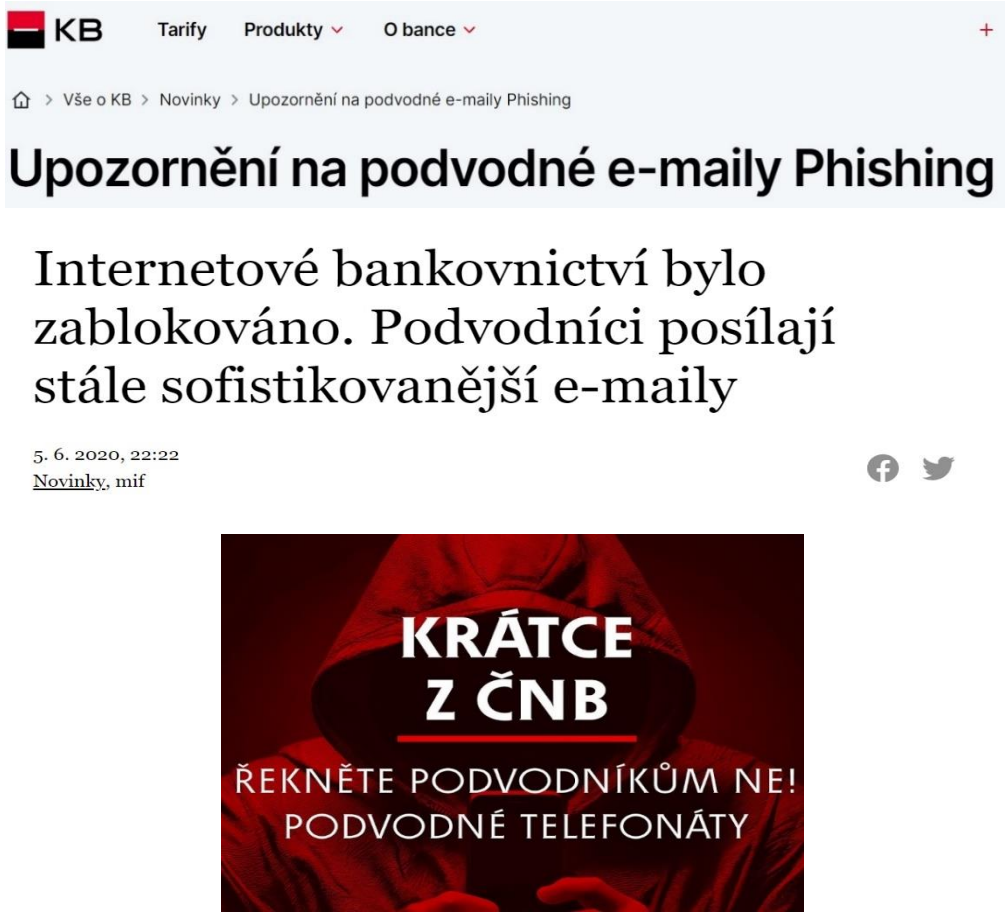
KYBERNETICKÉ ÚTOKY VŮČI KLIENTŮM BANK ZALOŽENÉ NA METODÁCH SOCIÁLNÍHO INŽENÝRSTVÍ: KDO NESE ODPOVĚDNOST ZA FINANČNÍ ZTRÁTU?

Anežka Karpjáková

15. 9. 2023

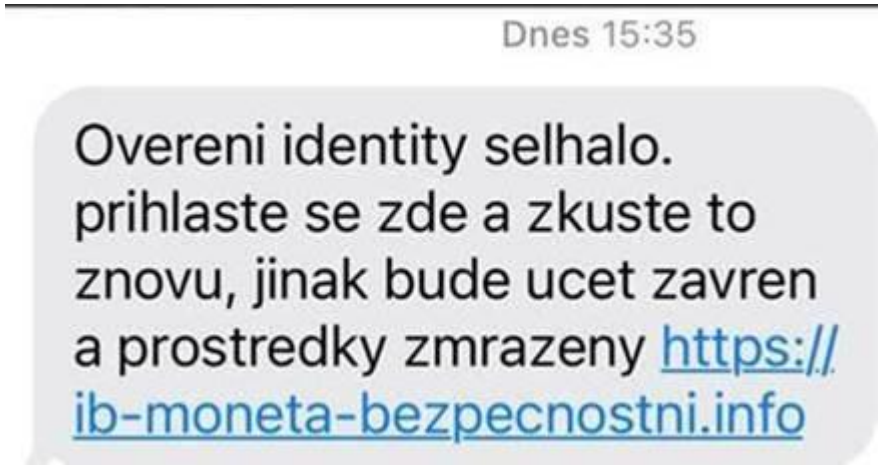
KYBERNETICKÉ ÚTOKY ZALOŽENÉ NA METODÁCH SOCIÁLNÍHO INŽENÝRSTVÍ

- Tzv. phishing
- Cíl útoků: zjištění citlivých údajů od klienta banky (např. přihlašovacích údajů do internetového bankovnictví, číslo účtu, kódu autorizační sms) za pomocí manipulativních praktik a po získání přístupu k finančním prostředkům klienta jejich převod na jiný účet.
- I přes značnou informační osvětu (média, NÚKIB, ČBA, ČNB, úvěrové instituce) počet úspěšných útoků rapidně narůstá.
- Za 1. půlrok 2023 celkem 31 323 nahlášených kybernetických útoků, 15 % nárůst oproti minulému roku.
- Průměrná finanční ztráta: okolo 25 000 Kč



NOVÉ TRENDY

- **Vyšší sofistikovanost a propracovanost útoků**
- **Nové metody:** spear phishing, vishing, smishing.
- **Využívání nových technologií:** spoofing, překladače založené na strojovém učení, deepfakes
- Nárůst případů, kdy se útočník vydává za „autoritu“ (např. PČR, ČNB, banku klienta)
- Neustálý vývoj nových postupů a praktik

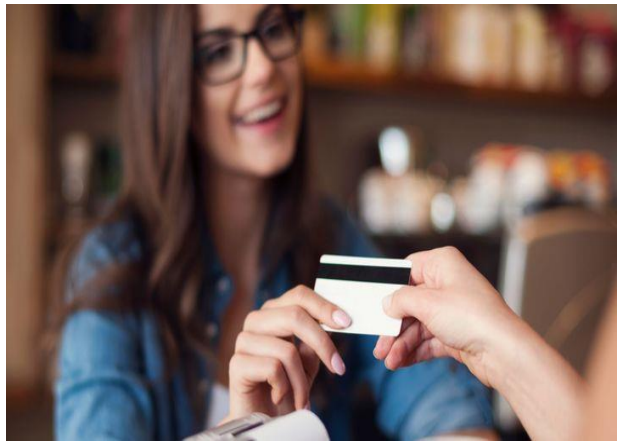


KDO NESE ODPOVĚDNOST ZA FINANČNÍ ZTRÁTY?

V daných případech lze uvažovat o třech subjektech:

Útočník

Banka (poskytovatel platebních služeb)



Klient (majitel účtu)

?

ODPOVĚDNOST ZA FINANČNÍ ZTRÁTU

- Podvodnou transakci provedenou útočníkem lze považovat za tzv. **neautorizovanou platební transakci** (tj. transakce provedena bez souhlasu majitele účtu).
- Upraveno v zákoně 370/2017 Sb., o platebním styku (dále jen „**ZoPS**"), vychází ze Směrnice EU 2015/2366, o platebních službách na vnitřním trhu (PSD2).
- Primární odpovědnost nese **banka**! Pov. vrátit danou částku zpět na účet klienta, na základě tzv. ***reklamace*** (§ 181 ZoPS)

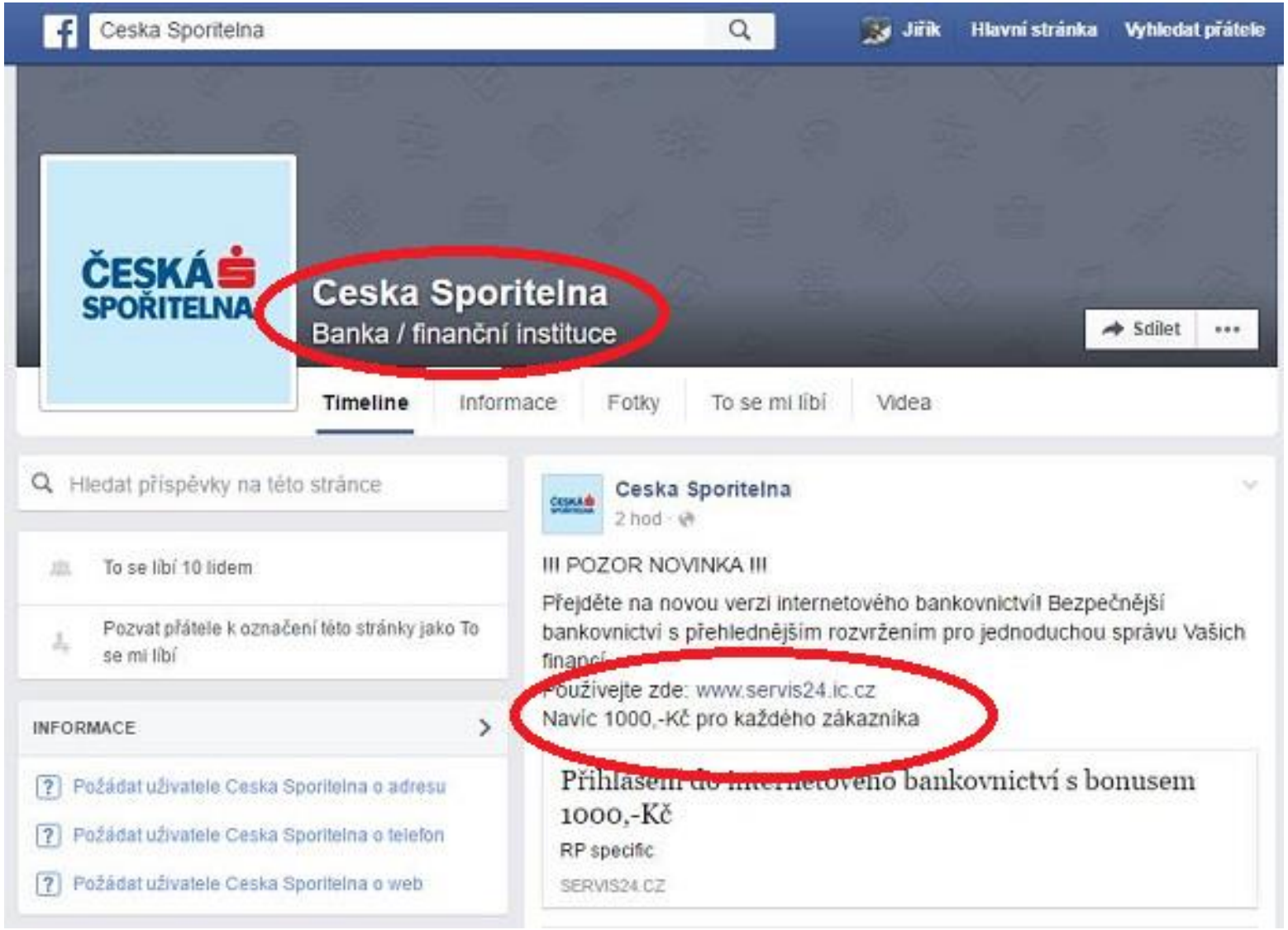
- **Výjimky z odpovědnosti banky** (§ 182 odst. 1 ZoPS):
  - Spoluúčast klienta ve výši 50 EUR, byla-li finanční ztráta způsobena použitím ztraceného nebo odcizeného platebního prostředku nebo **zneužitím platebního prostředku** (tj. internetového bankovnictví)
  - **Plná odpovědnost klienta,** způsobil-li tuto finanční ztrátu:
    - svým podvodným jednáním; nebo
    - tím, že úmyslně nebo z **hrubé nedbalosti** porušil některou ze svých zákonných povinností (tj. povinnost používat platební prostředek v souladu s rámcovou smlouvou, **zejména přijmout přiměřená opatření na ochranu osobních bezpečnostních prvků,** oznamovací povinnost bez zbytečného odkladu po zjištění zneužití platebního prostředku)

HRUBÁ NEDBALOST

- Hrubá nedbalost není v ZoPS ani NOZ definována.
- Nedbalost nejvyšší intenzity
- Hrubou nedbalost lze obecně vymezit jako ***„porušení náležité míry opatrnosti takovým způsobem , který se výrazně vymyká tomu, co je běžně akceptované. Hrubě nedbale jedná ten, tomu lze vytknout mimořádně výraznou míru neopatrnosti nebo lehkomyslnosti.***“
- Posouzení **vždy ad hoc!**
- Nedostatek relevantní judikatury, často však rozlišení mezi běžnou nedbalostí a hrubou nedbalostí spočívá v detailech.
- Ve vztahu k phishingovým útokům banky často specifikují ve svých smluvních podmínkách, které jednání klienta je považováno za hrubou nedbalost – to je pro posouzení hrubé nedbalosti **irelevantní.** Jedná se o právní pojem, který nemůže být modifikován dohodou smluvních stran!

DOSAVADNÍ PRAXE

- Banky v drtivé většině případů žádosti klientů o **reklamaci odmítají uznat** (odůvodnění: hrubá nedbalost, porušení smluvních podmínek)
- Úplná absence relevantní judikatury
- Nízký počet nálezů Finančního arbitra (FA):
  - doposud pouze **8 nálezů**
  - ve **všech** případech **zamítnutí** žádosti klienta, jelikož se dle FA klient banky dopustil **hrubé nedbalosti**
  - ve **všech** dosavadních případech se jednalo **o poměrně „jednoduché“ a méně propracované typy phishingových útoků** (např. reklama na FB, nedůvěryhodný e-mail - vyplnění identifikačních bezpečnostních údajů na falešné stránce „internetovém bankovnictví“ – následné kontaktování útočníkem na FB s žádostí o přeposlání autorizační SMS)
  - Často kumulace více závažných pochybení ze strany podvedeného klienta, jako např.:
    - opomenutí odlišné domény (př. namísto www.servis24.cz, falešná doména „sporitelna24_c_cz“ nebo „servis24.ic.cz“)
    - zprávy od útočníka obsahovaly gramatické chyby, překlepy
    - ignorace obsahu autorizační SMS
    - ignorace notifikací v internetovém bankovnictví upozorňující na dané typy útoků
    - opožděné oznámení útoku bance.


Ceska Sporitelna
Jiřík
Hlavní stránka
Vyhledat přátele
ČESKÁ SPOŘITELNA
Ceska Sporitelna
Banka / finanční instituce
Sdílet
Timeline
Informace
Fotky
To se mi líbí
Videa
Hledat příspěvky na této stránce
To se líbí 10 lidem
Pozvat přátele k označení této stránky jako To se mi líbí
INFORMACE
Požádat uživatele Ceska Sporitelna o adresu
Požádat uživatele Ceska Sporitelna o telefon
Požádat uživatele Ceska Sporitelna o web
Ceska Sporitelna
2 hod
III POZOR NOVINKA III
Přejděte na novou verzi internetového bankovnictví! Bezpečnější bankovnictví s přehlednějším rozvržením pro jednoduchou správu Vašich financí.
Používejte zde: www.servis24.ic.cz
Navíc 1000,-Kč pro každého zákazníka
Přihlášení do internetového bankovnictví s bonusem 1000,-Kč
RP specific
SERVIS24.CZ

BUDOUCÍ VÝVOJ?

- I přes neúspěch klientů bank v rámci dosavadní praxe FA se **nelze** domnívat, že ve všech případech úspěšných phishingových či obdobných útoků se jednání klienta bude považovat za hrubou nedbalost!
- Lze očekávat, že v budoucnu budou soudy či FA řešit případy sofistikovanějších typů těchto podvodů (např. případy spear phishingu nebo vishingu, kdy se útočník vydává za zaměstnance bank; útoky využívající deepfakes apod.)
- Očekávaná přísnější právní úprava: **Návrh Nařízení o platebních službách na vnitřním trhu** (zveřejněn v červnu 2023):
  - Nařízení se přímo věnuje otázce podvodů založených na metodách sociálního inženýrství
  - Obdobná právní úprava pro určení odpovědnosti v případě **neautorizované platební transakce**, avšak v případě hrubé nedbalosti klienta lze míru odpovědnosti klienta modifikovat!
  - ! Nově obsažena také úprava ***odpovědnost poskytovatele platebních služeb za podvody na základě vydávání se za zaměstnance banky*** !
    - Aplikace v případě **autorizovaných platebních transakcí**
    - Pouze pokud je klient spotřebitel
    - Podmínky: klient oznámí podvod bez zbytečného odkladu platební instituci i policii
    - Opět je stanoveny výjimky v případě podvodu a hrubé nedbalosti

DĚKUJI ZA POZORNOST

VZNIK TÉTO PREZENTACE BYL PODPOŘEN PROJEKTEM MUNI/A/1293/2022 (PRÁVO A TECHNOLOGIE XI).