Podvody v platebním styku a role České národní banky

Jan Frait, viceguvernér

Zuzana Silberová, ředitelka sekce dohledu nad finančním trhem

Česká národní banka

Podvodná jednání ve finančních službách jako aktuální fenomén a edukační aktivity ČNB

Jan Frait, viceguvernér

Česká národní banka

ČNB 30 ČESKÁ NÁRODNÍ BANKA

Obsah prezentace:

Úvod

- Z dohledové činnosti ČNB je zřejmé, že v roce 2022 docházelo na finančním trhu k nárůstu podvodných jednání ve finančních službách.
- Vysoký stupeň digitalizace finančních služeb na českém finančním trhu zvýšil atraktivitu tohoto trhu jako cíle útočníků.
- Nejčastěji útoky mířily na platební služby, jejichž poskytování se mj. v důsledku pandemické situace (COVID) přesunulo z významné části do on-line prostředí.
- Podvodná jednání se týkají i dalších finančních služeb – podvodné načerpání úvěru, podvodné investice, manipulace oběti k vložení hotovosti do kryptobankomatu atp.

Cíl útočníků a nebezpečnost podvodných jednání

- **Cíl útočníků – příjemci finančních služeb:**
  - spotřebitelé vč. zranitelných skupin spotřebitelů,
  - podnikatelé (FO i PO),
  - další subjekty – města, neziskové organizace, SVJ.

- **Nebezpečnost podvodných jednání zvyšují následující faktory:**
  - neustálé zdokonalování metod, scénářů útoku a manipulativních technik,
  - k podvodům dochází za nevědomé součinnosti podvedených osob,
  - podvodníci zneužívají jména autorit či osob, s nimiž jsou klienti ve smluvním vztahu.

ČNB se důrazně ohrazuje proti zneužití svého jména a jména svých představitelů a je připravena použít veškeré prostředky obrany proti podvodníkům, vč. úkonů v trestním řízení!

Nejčastější manipulativní techniky

- **Autorizace podvodných transakcí podvedenými osobami (uživateli)**
  - oběť útoku sama zadáním svých osobních bezpečnostní prvků v internetovém nebo mobilním bankovnictví potvrdí odchozí podvodnou transakci, často například v domnění, že potvrzuje příchozí transakci, nejčastěji:
    - úhradu za zboží
    - příjem přeplatku
    - výplatu sociální dávky aj.

- **Vylákání údajů z podvedených osob a jejich následné zneužití**
  - oběť útoku sdělí podvodníkům své osobní bezpečnostní prvky či je zadá do podvodné internetové stránky, umožní instalaci podvodné aplikace a tím odezírání zadaných údajů,
  - po získání údajů podvodníci údaje zneužijí např. k realizaci podvodných transakcí nebo k načerpání úvěru.

Nejčastější formy útoků

- **Phishing = útoky prostřednictvím podvodných odkazů**
  - způsob provedení: podvodné e-maily, chatovací aplikace, SMS zprávy (tzv. smishing)
  - typický scénář: oběť útoku uvěří, že útočník na bazarovém portálu nakoupí zboží, které oběť inzerovala, klikne na odkaz zaslaný v chatovací aplikaci a zadá své přihlašovací údaje do internetového bankovnictví. Dále dle instrukcí útočníka autorizuje platby, o kterých se domnívá, že jsou příchozí (ve skutečnosti však odchází z účtu oběti).

- **Vishing = útoky prostřednictvím telefonických hovorů**
  - způsob provedení: navolávání obětí (často v noci s využitím jejich zmatenosti)
  - typický scénář: útočník v oběti vyvolá strach (např. tím, že oběť uvěří, že jí byl napaden účet). Oběť podlehne nátlaku a potvrdí připojení podvodného zařízení ke svému účtu. Útočník pak sám odesílá podvodné transakce přímo z účtu oběti.

Hlavní činnosti ČNB v oblasti prevence před podvody

- Výkon dohledu nad poskytovateli a zprostředkovateli finančních služeb
- Spolupráce s ostatními subjekty státní správy a profesními organizacemi
- Zapojení do legislativních a reportingových aktivit na evropské i národní úrovni
- Přijímání a vyřizování podnětů veřejnosti a jejich využití pro dohledovou činnost
- Vydávání upozornění pro veřejnost
- Posilování finanční a ekonomické gramotnosti veřejnosti – zapojení do edukačních aktivit

Edukační aktivity k podvodům v platebním styku na webu ČNB

ČNB připravila novou stránku o podvodech na webu www.penizenauteku.cz.

- Vysvětlení nejčastějších technik útočníků, příklady podvodů, nejčastější scénář podvodů, návod k chování v případě útoku, zásady obezřetného chování, postup v případě, že je útok dokonán.

ČNB zveřejnila video varující před vishingovými podvody.

- Srozumitelný návod, jak útokům předcházet, jak je poznat a jak se jim bránit.

ČNB ČESKÁ NÁRODNÍ BANKA 30

Děkuji za pozornost

Jan Frait
viceguvernér ČNB

#řeknětepodvodníkůmNE

Výkon dohledu v oblasti prevence podvodů v platebních službách

Zuzana Silberová, ředitelka sekce dohledu nad finančním trhem

Česká národní banka

Obsah prezentace

1. Prevence před podvody jako průřezové téma
2. Dohledová činnost ČNB
3. Dohledová činnost v oblasti obezřetnosti
4. Dohledová činnost v oblasti AML/CFT
5. Dohledová činnost v oblasti odborné péče
6. Závěrečné shrnutí

Prevence před podvody jako průřezové téma

- ČNB vnímá téma podvodů ve finančních službách a jejich prevenci jako průřezové téma, kterému věnuje zvýšenou pozornost.
- Spolupráce s ostatními autoritami:
  - na evropské úrovni: spolupráce s orgány EBA, ESMA, EIOPA
  - na národní úrovni:
    - NÚKIB
    - FAÚ
    - Veřejný ochránce práv
    - Finanční arbitr
    - Orgány činné v trestním řízení
- Prevence před podvodnými jednáními se dotýká mnoha činností ČNB (regulatorní, dohledové, edukační, statistické, peněžní).

Dohledová činnost ČNB

Důležité cíle dohledové činnosti v oblasti platebního styku:

- zajištění bezpečného provádění platebního styku
- zajištění dodržování pravidel odborné péče ve vztahu ke klientům

ČNB při dohledu nad činností úvěrových institucí dlouhodobě klade důraz na řádné nastavení řídicího a kontrolního systému úvěrových institucí, vč. zavádění účinných mechanismů, kterými samy úvěrové instituce mohou podvodným jednáním v oblasti finančních služeb předcházet.

Metody a nástroje výkonu dohledu

Dohled na dálku:

- provádění dohledových šetření
- vyhodnocování informací a identifikace možných rizik
- sledování a vyhodnocování opatření k nápravě

Kontrola na místě:

- podrobnější ověřování funkčnosti procesů a dodržování právních předpisů zejména na vzorcích kontrolních případů
- ověřování informací získaných dohledem na dálku v praxi dohlížených institucí

Dohledová činnost v oblasti obezřetnosti

- **ČNB prověřuje robustnost a odolnost systémů a postupů finančních institucí**
  - Finanční instituce robustnost a odolnost systémů posilují, a to implementací bezpečnostních nástrojů a procesů, které jim umožní podvodná jednání monitorovat a do omezené míry jim předcházet.

- **Řízení rizika v souvislosti s podvody ve finančních službách je jedním ze vstupů do celkového hodnocení rizikového profilu finanční instituce (SREP)**

Dohledová činnost v oblasti AML/CFT

ČNB prověřuje zejména nastavení řídicího a kontrolního systému finančních institucí v oblasti prevence legalizace výnosů z trestné činnosti, mj. v souvislosti s podvodnými jednáními.

Důraz je kladen na zavedení a udržování řídicího a kontrolního systému pro dodržování povinnosti finančních institucí v souvislosti s:

- prováděním identifikace a kontroly klienta a
- odhalováním podezřelých transakcí.

Dohledová činnost v oblasti odborné péče – I

ČNB dohlíží na dodržování informačních povinností, např. aby finanční instituce:

- důsledně informovaly své klienty o aktuálních hrozbách v souvislosti s poskytováním finančních služeb, včetně vzorců podvodného jednání,
- zvyšovaly bezpečnostní povědomí uživatelů a informovaly o opatřeních, které sami klienti mají přijmout za účelem ochrany svých osobních bezpečnostních prvků a peněžních prostředků a
- informovaly o postupu v případě, že se klienti stanou obětí podvodu.

Dohledová činnost v oblasti odborné péče – II

ČNB dále dohlíží na dodržování dalších povinností:

- Postup finančních institucí směřující k eliminaci škod v případě, že již k podvodnému jednání došlo, včetně:
  - dodržování povinnosti umožnit klientům kdykoli blokovat platební prostředky,
  - spolupráce úvěrových institucí a poskytování součinnosti orgánům činným v trestním řízení tak, aby mohlo dojít k následnému zajištění podvodně získaných peněžních prostředků.

Pro výkon dohledu v oblasti odborné péče jsou jedním z relevantních zdrojů informací o podvodech na finančním trhu podání veřejnosti.

ČNB však nerozhoduje soukromoprávní spory mezi finančními institucemi a klienty. Zde je dána příslušnost finančního arbitra nebo soudu.

Závěrečné shrnutí: Řekněte podvodníkům NE!

ČNB apeluje na veřejnost, aby dodržovala bezpečnostní zásady a svým obezřetným jednáním předcházela podvodům a vzniku škody. Společně, tj. klienti, finanční instituce, ČNB a další autority pak zabráníme tomu, aby finanční trh ČR byl cílem útočníků.

- **Nespěchat** – nedělat unáhlená rozhodnutí. Nepodlehnout tlaku, pod který podvodník svou oběť záměrně dostává.
- **Ověřovat –** zda skutečně mluvíte s bankou, například zavěšením a zavoláním na oficiální infolinku banky. Zvážit možnost podvodu.
- **Chránit –** nikomu nesdělovat přihlašovací údaje do svého IB/MB, karetní údaje či jiné údaje, které by mohly být zneužity. Dodržovat bezpečnostní zásady dohodnuté s bankou.
- V případě dokonaného podvodu okamžitě kontaktovat banku, blokovat platební prostředky a oznámit podvod Policii ČR.

.

Děkuji za pozornost

Zuzana Silberová
ředitelka sekce dohledu nad finančním trhem ČNB

#řeknětepodvodníkůmNE

ČNB 30 ČESKÁ NÁRODNÍ BANKA

EXTRA SLIDY

Fáze útoku: příklad vishing

- **Důvěra**
  - Volající vzbudí pocit důvěryhodnosti – vydává za vaši banku, Polici ČR, ČNB – jde o autoritu či někoho, s kým jste ve smluvním vztahu. Název jeho pozice zní reálně, přestaví se vám jménem, telefonní číslo vypadá jako infolinka dané instituce. Důvěryhodnost volajícího může být zvýšena tím, že o vás má informace – např. na základě předchozího telefonního hovoru ví, která banka vede váš účet.
- **Emoce**
  - Útočník cílí na strach/radost a používá psychický nátlak, působí naléhavě – snaží se vás přesvědčit, že je třeba rychle jednat, abyste zabránili škodě (např. hrozícímu podvodu na vašem účtu), zrušili blokaci vašeho účtu či zabránili tomu, aby si na vás někdo vzal úvěr; telefon může zazvonit v noci, kdy spíte (útočník využívá zmatenosti) či v jinou nevhodnou dobu.
- **Manipulace**
  - Útočník vás donutí, často velmi profesionální cestou, sdělit vaše přihlašovací údaje či umožnit připojení podvodného zařízení k vašemu účtu či k jinému jednání.
- **Ztráta**
  - Útok je dokonán, útočník provedl podvodnou transakci či si vzal úvěr.