuj čas ostatních lidí
5. Vybuduj si dobrou online pověst
6. Sdílej odborné znalosti
7. Pomáhej držet pod kontrolou flamewars
8. Respektuj soukromí ostatních lidí
9. Nezneužívej svou moc
10. Buď smířlivý k chybám jiných

Kybernetická bezpečnost = kyberbezpečnost

- ochrana v digitálním světě
- co nám hrozí na Internetu:
  - HOAX, SPAM
  - finanční rizika a podvody
    - phishing (podvodný e-mail), podvodný telefonní hovor
    - podvodné investice
    - falešné e-shopy a e-bazary
  - krádež identity, přístupů
    - malware (spyware, ransomware)
    - Zzeužití účtů (e-mail, sociální sítě, …)
  - další rizika
    - únik osobních dat
    - kyberšikana
    - kopírování platebních karet

SPAM

- hromadně rozesílaný e-mail či zpráva
- většinou reklama, ale také přílohy s viry či odkazy na stránky obsahující malware
- spamem nejsou obchodní sdělení, k jejichž zasílání dáme souhlas, například při nákupu v e-shopu
  - × dle zákona 480/2004 Sb. musí obsahovat odkaz s možností odhlášení odběru těchto e-mailů.

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!!!!!!!!!!!!!!!*

- https://www.hoax.cz

Phishing (rybaření)

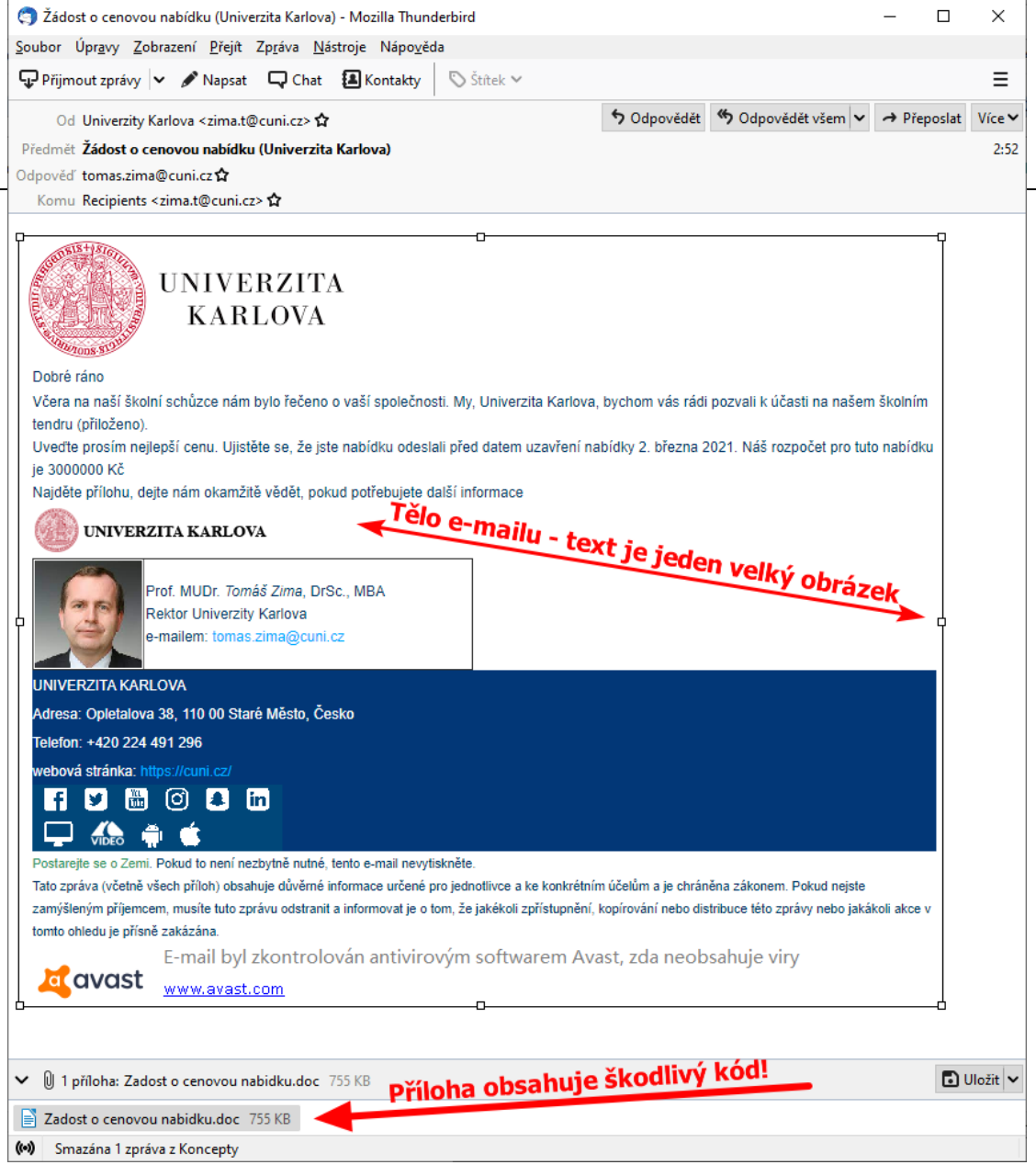
- obvykle email, ale může mít i podobu SMS nebo telefonního hovoru
- útočníci se vydávají za důvěryhodné subjekty (banka, pošta, e-shop, streamovací služba, …)
- cíl – vylákat citlivé údaje, přístup do bankovnictví, obchodní tajemství (*spear-phishing*) nebo peníze
- často odkazují na podvodné stránky – vypadají jako uživateli dobře známý web
- SMS mohou nabádat k instalaci aplikací či k potvrzení autorizačních zpráv např. z banky

Phishing

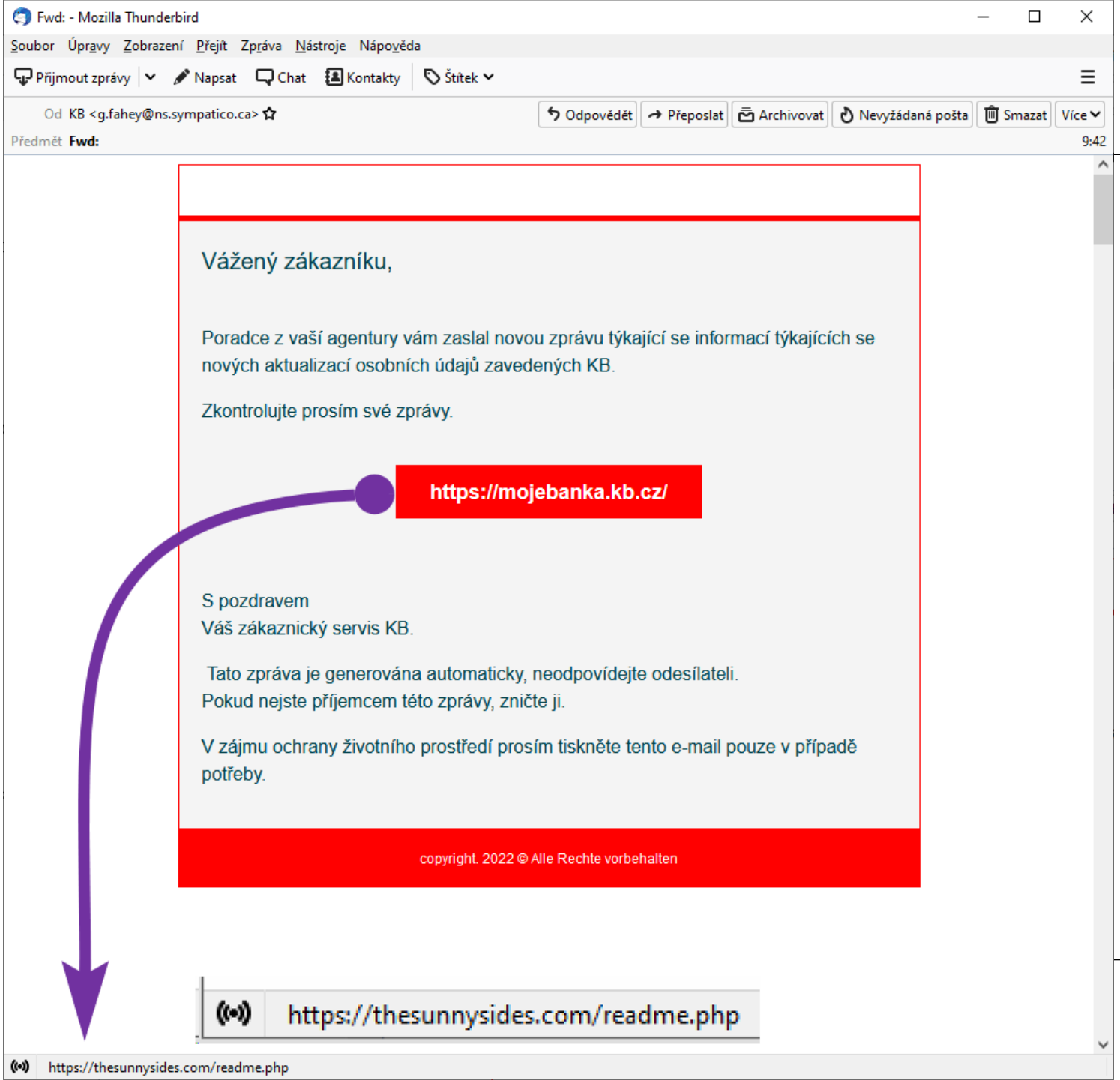
- využívá sociální inženýrství
  - lidský hacking – útok cílí na nejslabší článek zabezpečení – člověka a jeho „chyby" (důvěra, nepozornost nebo ochota pomoci, naléhavost a strach, lidská zvědavost a chamtivost, …)
- často se objevují:
  - Záměrné chyby v textu apod.
  - Nabídky finančního zisku, loterie 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)

Co mohou útočníci požadovat?

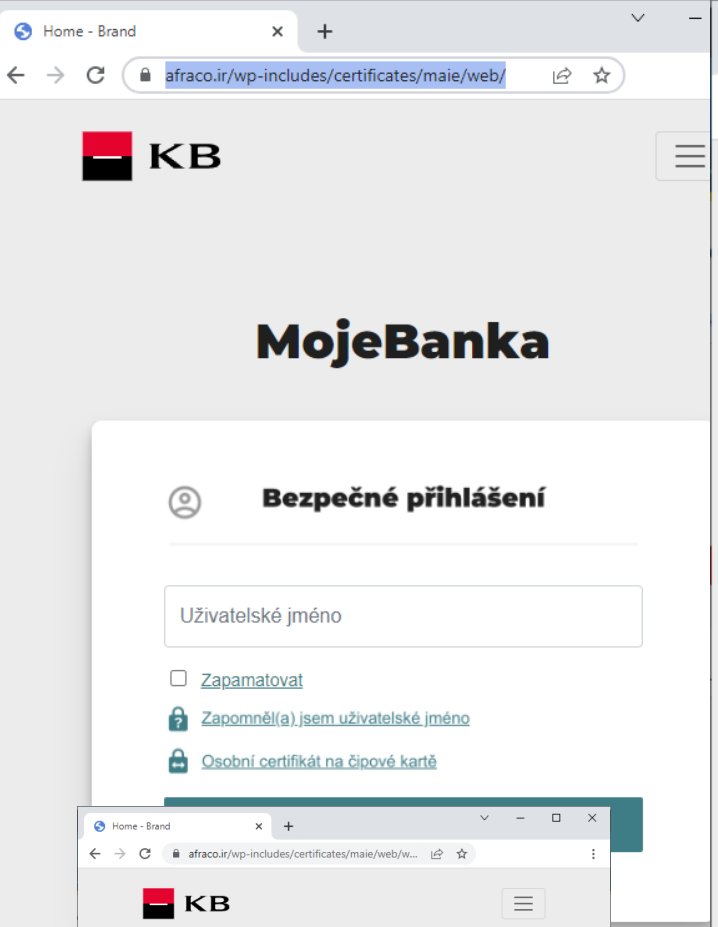
- uživatelská jména a hesla,
- rodná čísla,
- čísla bankovních účtů,
- kódy PIN,
- čísla platebních karet,
- jméno vaší matky za svobodna,
- datum narození, adresy,
- potvrzení ověřovací SMS
- nepřímá snaha o zaslání peněz
  - **Útočník:** *… žiji s malými dětmi na Ukrajině a je nám zima … pošli mi kamna, prosím …*
  - **Napadený:** *… poslání kamen je příliš drahé a komplikované … raději ti pošlu peníze a kamna si kup …*

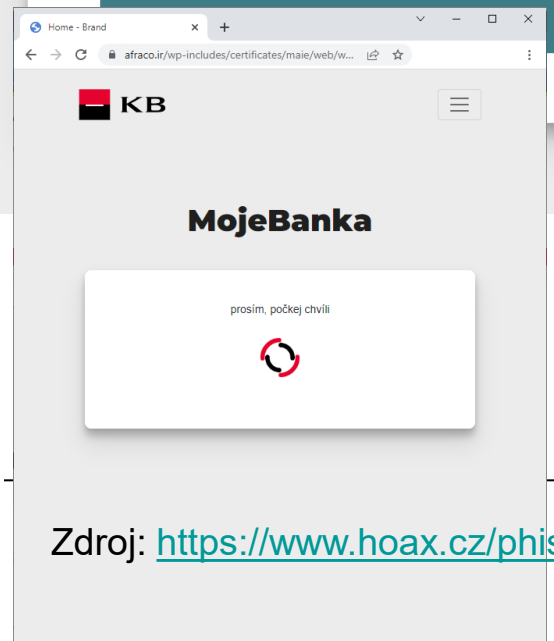


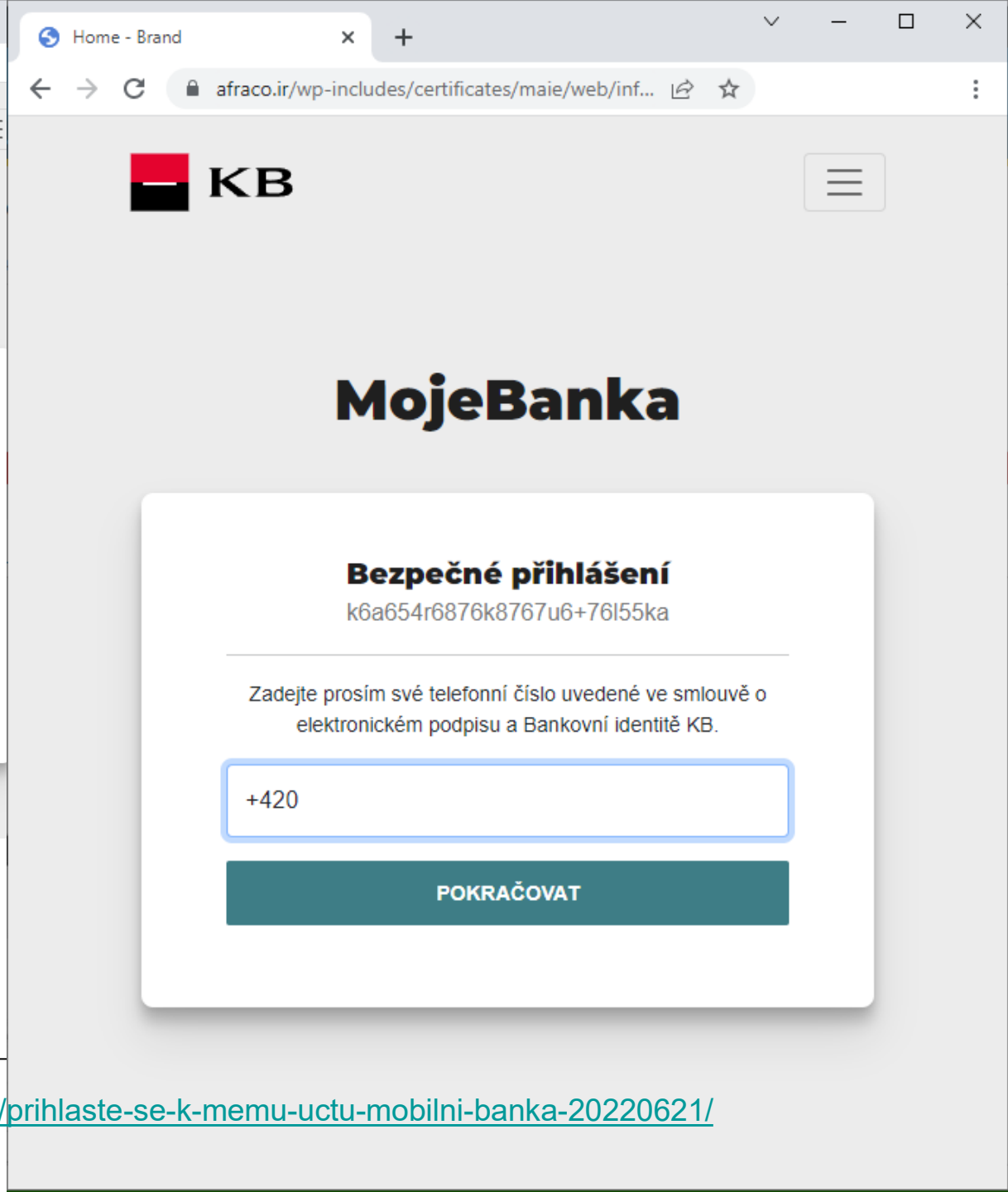
Zdroj: https://www.hoax.cz/malware/zadost-o-cenovou-nabidku-univerzita-karlova-20200326/



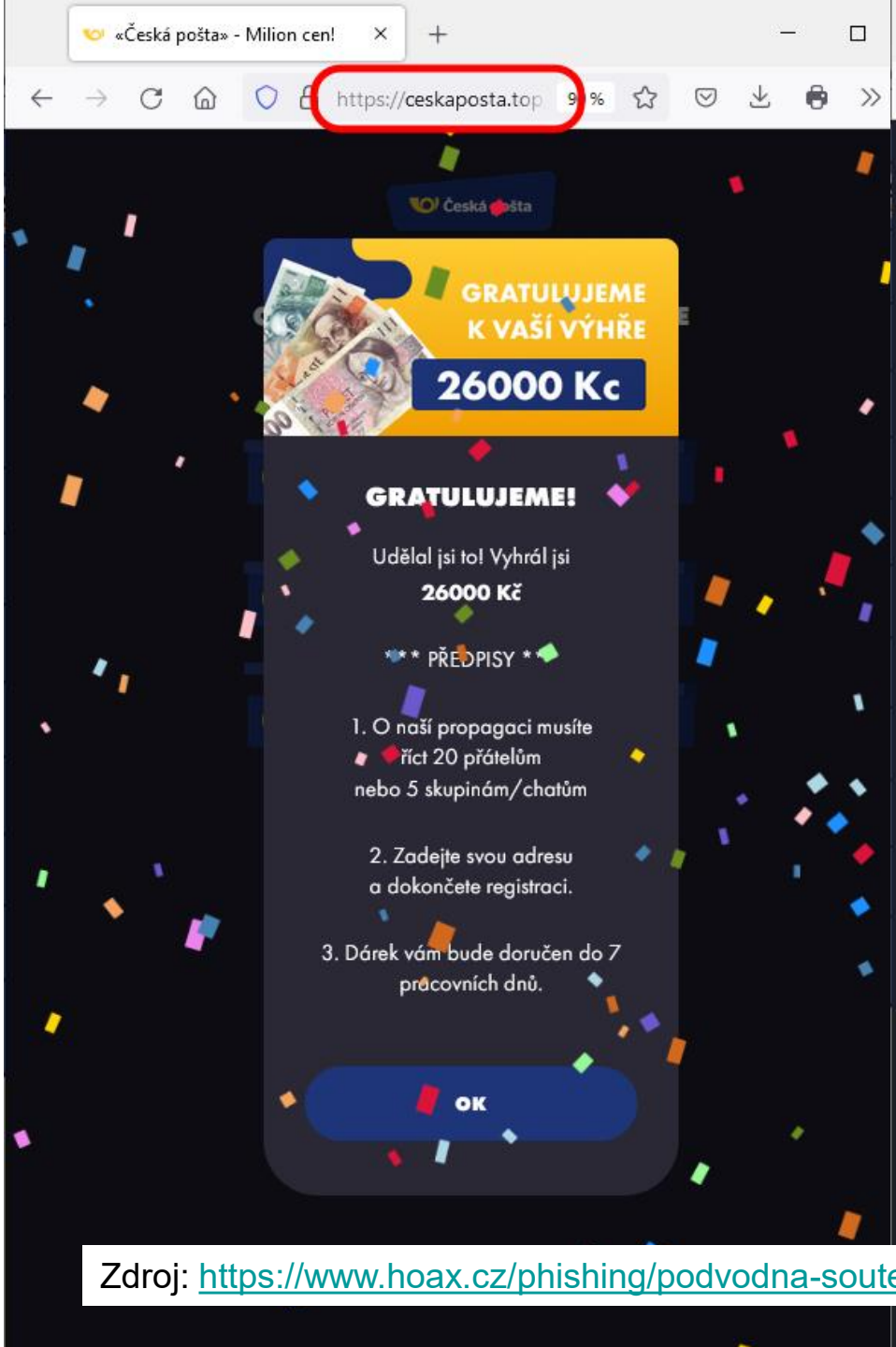
Zdroj: https://www.hoax.cz/phishing/prihlaste-se-k-memu-uctu-mobilni-banka-20220621/

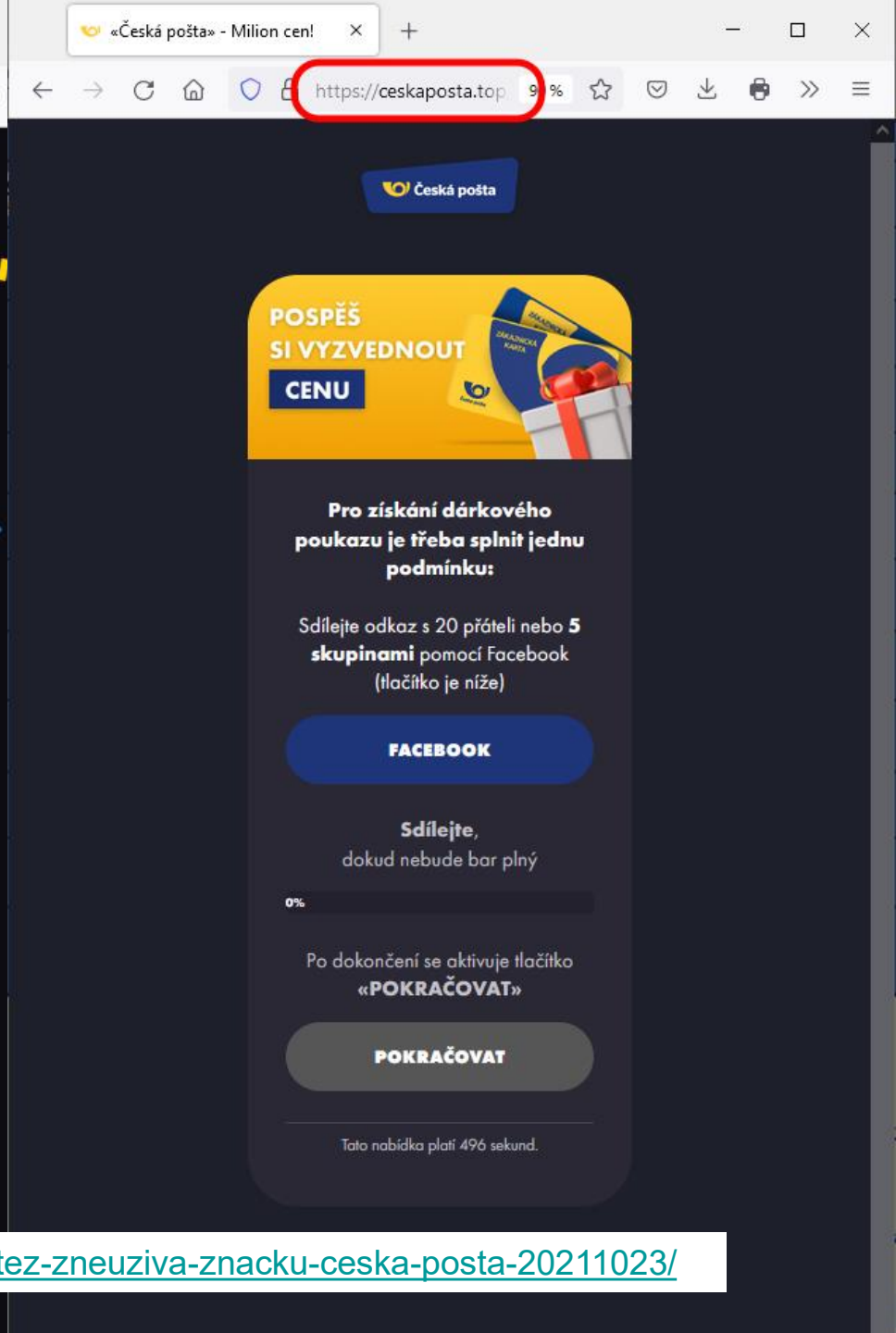




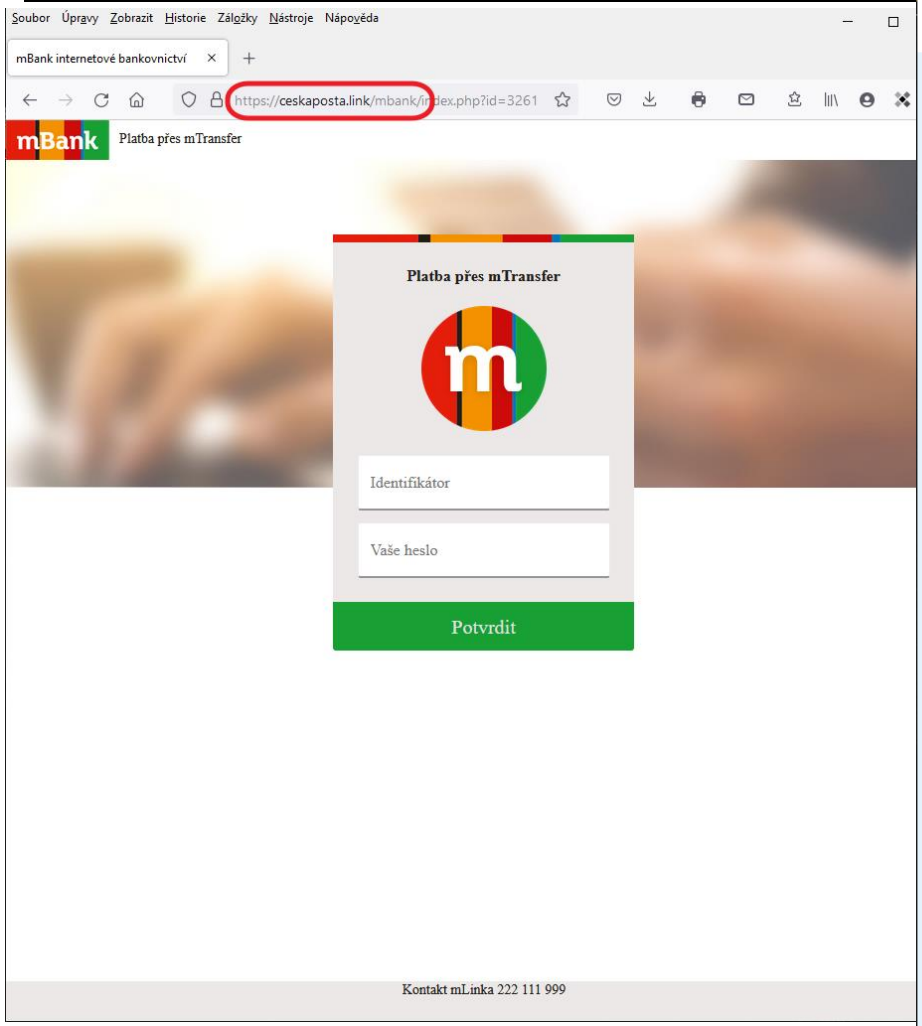


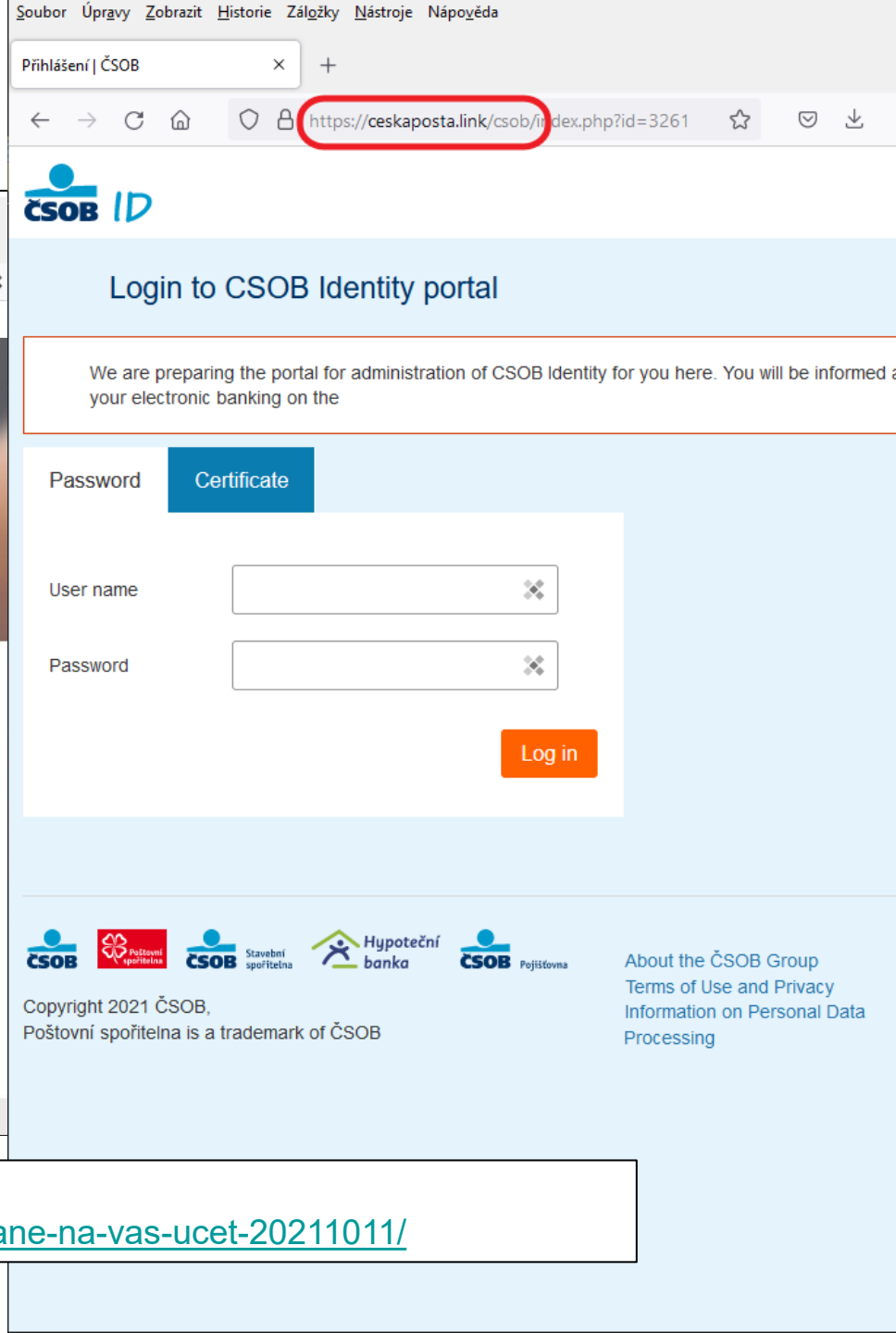
Zdroj: https://www.hoax.cz/phishing/prihlaste-se-k-memu-uctu-mobilni-banka-20220621/



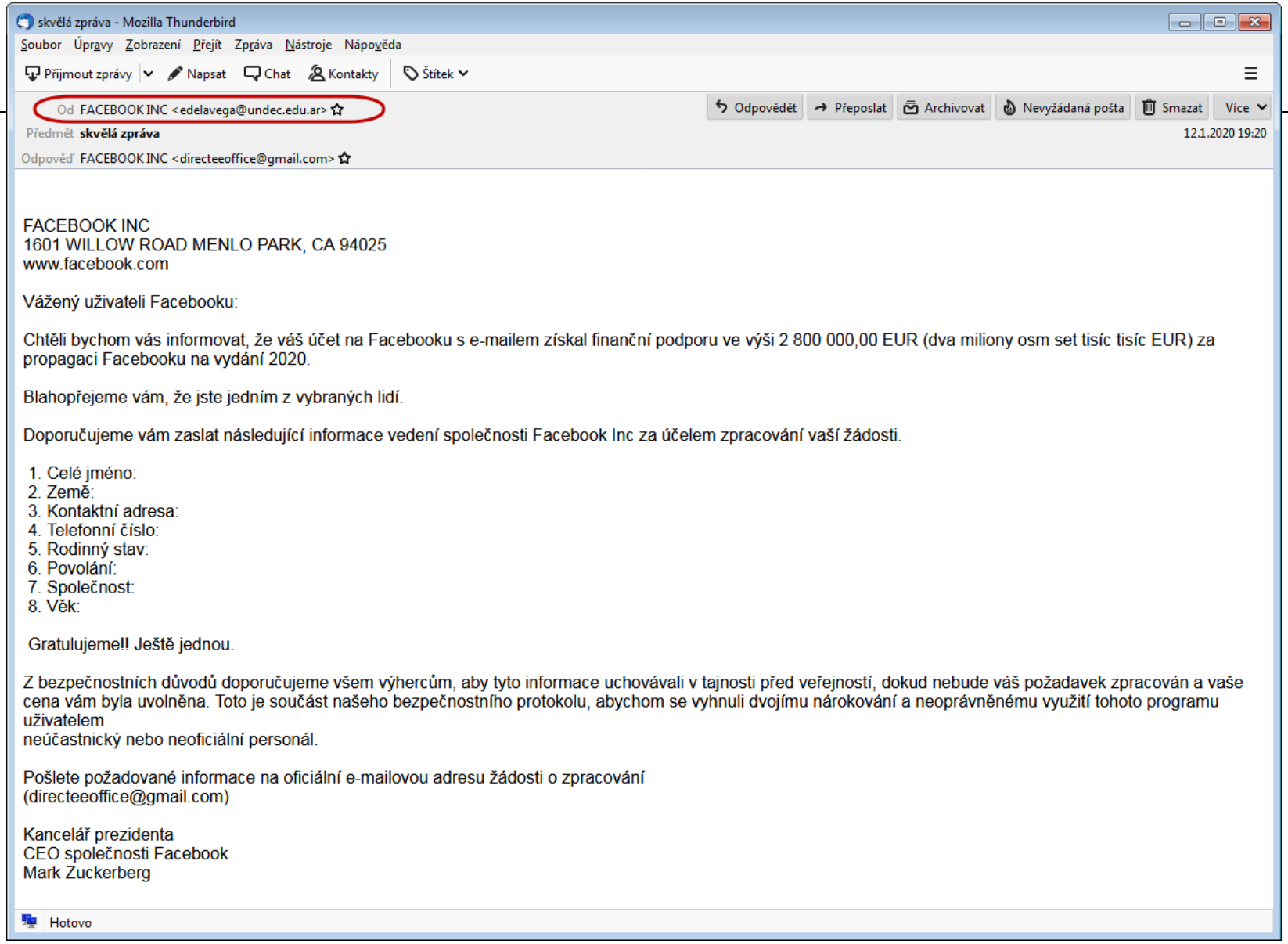


Zdroj: https://www.hoax.cz/phishing/podvodna-soutez-zneuziva-znacku-ceska-posta-20211023/





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



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/

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

Podvody v e-shopech, e-bazarech

- časté triky:
  - nakoupené zboží nedorazí, prodávající přestane reagovat
  - 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
- Co s tím?:
  - stražitost při podezřele nízké ceně
  - kontrolovat hodnocení/recenze e-shopu/prodávajícího
  - platit ideálně hotově při osobním převzetí a zkontrolování zboží
  - pro převod peněz na váš účet potřebuje kupující znát pouze číslo vašeho účtu
  - nikdy neklikat 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/

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

Malware

- *Malicious Software* – škodlivý software
- software navržený s cílem **napadnout, poškodit nebo neoprávněně získat přístup** k počítačovému systému, síti nebo datům, obvykle bez vědomí uživatele
- slouží ke krádeži dat, peněz, narušení provozu nebo získání kontroly nad zařízením
- různé způsoby přenosu
  - e-mailem – infikované přílohy nebo odkazy
  - stahování nelegálního obsahu nebo free programů z neověřených zdrojů
  - dírou v neaktualizovaném OS/aplikaci
  - fyzicky - infikované USB disky nebo jiné externí disky

Druhy malware 1

- viry (viruses)
  - připojuje k existujícím legitimním souborům (např. spustitelným programům, dokumentům) a šíří se, když je infikovaný soubor spuštěn nebo otevřen (vyžaduje k šíření aktivní akci uživatele)
  - cíl: poškodit data, smazat soubory, nebo infikovat celý systém
- červi (worms)
  - nemusí se připojovat k souborům a jsou samostatně replikovatelní
  - cíl: zpomalit síť (zahlcením provozem) nebo doručit a spustit další typy malwaru
- trojské koně (trojans)
  - maskuje se jako užitečný nebo neškodný software (např. hra, aktualizace, bezplatný program)
  - po instalaci (uživatelem) provádí škodlivé aktivity v pozadí
  - cíl: otevřít zadní vrátka (backdoor) pro vzdálený přístup, instalovat jiný malware nebo krást data

Druhy malware 2

- Ransomware (ransom = výkupné + software)
  - po infikování zašifruje všechna data na zařízení nebo v síti (znepřístupnění), následně požadavek výkupného (např. v bitkoinech) za klíč k jejich dešifrování (× není garance, doporučeno neplatit)
  - cíl: finanční zisk prostřednictvím vydírání (příp. tzv. dvojité vydírání – data nejprve ukradnou a hrozí jejich zveřejněním)
- spyware
  - tajně monitoruje a shromažďuje informace o uživateli a jeho aktivitě (navštívené webové stránky, stisky kláves, hesla)
  - cíl: krádež osobních údajů, bankovních přístupů a hesel
  - keyloggery – zaznamenávající stisky kláves
- adware
  - automaticky generuje, zobrazuje nebo stahuje nevyžádané reklamy (pop-up okna, bannery) často agresivní a obtěžující formou.
  - někdy součástí bezplatného softwaru
  - cíl: finanční zisk z reklamy

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/

Skimming – kopírování platební karty

- fyzicky – umístění zařízení přímo v bankomatu (na ústupu)
  - zakrývat klávesnici bankomatu při zadávání PIN kódu
  - před použitím bankomatu hledat podezřelé prvky
  - bezkontaktní výběr peněz (nevkládat kartu přímo do bankomatu)
- digitální
  - Napadení platebního formuláře, vložení škodlivého kódu -> zachycení údajů ke kartě
  - Náhodné přečtení NFC čipu bez kontroly biometrie
- ochrana
  - mít rozumně nastavené limity na kartě.
  - mít na účtu spojeném s kartou pouze minimální obnos financí.

Dobré rady (obecně)

- Obezřetnost na prvním místě.
  - pokud se nám něco nezdá, důkladně zkontrolovat
  - ďábel se skrývá v detailu
  - zejména pokud jde o časovou tíseň nebo je nabídka extrémně výhodná
- 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.
- Používejte silná hesla.

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

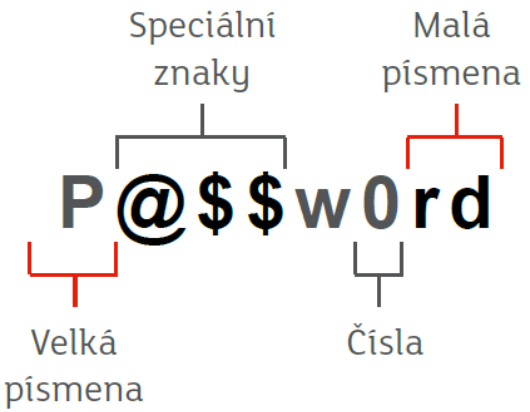
Ochrana počítače

- antivirový program (antivirus)
  - specializovaný software určený k vyhledávání, identifikaci, prevenci a odstraňování virů, červů, trojských koní a dalšího obecného malwaru
  - kontroluje soubory, které otevíráme, stahujeme nebo máme v počítači
  - virové slovníky, databáze – nutná pravidelná aktualizace
  - AVG, ESET NOD32, avast...

- firewall
  - bezpečnostní systém, který kontroluje a filtruje veškerý síťový provoz (data) putující mezi vaší sítí/zařízením a vnějším světem (internetem)
  - „digitální vrátný“
  - sledování komunikace na portech, blokování podezřelých programů
  - skrývá systém před nechtěnými skeny zvenčí, brání neoprávněným programům v odesílání dat
  - i součástí MS Windows

Hesla

- Při pocitu, že heslo bylo někým zneužito/odcizeno, ho okamžitě změnit
- používat silná hesla
  - min. 8 znaků
  - kombinace malých/velkých písmen, čísel a speciálních znaků.



- zvážení využití systému pro správu hesel (Lastpass, …)

Varování ve webovém prohlížeči

- 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

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/

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

?