PHISHING A PROBLÉMY S JEHO TRESTNĚPRÁVNÍ KVALIFIKACÍ V TEORII A PRAXI

JIŘÍ KRUPIČKA

1. ÚVOD

Internet v mnoha ohledech usnadňuje každodenní život velké většiny obyvatelstva a lze bez nadsázky říci, že si již život bez něj dokážeme představit jen stěží. Krok za krokem se na něm naše společnost stala závislá. Internet nepřinesl však jen samé výhody, stejně jako dobře slouží naší společnosti, tak podobně dokáže posloužit i zločinu. Jednou z konkrétních podob tohoto nebezpečí je phishing, jímž se podrobněji zabývá tento příspěvek.

Phishing je jako druh kybernetické kriminality v mnoha ohledech specifický. Na jedné straně se v podstatě jedná jen o podvodné jednání, na druhou stranu jeho zvláštní charakter profitující z výhod, které nabízí internetové prostředí, jej od jiných druhů podvodů známých s reálného světa zcela zásadně odlišuje. Phishing tak stojí na pomezí mezi tzv. přímou internetovou kriminalitou, u které kriminální aktivity nemají obvykle výrazně podobný ekvivalent mimo kybernetický svět, a internetovou kriminalitu nepřímou, u níž naopak nelegální aktivity zcela existují i ve světě fyzickém.

Toto ambivalentní postavení phishingu pak může někdy činit potíže i při jeho trestněprávní kvalifikaci. Je to dáno zejména nesprávným pochopením tohoto druhu kriminality, popř. konkrétního způsobu spáchání trestného činu. Cílem tohoto příspěvku je proto jednak v krátkosti tento jev popsat, srovnáním jeho historických předchůdců vysvětlit způsob jeho fungování a následně na konkrétním příkladu poukázat na nesprávné právní vyhodnocení tohoto jevu orgány činnými v trestním řízení. Jelikož předkládaný případ se stal ještě za účinnosti starého trestního zákona, bude v poslední části tohoto příspěvku věnována pozornost stávající trestně právní kvalifikaci phishingu podle nového trestního zákoníku, neboť ten na poli kybernetické kriminality přinesl některé významné změny.

2. PHISHING JAKO FENOMÉN

2.1 DEFINICE PHISHINGU

Phishing může být definován jako kriminální jednání, jehož cílem je prostředky elektronické komunikace podvodně získat či vylákat citlivé informace, jako jsou přihlašovací jména, hesla a údaje o kreditních a debetních kartách, tak, že se pachatel maskuje za důvěryhodnou osobu či organizaci.[1, 2]

Etymologicky tento pojem vychází z anglické parafráze na slovo „fishing", tedy „rybaření".[3] Důvod je zřejmý. Pachatel phishingu vhazuje své oběti návnadu, na kterou se jí snaží „chytit". Zároveň rybaření odpovídá phishingu i v tom, že stejně jako případný pachatel i rybář ví, že se na jeho návnadu všechny ryby v rybníce nechytí. Oběma však bohatě postačí, když alespoň nějaká oběť jejich lovu na jejich návnadu zabere. V literatuře se někdy lze setkat s českým překladem slova phishing v podobě „rhybaření",[4] ten se však u široké veřejnosti neujal a obvykle se tento jev i v českých podmínkách označuje původním názvem z angličtiny.

Podstatou phishingu je využívání tzv. sociálního inženýrství. To zahrnuje umění získat pomocí určitých psychologických technik citlivé údaje či další informace od oběti samotné.[5] Pachatel se tak často snaží získat důvěru oběti, která pak potřebné informace či údaje vlastně sdělí dobrovolně.[6] Tuto důvěru může získat buď bezprostředním kontaktem, což však od pachatele vyžaduje velkou míru odvahy a sebejistoty, nebo pomocí prostředků elektronické komunikace.[7] Tato varianta na pachatele neklade zdaleka tak vysoké nároky na komunikační a rétorické schopnosti, navíc skýtá velkou míru anonymity. Potenciální pachatel navíc může těžit z masovosti sítě elektronických komunikací, která mu umožňuje napadnout naráz obrovské množství potenciálních obětí. Děje se tak např. elektronickou poštou, na různých internetových diskusních fórech, sociálních sítích či na vlastních webových stránkách.

2.2 PŘEDCHŮDCI PHISHINGU

O phishingu jako takovém se začíná hovořit až s rostoucím rozvojem internetu v druhé polovině 90. let minulého století a zejména s rozmachem elektronického bankovnictví, na které bývá phishing často zaměřen. Je však zřejmé, že phishing měl své předchůdce ještě v dobách, kdy internet v dnešní podobě vůbec neexistoval. Sociální inženýrství se totiž neomezuje, jak už bylo řečeno, pouze na elektronický svět. Jedním z prvních předchůdců dnešního phishingu bylo jednání známé pod ná-

---

1 CHOO, K.-K. R. Cyber threat landscape faced by financial and insurance industry. *Trends & issues in crime and criminal justice series*, 2011, č. 408, s. 3.
2 Podobně též VOLOVECKÝ, P. Kybernetické hrozby a jejich trestně právní kvalifikace. *Trestní právo*, 2011, roč. 15, č. 1, s. 15.
3 DUMAS, B. M. *Information Technology and Society*. Routledge, 2012, s. 169.
4 Srov. např. BAUDIŠ, P. Staronové nebezpečí Rhybaření. *CHIP.CZ*, 2006, č. 4, s. 14 n.
5 ČEPIČKA, D., ARNOLD, A., BEHRENS, D. Odhalte triky hackerů. *PC WORLD*, 2007, č. 12, s. 68 n.
6 WORKMAN, M. Gaining Access with Social Engineering: An Empirical Study of the Threat. *Information Systems Security*, 2007, č. 16, s. 316.
7 Idem., s. 321.

zvem španělský vězeň. Toto podvodné jednání sahá až do druhé poloviny 19. století[8] a bylo dokonce podrobně literárně zpracováno v povídce Arthura Traina z roku 1910.[9] Jeho podstatou je přesvědčení oběti, že jistý velmi bohatý vězeň bude ochoten se o své bohatství podělit, pokud prostřednictvím svého důvěrníka obdrží určitý obnos na podplacení stráží, které jej vězní. Poté, co oběť požadovanou částku důvěrníkovi zaplatí, se objeví neočekávané komplikace, pro které bude třeba uhradit další a další prostředky. Jediného, čeho se pak oběť tohoto podvodu dočká, je přivedení sebe sama na mizinu.

V dnešní době by se na takovou báchorku nechal nachytat asi málokdo. Stačí však příběh jen trochu pozměnit, aby zapadl do dnešního světa, a je na světě velice rafinované podvodné jednání, které v malých obměnách dokázalo způsobit obrovské škody. Právě španělským vězněm se totiž beze zbytku inspirovali tvůrci tzv. nigerijských listů, také známých pod označením „419 scam“[10].[11] V tomto případě pachatelé využívají obecně nízkou povědomost osob o politickoekonomické situaci v západoafrických zemích. Záminka pro samotné vylákání peněz je různá. Někdy to bývá převedení mnohamilionových částek z „mrtvých kont“ po obětech nebo svržených diktátorech po proběhlé občanské válce v Nigerii či jiné africké zemi. Podobnou zástěrkou je příběh místních bohatých podnikatelů a farmářů, kteří jsou po převratu ohroženi na životě a majetku, a tak se rozhodli emigrovat, přičemž nechtějí za sebou zanechat veškerý poctivě a namáhavě vydělaný majetek. Stejně jako u španělského vězně se však záhy objeví problémy – např. nutnost založit konto v místní bance, na které budou nejprve peněžní prostředky přeposlány, potřeba zaplatit poplatek finančnímu úřadu, poplatek za převod samotný, atp. Tyto taktiky vždy spoléhají na zákonitosti fungování lidské psychiky, kdy oběť v okamžiku, kdy se rozhodne prvotní částku zaplatit, není ochotna se své investice vzdát a neustále následuje vidinu snadného zbohatnutí. Jak se zvyšuje částka, kterou oběť pachatelům poskytla, je stále obtížnější ztrátu přijmout a naopak roste (částečně ze zoufalství) očekávání, že právě poslední splátka byla ta opravdu poslední a nyní bude již jen následovat sladká odměna.

Samotné nigerijské listy by měly, pokud by byly využívány pouze klasické prostředky komunikace (např. dopisy), pouze omezený rozsah. Co však z nich učinilo celosvětovou hrozbu, je elektronická pošta. Ta totiž umožňuje rozesílat podvodné dopisy (pod jakoukoliv záminkou k vylákání peněz) neomezenému počtu adresátů. Tím tento způsob podvodů vydláždil cestu phishingu.

Jak již bylo uvedeno výše, pozadí, za kterým se skrývá podvodné jednání, může nabývat nejrůznějších podob. Autor tohoto příspěvku sám čelil poměrně rafinovanému podvodnému útoku, a to při nákupu ojetého mopedu na německých serverech sdružujících inzeráty potenciálních prodávajících. Poté, co autor (německy) odpověděl na inzerát k prodeji skútru za cca 850 €, což byla cena sice výhodná, avšak nikoliv nereálná, přišla od „majitele“ motocyklu tato e-mailová odpověď:

---

[8] AN OLD SWINDLE REVIVED. The “Spanish Prisoner” and Buried Treasure Bait Again Being Offered to Unwary Americans. *The New York Times*, 20 March 1898, s. 12.
[9] TRAIN, A. The Spanish Prisoner. *The Cosmopolitan Magazine New York*, March 1910, č. 43, s. 465 n.
[10] Výraz odkazuje na číslo ustanovení nigerijského trestního zákoníku upravujícího podvodné jednání.
[11] TIVE, Ch. *419 Scam: Exploits of the Nigerian Con Man*. iUniverse, 2006, s. VII.

„Sir,

Re: 2010 Yamaha Aerox 50 r with 5400 km

Because of my financial problems that i have got i am willing to give it for € 700,- – shipping included .

It is in perfect condition with no damage on it. Technical inspection and emissions testing is passed and stamped as well. It has title of ownership, cleared of any obligations or fees and comes with all the documents you need to register it. You will not have to pay additional taxes for this (VAT reclaimable). (the bike is register in Germany and have german documents) It's my personal bike. I have worked in Germany for one year and I've purchased the motorcycle there. My company wanted me back home, so currently I'm in England (United Kingdom).The motorcycle it's now located in ENGLAND – United Kingdom.

it's a pity to keep such a motorcycle and not to use it.

UK registration tax is too high and have some financial problems to deal with and selling this motorcycle at this low price is the only option that I have right now. I am aware that I'm selling it way too cheap but I have no other solution.

I list my motorcycle under Europe Handler websites so I can sell it faster and for more publicity. The price is correct and the motorcycle can be transported to any location. My motorcycle is already at one Transport company from UK. I paid them to take care for my motorcycle sale protection. I can deliver the motorcycle to any location in Europe on my cost.

Please write me back to discuss only if you are interested!"

Z textu vyplývá, že požadovaná motorka je stále na prodej, nyní dokonce o 150 € levněji, avšak v současné době není k dispozici v Německu, ač tam byla zakoupena, ale v docích v Anglii, kam byl pisatel povolán zaměstnavatelem. Jelikož je registrace ve Spojeném Království příliš vysoká, nevyplatí se majiteli moped na ostrovech provozovat, a tak se ho rozhodl prodat. Moped majitel inzeroval přes německého prodejce, aby zvýšil publicitu inzerátu a prodej urychlil. Motorka je v současné době uschována u jednoho britského dopravce, na náklady majitele je možné ji dopravit na kterékoliv místo v Evropě. Ke zprávě bylo rovněž přiloženo 7 podrobných fotografií prodávané motorky.

Z odpovědi sice nikterak nevyplývá, že by zájemce musel uhradit jakékoliv prostředky navíc, je však možné, že by v další komunikaci byl ze strany majitele vznesen požadavek na (zálohovou) platbu předem, nejlépe prostřednictvím služeb Western Union, která zaručuje prakticky absolutní anonymitu příjemce. Rovněž lze očekávat požadavek na platbu pojištění přepravy apod.

Autor tohoto příspěvku byl s obdobnými praktikami na automobilových serverech obeznámen, avšak i pro něj bylo překvapivé, že podvodníkům stojí za snahu pokoušet své štěstí i na serverech inzerujících mopedy, jejichž cena je na rozdíl od automobilů řádově nižší. Navíc se u motocyklů nemůže uplatnit zástěrka nepoužitelnosti automobilů s levostranným řízením v Anglii. Přesto však již sama zpráva vzbuzuje určité pochybnosti. Jednak je neobvyklé, že majitel posílá svou zprávu v angličtině, ačkoliv zájemce odpovídal na inzerát ve spisovné němčině, navíc když majitel měl dle svých slov rok pracovat v Německu. I kdyby se za tu dobu německy nenaučil, prozrazuje podvodníka

samotný jazyk. Ačkoliv o sobě tvrdí, že je v Anglii doma, z textu je patrné (kromě jiných chyb), že angličtinu příliš neovládá, neboť přestože v názvech států důsledně dodržuje psaní velkých písmen („Germany“, „England“, „United Kingdom“), v případě přídavného jména „německý“, tj. „German“, píše toto slovo s malým počátečním písmenem, což je typické pro kontinentální země.

Uvedená zpráva vyvolala ihned u svého příjemce podezření z podvodného jednání. Přesto je třeba poznamenat, že pro osobu, která se rozhodla např. právě ke koupi motocyklu a už se viděla, jak se stane jeho hrdým majitelem, je tato nabídka opravdu lákavá. Přeci jen, co kdyby to nebyl podvod… I pro autora tohoto příspěvku, který metody sociálního inženýrství a nigerijských listů velmi dobře zná, bylo pokušení opravdu velké. Jak potom musí působit na neinformované osoby?

Autor, nyní však již z čirého zájmu, napsal (v angličtině) majiteli, že zájem o motorku stále má, je sice ochoten ji převzít na majitelem původně udávaném místě v Dortmundu, v žádném případě však nebude hradit jakékoliv poplatky ani zálohy za uvedenou motorku. Ze zprávy však bylo jasně patrné, že její autor je obeznámen s podvodnými praktikami. Odpověď od „majitele“ přišla nečekaně z e-mailové adresy s doménou registrovanou ve východní Evropě. Tato zpráva by však již pro svou vulgaritu nemohla být v tomto příspěvku publikována.

2.3 KONKRÉTNÍ PODOBA PHISHINGU

Phishingové praktiky se tedy inspirovaly v podvodných jednáních typu nigerijských listů ve dvojím směru. Jednak v metodách sociálního inženýrství, jednak v masivním využívání prostředků elektronických komunikací (zejména služby elektronické pošty, diskusních internetových fór, sociálních sítí apod.). Ty dokáží vzhledem k obrovskému počtu potenciálních obětí snižovat pravděpodobnost neúspěchu a zároveň díky své relativní anonymitě snižují i riziko odhalení.

Jedna z nejčastějších podob phishingu spočívá ve snaze pachatele vylákat z oběti údaje a hesla k internetovému bankovnictví, popř. číslo kreditní (platební)[12] karty, její dobu platnosti a tzv. Card Validation Code (CVC), tedy číslo k ověření platnosti karty nacházející se na její zadní straně. Pomocí těchto údajů pak může útočník z bankovního (karetního) účtu oběti odčerpat někdy i všechny finanční prostředky. Samotný útok obvykle probíhá v několika fázích. První z nich (přípravná fáze) zahrnuje opatřování potřebného (obrovského) počtu e-mailových adres potenciálních obětí. Toho lze dosáhnout hned několika způsoby. Jedním z nich je odkoupení (či jiné obstarání) databáze cizích e-mailových adres, která byla získána buď např. od internetových obchodníků přímo (v rozporu se zásadami ochrany osobních údajů), nebo bývá sama terčem např. hackerských útoků na systémy, kde jsou tyto databáze uloženy. V dnešní době se objevují dokonce i webové servery a internetová fóra s omezeným přístupem (tzv. carding

[12] Ve společnosti se obvykle oba výrazy zaměňují, resp. převažuje využívání výrazu „kreditní karty“ i pro karty platební. Z hlediska bankovního je však mezi oběma značný rozdíl, neboť prvně uvedený výraz slouží k čerpání prostředků z již bankou poskytnutého úvěru, jedná se tak v podstatě o úvěrovou kartu, v druhém případě se jedná o kartu sloužící k čerpání peněz (platbě) z běžného či sporožirového účtu.

forums), kde probíhá čilý černý trh s kradenými osobními a finančními údaji.[13] Další způsob spočívá ve využití počítačového generátoru adres. Jedná se vlastně o počítačový program, který za pomoci slovníkových hesel, telefonních seznamů a seznamu registrovaných domén uměle vytváří jednotlivé e-mailové adresy s tím, že lze očekávat, že existující adresy budou obsahovat kombinaci takovýchto slov. Při tomto způsobu sice vzniká obrovské množství neexistujících adres, to však útočníkům nevadí, pokud zároveň získají dostatečný počet adres existujících.

V této souvislosti je třeba si uvědomit, že phishingu značně napomáhá neostražitost uživatelů internetu, kteří neváhají svou soukromou e-mailovou adresu vyplnit při registraci i na stránkách, jejichž solidnost je minimálně pochybná. Koncový uživatel totiž prakticky nemá žádnou kontrolu, co se s jeho údaji vyplněnými při registraci děje a zda není třeba právě jeho e-mailová adresa poskytnuta třetím osobám. Pokud by si uživatelé internetu zřizovali více e-mailových schránek, přičemž jednu by např. používali k oficiální komunikaci a jednu jako tzv. „spamovou" schránku, která by byla využívána při nejrůznějších registracích na webových serverech, jistě by tím do značné míry omezili možnost být adresátem pokusů o phishing.

Součástí přípravné fáze pak rovněž bývá i vytvoření webových stránek pod takovou doménou, která odpovídá očekávání oběti o webové stránce, kam bude údaje (dobrovolně) vyplňovat. Pokud tedy útok míří kupříkladu na klienty určité banky, bude se útočník snažit napodobovat webové stránky internetového bankovnictví tohoto bankovního ústavu, a to pod doménou (adresou), která tomuto účelu bude odpovídat. Oběť pak snadněji uvěří, že jí vyplněné údaje míří do správných rukou. Zároveň pachatel s webovými stránkami vytvoří i e-mailovou adresu, ze které bude uskutečněn samotný útok a která bude rovněž názvem odpovídat obětí očekávanému odesílateli.

Po těchto přípravách následuje vlastní phishingový útok. Ten spočívá v rozeslání e-mailové zprávy na získané adresy schránek, která má za úkol přimět oběť k vyzrazení požadovaných údajů. Právě v této chvíli se uplatní metody sociálního inženýrství. I ta nejdůvěřivější osoba totiž nevyzradí tak důvěrné informace zcela bez důvodu. Zástěrka bývá v tomto ohledu různorodá, nejčastěji se lze setkat s tím, že pachatel vydávající se za bankovní ústav bude jejího klienta informovat o přechodu na nové (lepší) webové rozhraní internetového bankovnictví, pročež je zapotřebí, aby se klient na nich přeregistroval pomocí původních přihlašovacích údajů. Rafinovanější varianta využívá obeznámenosti veřejnosti s existencí phishingu, a proto v tomto případě útočník kontaktuje oběť s tím, že její banka aktivně reaguje na zvyšující se phishingové nebezpečí. Proto banka zavádí bezpečnější systém, kam se má klient přihlásit pomocí stávajících údajů a autentifikovat jejich pravost. Vždy je však v e-mailové zprávě uveden odkaz, který klienta přesměruje přímo na „zabezpečené" stránky. V tuto chvíli nastává rozhodující chvíle, zda se phishingový útok vydaří či nikoliv. Pokud bude oběť zprávě důvěřovat, útočníkovi s největší pravděpodobností v sítích uvízne. Odradit by ji totiž mohlo už jen podezřelé či nekvalitní zpracování webového rozhraní stránek, na které ji odkaz poslal. V případě, že oběť „klikne" na odkaz uvedený v e-mailové zprávě a na stránkách vy-

[13] K tomu blíže v: PERETTI, K. K. Data Breaches: What the Underground World of "Carding" Reveals. *Santa Clara Computer and High Technology Journal*, 2008, č. 2, s. 375 n.

tvořených útočníky údaje do podstrčeného formuláře vyplní, získají pachatelé okamžitě přístupové údaje k internetovému bankovnictví.

Poslední fáze phishingového útoku konečně zahrnuje neoprávněné odčerpání prostředků z bankovního účtu oběti pomocí vylákaných přihlašovacích údajů, popř. zakoupení hodnotného zboží prostřednictvím vyzískaných údajů o kreditní kartě oběti. Jelikož elektronické peněžní přesuny bývají poměrně dobře vysledovatelné, využívají často pachatelé-organizátoři nastrčených osob (bílých koní). V případě bezhotovostního odčerpání peněžních prostředků oběti tito za určitou odměnu zakládají bankovní účty, na které následně phishingem podvodně získané finanční prostředky přicházejí. Ať již pomocí platebních karet v bankomatech či přímo na pobočce jsou neoprávněně nabyté prostředky vybírány a v hotovosti či právě pomocí platebních příkazů Western Union předávány hlavním pachatelům. V případě nákupu zboží na základě vylákaných (či odkoupených) údajů z platebních a kreditních karet spolupracují tito bílí koně nezřídka nevědomky. Pouze přijmou nikterak obtížnou „administrativní" práci v podobě kontroly obsahu a přeposílání zásilek, které jim po uzavření „pracovní smlouvy" začnou být ve velkém počtu doručovány, na předem dané adresy. Tímto způsobem je pak možné zastřít původ zboží z phishingových aktivit.

3. TRESTNĚPRÁVNÍ KVALIFIKACE PHISHINGU PODLE TR. ZÁKONA

3.1 PŘÍPAD NEPOCHOPENÉHO PHISHINGU

Předkládaný případ názorně ukazuje, jak je někdy pro orgány činné v trestním řízení obtížné konkrétní podobu internetové kriminality uchopit. V dané věci napadla obžaloba pro dva skutky spočívající v tom, že:[14]

1) „Obžalovaný R. F. po vzájemné dohodě s již odsouzeným K. Z. a další dosud neustavenou osobou, či dalšími osobami, prostřednictvím e-mailu, zaslaného na e-mailovou adresu poškozené A. L. R., nechal podvrhnout falešný internetový formulář, vložený prostřednictvím http://citionline.czechrepublic-online.com/index2html, na originální stránky Citibank, a. s., předstírající, že je originální internetový formulář https://czechrepublic.2.online.citibank.cz/HomeBankingSecure/Pers/StartSession.asp?), kdy pod záminkou potvrzení údajů, týkající se transakce ke dni 24. 3. 2006, nechal vylákat od A. L. R. citlivé údaje k jejímu účtu vedenému u Citibank, a. s., č. účtu X a poté, co A. L. R., dle příslušných odkazů uvedených na podvrženém internetovém formuláři, se dostala na nezabezpečené falešné stránky, předstírající, že patří bankovnímu ústavu Citibank, a. s., a dispoziční údaje k předmětnému účtu zadala spolu s HPINem, tedy heslem k uvedenému účtu, nechal provést prostřednictvím služby internetového bankovnictví podvodnou transakci vyplněním příslušných údajů do předepsaného formuláře poskytnutého bankou, aby z účtu plátce, tedy účtu č. X byly převedeny finanční prostředky ve výši 999,79 EU na účet č. Y, na základě

[14] Text je ohledně prvého skutku v autentickém znění, pouze anonymizován, u druhého skutku je parafrázován.

takto vyplněného a posléze odeslaného formuláře do Citibank, a. s., skutečně došlo k odúčtování uvedené finanční částky z předmětného účtu majitelky A. L. R., vedeného u pobočky Citibank, a. s., v Praze 6, Evropská 178, bez jejího vědomí došlo, přičemž dne 27. 3. 2006 byla částka 999,79 EU v ekvivalentu 28 664 Kč převedena na účet Y u eBanky v Praze 1, Václavské nám. 43, který si zatím účelem a s příslibem provize v částce 3000 Kč na pokyn obv. R. F. založil dne 20. 3. 2006 K. Z., jenž dne 29. 3. 2006, když se pokoušel z účtu peníze vyzvednout, byl zadržen."

2) R. F. po vzájemné dohodě s S. K. padělali podpis třetí osoby na formulářích příkazů k úhradě, které pak S. K. vhodil do sběrných boxů, případně odevzdal na přepážce banky, přičemž převod prostředků na účet zřízený S. K. a následný výběr hotovosti byl proveden ohledně částky 95 000 Kč pouze jedenkrát, za což obžalovaný S. K. obdržel odměnu ve výši 5000 Kč. V dalších pěti případech k převodu částky ve výši 95 000 Kč, resp. 97 000 Kč (v jednom případě) nedošlo, neboť při provádění kontroly podpisových vzorů k těmto příkazům k úhradě vzniklo podezření, že podpisy na nich jsou zfalšovány. Obžalovaní tak měli způsobit poškozené bance H. B. C. R. škodu ve výši 95 000 Kč a pokusit se o způsobení škody v celkové výši 479 500 Kč.

Skutek pod bodem 1. obžaloby byl státním zástupcem kvalifikován jako „trestný čin padělání a pozměňování peněz podle § 140 odst. 2 zákona č. 140/1961 Sb., trestní zákon (dále jen „tr. zákon"), za užití ustanovení § 143 tr. zákona formou spolupachatelství podle § 9 odst. 2 tr. zákona v jednočinném souběhu s trestným činem podvodu podle § 250 odst. 1, odst. 2 tr. zákona ve stádiu pokusu podle § 8 odst. 1 tr. zákona formou spolupachatelství podle § 9 odst. 2 tr. zákona a v jednočinném souběhu s trestným činem poškození a zneužití záznamu na nosiči informací dle § 257a odst. 1 písm. a) tr. zákona, formou spolupachatelství podle § 9 odst. 2 tr. zákona". Skutek pod bodem 2. obžaloby pak byl kvalifikován jako „trestný čin padělání a pozměňování peněz dle § 140 odst. 2, 3, písm. b) tr. zákona za užití ustanovení § 143 tr. zákona spáchaný formou spolupachatelství podle § 9 odst. 2 tr. zákona v jednočinném souběhu s trestným činem podvodu podle § 250 odst. 1, odst. 3 písm. b) tr. zákona dílem dokonaný dílem ve stádiu pokusu podle § 8 odst. 1 tr. zákona spáchaný formou spolupachatelství podle § 9 odst. 2 tr. zákona".

Po provedeném dokazování Městský soud v Praze jako soud prvního stupně oproti obžalobě považoval jednání popsané pod bodem 1. obžaloby pouze jako další dílčí útok pokračování v podvodném jednání uvedeném pod bodem 2. obžaloby, a proto škodu z jednání pod bodem 1. přičetl do celkové částky škody, o kterou se obžalovaní měli pokusit, jinak však samotný popis jednotlivých útoků ponechal beze změn. Skutek, pro který byli obžalovaní uznáni vinnými, následně kvalifikoval ohledně obžalovaného R. F. jako „trestný čin padělání a pozměňování peněz podle § 140 odst. 2, al. 2 tr. zákona za užití ust. § 143 tr. zákona ve spolupachatelství podle § 9 odst. 2 tr. zákona v jednočinném souběhu s trestným činem podvodu podle § 250 odst. 1, odst. 3 tr. zákona dílem dokonaným, dílem ve stádiu pokusu podle § 8 odst. 1 tr. zákona ve spolupachatelství podle § 9 odst. 2 tr. zákona a v bodě 1. v jednočinném souběhu s trestným činem poškození a zneužití záznamu na nosiči informací dle § 257a odst. 1 písm. a) tr. zákona". Ohledně obžalovaného S. K. byl skutek, kterým byl uznán vinným, kvalifikován jako „trestný čin padělání a pozměňování peněz podle § 140 odst. 2, al. 2 tr. zákona za užití

ustanovení § 143 tr. zákona ve spolupachatelství podle § 9 odst. 2 tr. zákona v jednočinném souběhu s tr. činem podvodu podle § 250 odst. 1, odst. 3 tr. zákona dílem dokonaným, dílem ve stádiu pokusu podle § 8 odst. 1 tr. zákona ve spolupachatelství podle § 9 odst. 2 tr. zákona".

Vrchní soud v Praze jakožto soud odvolací se s kvalifikací jednání pod bodem 1. rozsudku jakožto dílčího útoku pokračování v podvodném jednání, jehož další útoky jsou uvedeny pod bodem 2. rozsudku, ztotožnil, přesto však zrušil výrok o vině i o trestu. Dle autora tohoto příspěvku vrchní soud zcela správně dospěl k závěru, že vzhledem k celkově způsobené škodě ve výši 95 000 Kč nemohl být trestný čin podvodu podle § 250 odst. 1, 3 písm. b) tr. zákona ani dílem dokonaný, neboť uvedená kvalifikace vyžadovala způsobení škody značné, tedy ve smyslu § 89 odst. 11 tr. zákona nejméně 500 000 Kč. Odvolací soud proto znovu uznal oba obžalované vinnými, avšak ohledně trestného činu podvodu podle § 250 odst., 3 písm. b) tr. zákona nikoliv dílem dokonaného a dílem nedokonaného, ale zcela ve stádiu pokusu podle § 8 odst. 1 tr. zákona. Jinak ponechal kvalifikaci soudu prvního stupně beze změn.

Za výše uvedené trestné činy vrchní soud odsoudil obžalovaného R. F. k úhrnnému trestu v trvání pěti let, pro který jej zařadil do věznice s dozorem. Zároveň jej oproti výroku o trestu soudu prvního stupně navíc odsoudil i k trestu vyhoštění na dobu pěti let. Obžalovaný S. K. byl odvolacím soudem odsouzen k trestu odnětí svobody v trvání tří let, jenž mu byl podmíněně odložen na zkušební dobu v trvání pěti let s dohledem. Konečně byla oba obžalovaným stanovena rozsudkem odvolacího soudu povinnost společně a nerozdílně nahradit poškozené bance H. B. C. R. částku 95 000 Kč na náhradě škody.

3.2 PROBLÉMY PRÁVNÍ KVALIFIKACE PŘÍPADU

Z uvedených rozhodnutí soudů obou stupňů vyplývá hned několik sporných otázek, které lze rozdělit do několika okruhů:

1) Lze podvodné jednání spočívající v odčerpání prostředků z účtů různých osob pomocí přístupových údajů k internetovému bankovnictví vylákaných od oběti cestou phishingu na jedné straně a na základě zfalšovaných papírových formulářů jednorázového příkazu k úhradě vhozeného do sběrného boxu v bance na straně druhé považovat celkově za pokračování v trestném činu ve smyslu § 89 odst. 3 tr. zákona, resp. § 116 tr. zákoníku?
2) Pokud na základě zfalšovaných příkazů k úhradě (ať už elektronických či listinných) dojde k transakci peněžních prostředků (v podobě tzv. žirálních peněz)[15] na jiný účet, v kterém okamžiku bude dokonán trestný čin podvodu?
3) Lze kvalifikovat elektronické zadání příkazu k úhradě na základě autentifikačních údajů vylákaných phishingem provedené před 1. 1. 2010 jako trestný čin padělání a pozměňování peněz podle § 140 odst. 2 alinea 2 tr. zákona?
4) Je možné samotné phishingové jednání v tomto případě kvalifikovat jako trestný čin poškození a zneužití záznamu na nosiči informací dle § 257a odst. 1 písm. a) tr. zákona?

Řešením těchto otázek se bude v následujícím textu zabývat tento příspěvek.

[15] Tj. bezhotovostních peněz vedených na účtech.

3.2.1 PHISHING JAKO DÍLČÍ ÚTOK POKRAČOVÁNÍ V TRESTNÉM ČINU PODVODU

Jak již bylo zmíněno výše, soudy obou stupňů na rozdíl od obžaloby státního zástupce považovaly jednání uvedené pod bodem 1. obžaloby, tedy elektronické odčerpání prostředků z účtu oběti phishingu, pouze jako dílčí útok pokračování v trestném činu podvodu (resp. jeho pokusu). Přitom ostatní útoky tohoto pokračujícího trestného činy nebyly realizovány elektronicky, nýbrž písemnými formuláři příkazu k úhradě s falšovanými podpisy oprávněné osoby. Autor tohoto příspěvku se s tímto závěrem ztotožňuje. Ustanovení § 89 odst. 11 tr. zákona stejně jako ustanovení § 116 zákona č. 40/2009 Sb., trestní zákoník (dále jen „tr. zákoník"), považuje za pokračování v trestném činu jednání, jehož jednotlivé dílčí útoky vedené jednotným záměrem naplňují (v tr. zákoníku je již výslovně uvedeno „byť i v souhrnu") skutkovou podstatu stejného trestného činu, jsou spojeny stejným nebo podobným způsobem provedení a blízkou souvislostí časovou a v předmětu útoku.

Je zřejmé, že jednání pod bodem 1. i 2. rozsudku byla vedena jednotným záměrem, a to podvodně pomocí falšovaných příkazů k úhradě vylákat finanční prostředky z účtů různých klientů bank. Zároveň všechna tato jednání naplnila, mimo jiné, skutkovou podstatu stejného trestného činu, a to podvodu podle § 250 tr. zákona, resp. jeho pokusu. V daném případě byla splněna i podmínka blízké souvislosti časové, byť útok spáchaný prostřednictvím elektronického bankovnictví a útoky v podobě padělaných listinných příkazů k úhradě od sebe dělila doba skoro 4 měsíců. Jednak tato doba není natolik dlouhá, aby zakládala automatické přetržení časové souvislosti, a jednak dle stávající judikatury Nejvyššího soudu ČR nelze blízkou časovou souvislost mezi dílčími útoky přesně ohraničit maximální lhůtou, ale je ji třeba posoudit s ohledem na konkrétní skutkové okolnosti každého případu.[16] V posuzovaném případě nasvědčuje pokračování zejména velice obdobný postup pachatele R. F., který si vždy před samotným pokusem o odčerpání finančních prostředků zajistil osobu, která pro něj založila „čistý" bankovní účet, na který vylákané prostředky později zašle. Tyto osoby pak měly poté, co peníze na účet dorazí, tyto vybrat a předat pachateli R. F. Oba druhy jednání se tak od sebe lišily jen v tom, že v prvním případě podvod probíhal cestou elektronických příkazů k úhradě, který byl falešně autentifikován přístupovými údaji pocházející od oběti phishingu, v druhém případě pak formulářů k jednorázovému příkazu k úhradě, na kterém byl zfalšován podpis oprávněného disponenta. Lze proto shrnout, že všechny útoky podvodného jednání byly spojeny obdobným způsobem provedení. Konečně byl splněn i znak souvislosti v předmětu útoku, když všechny dílčí útoky mířily proti bezhotovostním penězům uloženým na účtech různých bankovních ústavů.

3.2.2 DOKONÁNÍ TRESTNÉHO ČINU PODVODU V PŘÍPADĚ, KDY TRANSAKCE NA ZÁKLADĚ PADĚLANÝCH PŘÍKAZŮ BYLA PROVEDENA.

Z předložených rozsudků, stejně jako obžaloby vyplývá, že orgány činné v trestním řízení považovaly za dokonaný (alespoň v základní skutkové podstatě) pouze

[16] Viz např. usnesení Nejvyššího soudu ČR ze dne 2. 6. 2010, sp. zn. 7 Tdo 440/2010.

jediný dílčí útok pokračujícího trestného činu podvodu, a to ten, při kterém pachatelé dokázali neoprávněně převedené prostředky na základě zfalšovaného podpisu na formuláři příkazu k úhradě z účtu vybrat. Dle názoru autora tohoto příspěvku však takový závěr není správný. Trestný čin podvodu podle § 250 odst. 1 tr. zákona je dokonán v tom případě, když pachatel ke škodě cizího majetku sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou. V případě podvodných odčerpání finančních prostředků z bankovních účtů proto k dokonání trestného činu musí dojít v okamžiku, kdy banka uvedená v omyl ohledně osoby příkazce (jeho identity) platební transakci provede. V ten okamžik totiž oprávněný klient banky ztrácí nad těmito žirálními penězi kontrolu (dispozici), kterou naopak získává příjemce z provedené platební transakce. To platí zejména v těch případech, kdy peněžní prostředky jsou připsány na účet bankovního ústavu odlišného od banky domnělého plátce, kde kontrolu nad těmito prostředky banka plátce dokonce zcela ztrácí.

Peníze na účtech představují pohledávku za bankou. Z pohledu trestního práva se na ně vztahují i ustanovení o věcech (§ 89 odst. 13 věta druhá tr. zákona), jejichž hodnota se rovná jejich nominální výši. Pokud jsou tedy v rámci podvodné činnosti převedeny peněžní prostředky na jiný účet (oprávněnou osobu s ním disponující), vzniká tím původnímu majiteli této majetkové hodnoty škoda a naopak příjemci neoprávněný prospěch. Jejich zpětná výměna v nominální hodnotě je tak z hlediska okamžiku dokonání podvodu irelelevantní, neboť již předtím došlo k převodu majetkové hodnoty (věci) ve stejné nominální výši.

Pokud tedy v případě prvého útoku, který využíval přístupových údajů k elektronickému bankovnictví získaných phishingem, došlo na základě elektronického příkazu k úhradě k bezhotovostnímu převodu finančních prostředků a tyto byly připsány na účet zřízený pachateli u jiné banky, byl okamžikem připsání těchto prostředků trestný čin podvodu dokonán, a to vzhledem k výše vzniklé škody a neoprávněného prospěchu 28 664 Kč dle ustanovení § 250 odst. 2 tr. zákona. To samozřejmě nic nemění na tom, že vzhledem k dalším dílčím útokům bylo třeba jednání pachatelů v souhrnu kvalifikovat jako pokus pokračujícího trestného činu podvodu podle § 8 odst. 1, § 250 odst. 3 písm. b) tr. zákona, neboť aby tento trestný čin mohl být alespoň dílem dokonaný, musel by součet dílčími útoky způsobené škody dosahovat částky 500 000 Kč, což se v daném případě nestalo.

U zbylých útoků, které byly uskutečněny pomocí formulářů k jednorázovému příkazu k úhradě s padělaným podpisem, nedošlo k provedení bezhotovostního platebního převodu na účet ve formuláři uvedeného příjemce. Z toho důvodu nemohla být u těchto útoků naplněna skutková podstata trestného činu podvodu ani v prvním odstavci, a jednalo se tak pouze o ukončený pokus.

Lze tak uzavřít, že správně měla být skutková věta rozsudku Vrchního soudu v Praze doplněna tak, že obžalovaný R. F. způsobil jednáním pod bodem 1. poškozené Citibank, a. s., škodu ve výši 28 664 Kč, a zároveň o tuto částku měla být ponížena výše celkové škody, ke které dle odsuzujícího rozsudku mělo směřovat jednání obžalovaného R. F.

3.2.3 TRESTNĚPRÁVNÍ KVALIFIKACE ELEKTRONICKÉHO ZADÁNÍ PŘÍKAZU K ÚHRADĚ NA ZÁKLADĚ AUTENTIFIKAČNÍCH ÚDAJŮ VYLÁKANÝCH PHISHINGEM

Dalším problematickým okruhem týkajícím se phishingu je trestněprávní kvalifikace samotného aktu, kdy pachatel neoprávněně získané autentifikační údaje použije k zadání jednorázového příkazu k úhradě pomocí služby elektronického bankovnictví. Je nesporné, že toto jednání je třeba (pokud na základě něho dojde k transakci prostředků) posoudit jako trestný čin podvodu, popř. jeho pokusu, v době vydání předkládaných rozhodnutí podle § 250 tr. zákona. Tím však není výčet v úvahu připadajících trestných činů vyčerpán. Orgány činné v trestním řízení v předkládané věci toto jednání posoudili jako jednočinný souběh trestného činu podvodu (ve stádiu pokusu) podle § 8 odst. 1, § 250 odst. 1, 3 písm. b) tr. zákona a trestného činu padělání a pozměňování peněz podle § 140 odst. 2 alinea 2 tr. zákona. Všechny ve věci rozhodující orgány přitom vycházely ze společných ustanovení § 143 tr. zákona, které přiznávají ochranu proti padělání též tuzemským a cizozemským platebním prostředkům.

Konkrétní úpravu příkazu k úhradě obsahovala do 28. 6. 2011 prováděcí vyhláška ČNB č. 62/2004 Sb., kterou se stanoví způsob provádění platebního styku mezi bankami, zúčtování na účtech u bank a technické postupy bank při opravném zúčtování (dále jen „vyhláška“). Podle § 2 této vyhlášky provádějí banky tuzemský platební styk formou úhrady nebo inkasní formou placení, přičemž úhradou se rozumí operace prováděná na základě příkazu, který dal příkazce své bance za účelem převedení peněžních prostředků ve prospěch příjemce.[17] Podle odst. 4 uvedeného ustanovení vyhlášky může být úhrada uskutečňována odepsáním peněžních prostředků z účtu plátce a jejich připsáním na účet příjemce (dále jen „bezhotovostní platební styk“). Podle § 3 odst. 1 vyhlášky pak banky používají v tuzemském bezhotovostním platebním styku ve vztahu s klienty příkazy k úhradě a příkazy k inkasu, které mohou být bance předávány na tiskopisech, formou elektronických dat nebo jiným sjednaným způsobem.

Z uvedených ustanovení tedy vyplývá, že zákon o platebním styku z roku 2002 i vyhláška ČNB z roku 2004 přiznávaly příkazům k úhradě postavení platebního prostředku, a to jak v jejich tiskopisných formách, tak i v elektronických, předávaných např. službou elektronického bankovnictví. Vzhledem k tomu, že přístupové údaje k elektronickému bankovnictví slouží v podstatě k autentifikaci osoby oprávněné disponovat prostředky na účtu stejně, jako je tomu v případě podpisu na tiskopisu příkazu k úhradě, bylo lze subsumovat jednání, kdy pachatel autentifikačními údaji jiné osoby potvrdil oprávněnost elektronického příkazu k úhradě z účtu oběti, pod skutkovou podstatu trestného činu padělání a pozměnění peněz podle § 140 odst. 2 alinea 2 tr. zákona ve spojení s § 143 tr. zákona. V tomto směru se proto lze se závěry obou soudů v předkládané věci zcela ztotožnit.

---

[17] Paragraf 3 odst. 1 zákona č. 124/2002 Sb., o platebním styku, v časově relevantním znění.

3.2.4 TRESTNĚPRÁVNÍ KVALIFIKACE SAMOTNÉHO PHISHINGOVÉHO JEDNÁNÍ PODLE § 257a ODST. 1 PÍSM. a) TR. ZÁKONA

Soudy obou stupňů rovněž shodně s obžalobou kvalifikovaly výše popsané jednání pod bodem 1. jako trestný čin poškození a zneužití záznamu na nosiči informací dle § 257a odst. 1 písm. a) tr. zákona. Tato kvalifikace je však dle autora tohoto příspěvku nesprávná a vychází z určitého nepochopení modu operandi phishingu. O tom svědčí již skutková věta pod bodem 1. odsuzujícího rozsudku Vrchního soudu v Praze, kde je odsouzený R. F. uznán vinným tím, že jako spolupachatel „prostřednictvím e-mailu, zaslaného na e-mailovou adresu poškozené A. L. R., nechal podvrhnout falešný internetový formulář, vložený na originální stránky Citibank, a. s., […]". Je totiž v praxi velice obtížné, aby pachatelé cokoliv „podvrhovali", natož falešný internetový formulář k vyplnění přístupových údajů k elektronickému bankovnictví, na *originální* stránky jakéhokoliv bankovního ústavu. Ty bývají velmi důkladně zabezpečené, uložené na obtížně přístupných serverech chráněných víceprvkovou ochranou, a proto by jejich narušení v takové míře bylo obtížné i pro velmi schopného hackera. Pachatelé phishingu tak na originální stránky banky nic nevkládají. Místo toho (jak bylo rozvedeno výše) vytvoří webové stránky vypadající shodně s rozhraním využívaným poškozenou bankou a následně zašlou oběti e-mailovou zprávu, která ji má přesvědčit, aby přístupové údaje na těchto stránkách, kam ji nasměruje odkaz v e-mailové zprávě, zadala. Oběť tedy pachatelům své přístupové údaje vlastně „dobrovolně" předá v domnění, že je poskytuje svému bankovnímu ústavu.

Pachatelé phishingu proto nezískávají přístup k nosiči informací a takových informací neoprávněně neužívají v úmyslu získat sobě neoprávněný prospěch ve smyslu ustanovení § 257a tr. zákona. I když neoprávněně užívají určité informace (identifikační údaje k elektronickému bankovnictví), nemusí k nosiči s těmito informacemi ať už u banky či přímo u oběti získávat přístup, nýbrž je sami přímo obdrží od oběti na vlastní webový server. Naplnění skutkové podstaty uvedeného trestného činu tak připadá v úvahu pouze u poměrně malého množství phishingových případů. Bude tomu tak zejména v situacích, kdy budou k získání informací použity hackingové metody, např. pokud e-mailová zpráva určená oběti bude obsahovat určitý škodlivý kód, typicky tzv. keylogger, pomocí něhož bude možné „odposlechnout" potřebné údaje. V případech, kdy ale pachatelé zvolili klasickou metodu phishingu, nebylo toto jednání možné pod skutkovou podstatu trestného činu poškození a zneužití záznamu na nosiči informací podřadit.

Stejně tak nelze dospět k závěru o naplnění trestného činu podle § 257a tr. zákona tím, že pachatel phishingem vyláká přístupové údaje k internetovému bankovnictví (tedy k nosiči informací obsluhujícího tuto službu banky) a informace (např. o stavu účtu) tam svým příkazem změní. Pachatelé phishingu sami takovéto informace nemění, nýbrž je to banka, resp. její systém internetového bankovnictví, která v důsledku transakce uskutečněné pachatelem phishingu provede změnu informací o zůstatku na bankovním účtu.

Lze proto uzavřít, že samotný phishing bylo podle právní úpravy do 31. 12. 2009 možné postihnout jen jako přípravné jednání k trestnému činu podvodu a padělání a pozměňování peněz, ne již však jako dokonaný trestný čin, pokud nedošlo k realizaci

peněžní transakce. Přitom je zřejmé, že nebezpečnost phishingu pro společnost je velmi vysoká a může vést k astronomickým škodám. V tomto směru lze tedy považovat předchozí právní úpravu postihu phishingu za nedostatečnou.

Na předloženém případu phishingu je poměrně pozoruhodné i to, že obžalovaný R. F. byl odsouzen za podvodné vylákání přístupových údajů oběti, aniž by byl proveden jakýkoliv důkaz, jak obžalovaný k těmto údajům přišel. Z dokazování totiž vyplynulo pouze to, že obžalovaný požádal svého známého, aby založil bankovní účet s tím, že jakmile na něj dorazí určité finanční prostředky, má tyto vybrat a odevzdat je obžalovanému R. F. Na nově otevřený účet následně peníze skutečně došly, a to na základě elektronického příkazu k úhradě, který zadala nezjištěná osoba, a to pomocí přihlašovacích údajů, které byly získány opět neznámou osobou či osobami z phishingu. V průběhu hlavního líčení však nikterak nebylo prokázáno, že se obžalovaný R. F. na samotném vylákávání údajů reálně podílel. Ten se přitom mohl k přihlašovacím údajům dostat tak, že by je prostě od někoho odkoupil, či mohl být jen osobou, která se dohodla se samotným původcem phishingu, že mu takto pomůže peníze z účtu oběti odčerpat. I v tomto směru tak lze považovat předkládané rozsudky za chybné.

4. TRESTNĚPRÁVNÍ KVALIFIKACE PHISHINGOVÉHO JEDNÁNÍ PODLE NOVÉHO TRESTNÍHO ZÁKONÍKU

Nový trestní zákoník vstoupil v platnost zákonem č. 40/2009 Sb., trestní zákoník, s účinností od 1. 1. 2010. Tento zákoník měl odstranit některé nedostatky původní úpravy a harmonizovat vnitrostátní trestní právo s mezinárodními úmluvami a závazky plynoucími z komunitárního práva. V oblasti počítačové kriminality byla hlavním zdrojem této harmonizace Úmluva o počítačové (správněji však kyber) kriminalitě (Úmluva Rady Evropy č. 185, Budapešť, 2001), kterou Česká republika podepsala dne 9. 2. 2005,[18] avšak doposud ji neratifikovala. Ačkoliv Česká republika není touto úmluvou vázána, zákonodárce již v důvodové zprávě k novému trestnímu zákoníku vyjadřuje vůli zavést trestněprávní úpravu kyberkriminality, která by s předmětnou úmluvou byla v souladu, a splnit tak případné budoucí závazky napřed.[19]

4.1 POSTIH PODLE § 230–232 TR. ZÁKONÍKU

Do nové trestněprávní úpravy majetkových trestných činů v ustanoveních § 230–232 byly začleněny tři trestné činy postihující kybernetickou kriminalitu. Prvním z nich je trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací, který v podstatě rozšiřuje původní trestný čin poškození a zneužití záznamu na nosiči informací dle § 257a odst. 1 písm. a) tr. zákona. Dle názoru autora tohoto příspěvku však phishingové jednání v jeho čisté formě, tzn. nezahrnující hackingové aktivity,

[18] Rada Evropy, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=13/04/2011&CL=ENG [cit. 2012-04-10].

[19] Důvodová zpráva k § 228–230 (dnes § 230–232) vládního návrhu trestního zákoníku, Poslanecká sněmovna Parlamentu České republiky, 5. volební období, 2006–2010, sněmovní tisk č. 410/0.

nemůže být podle tohoto trestného činu postiženo, a to v podstatě ze shodných důvodů, jako v úpravě předchozí.

Skutková podstata trestného činu podle § 230 odst. 1 tr. zákoníku vyžaduje překonání bezpečnostního opatření, a tím neoprávněného získání přístupu k počítačovému systému nebo k jeho části. To se však v případě phishingu neděje, neboť pachatel získá přístupové údaje k elektronickému bankovnictví přímo od oběti, a nemusí tak překonávat žádné bezpečnostní opatření.

Druhá základní skutková podstata obsažená v odst. 2 citovaného ustanovení pak postihuje (podobně jako úprava předchozí) „získání přístupu k počítačovému systému a nosiči informací" a další aktivity s tam uloženými daty či naopak učinění zásahu do programového nebo technického vybavení počítače. Jak již však bylo zmíněno výše, pachatel potřebné informace (data) sám obdrží od oběti a nemusí získávat přístup ve smyslu uvedeného ustanovení.

Phishing však nebude možné trestat ani podle nově zavedeného trestného činu opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat podle § 231 tr. zákoníku. Ten sice postihuje již samotné opatření, přechovávání a další způsoby zpřístupnění přístupových dat, kódů, hesel apod., ovšem pouze v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv nebo právě trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací, což opět není případ klasického phishingu.

Třetí nově zavedený „počítačový" trestný čin podle § 232 tr. zákoníku dopadá na případy nedbalostního poškození nebo zásahu do počítačového systému či vybavení počítače, a proto ani ten nebude na phishing dopadat.

4.2 POSTIH PODLE § 234 TR. ZÁKONÍKU

Trestní zákoník rovněž nově rozlišuje ochranu proti padělání a pozměnění peněz na jedné straně a platebního prostředku na straně druhé. Zároveň byl s účinností k 1. 11. 2009 přijat nový zákon č. 284/2009 Sb., o platebním styku, který přináší definici platebního prostředku. Ten je v § 2 odst. 1 písm. d) vymezen jako „zařízení nebo soubor postupů dohodnutých mezi poskytovatelem a uživatelem, které jsou vztaženy k osobě uživatele a kterými uživatel dává platební příkaz".

Jelikož skutková podstata trestného činu neoprávněného opatření, padělání a pozměnění platebního prostředku podle § 234 odst. 1 tr. zákoníku považuje mimo jiné za trestné i opatření a přechovávání platebního prostředku jiného, vyvstává tu otázka, zdali přístupové údaje k elektronickému bankovnictví naplňují výše uvedenou definici platebního prostředku. V takovém případě by bylo lze stíhat samotné podvodné vylákání těchto údajů jako tento dokonaný trestný čin. Ke kladnému závěru dospívá např. Volovecký.[20]

Autor tohoto příspěvku zastává názor, že nikoliv, a to proto, že shora uvedená definice označuje za platební prostředek až (celý) soubor postupů, které jsou vztaženy k osobě uživatele a kterými uživatel dává platební příkaz, nikoliv samotné přístupové údaje. Ty

[20] VOLOVECKÝ, P. Kybernetické hrozby a jejich trestně právní kvalifikace. *Trestní právo*, 2011, roč. 15, č. 1, s. 15.

ostatně od platebního příkazu zřetelně rozlišuje, když v ustanovení § 2 odst. 3 písm. h) zákona č. 284/2009 Sb., o platebním styku, dále definuje jedinečný identifikátor jako kombinaci písmen, číslic nebo symbolů, kterými se podle určení poskytovatele identifikuje uživatel nebo jeho účet při provádění platebních transakcí, což není nic jiného než údaje, které pachatelé phishingem vylákávají.

Pachatelé phishingu proto dokonají trestný čin neoprávněného opatření, padělání a pozměnění platebního prostředku pouze v tom případě, že elektronický příkaz na základě podvodně získaných identifikačních údajů oběti zadají, čímž použijí padělaný platební prostředek jako pravý nebo platný podle § 234 odst. 3 alinea druhá tr. zákoníku, a to v jednočinném souběhu s trestným činem podvodu podle § 209 tr. zákoníku, popř. jeho pokusu. Dokud tak neučiní, bude jejich phishingové jednání možné posoudit pouze jako přípravu k těmto trestným činům.

5. ZÁVĚR

Tento příspěvek se snaží poukázat na teoretické i praktické problémy při posuzování trestnosti phishingu. Ty vycházejí zejména z určité rezignace orgánů činných v trestním řízení na pochopení jeho průběhu, a to zejména z důvodu nutnosti zabývat se jeho jednotlivými technickými aspekty, které se pro mnohé mohou zdát odtažité a nepochopitelné. To ukazuje zejména předkládaný případ phishingu, který byl českými soudy posuzován. Aby totiž mohl být phishing správně trestně právně posouzen, musí být nejprve pochopen způsob a pozadí jeho provedení.

V první části tohoto příspěvku jsou v krátkosti představeni předchůdci phishingového jednání, jejichž metody jsou phishingem doposud využívány. Na předloženém případě jsou následně diskutovány jednotlivé problémové okruhy jeho trestněprávní kvalifikace, a to vzhledem k době jeho spáchání podle trestního zákona z roku 1961, v relevantním znění. Tato původní úprava je v této práci shledána jako nedostačující k postihu phishingu.

Určité změny do problematiky kyberkriminality, a to i phishingu, přinesl nový trestní zákoník. Poslední část tohoto příspěvku se proto zabývá otázkou, zdali lze phishing posoudit podle nově zavedených skutkových podstat trestných činů směřujících proti kyberkriminalitě. Z provedené analýzy ovšem vyplývá, že i současná úprava považuje za dokonaný trestný čin až moment, kdy pachatel phishingu provede elektronickou úhradu, resp. zadá elektronický příkaz k úhradě. Samotné opatření si přístupových údajů pomocí phishingu tak nadále lze stíhat pouze jako přípravu trestného činu podvodu a neoprávněného opatření, padělání a pozměnění platebního prostředku, a to při splnění podmínek trestnosti přípravy.

PHISHING AND PROBLEMS WITH ITS LEGAL CLASSIFICATION IN THEORY AND PRACTICE

Summary

This paper deals with the criminological and criminal law aspects of phishing, both in theory and practice of decision-making law enforcement agencies and judicial bodies. The contribution addresses the nature of this criminal phenomenon, its forerunners, and the usual modus operandi of the phishing. The second part of this paper consists of a study of concrete judicial case of phishing analyzing the problems with its legal classification, not only from the perspective of the former Czech criminal code, but also in the terms of the new Czech criminal code.

Key words: phishing, Penal code, criminal law

Klíčová slova: pishing, trestní zákoník, trestní právo