Hrozby a trendy Internetbankingu

Pohled banky na bezpečnost přímého bankovnictví

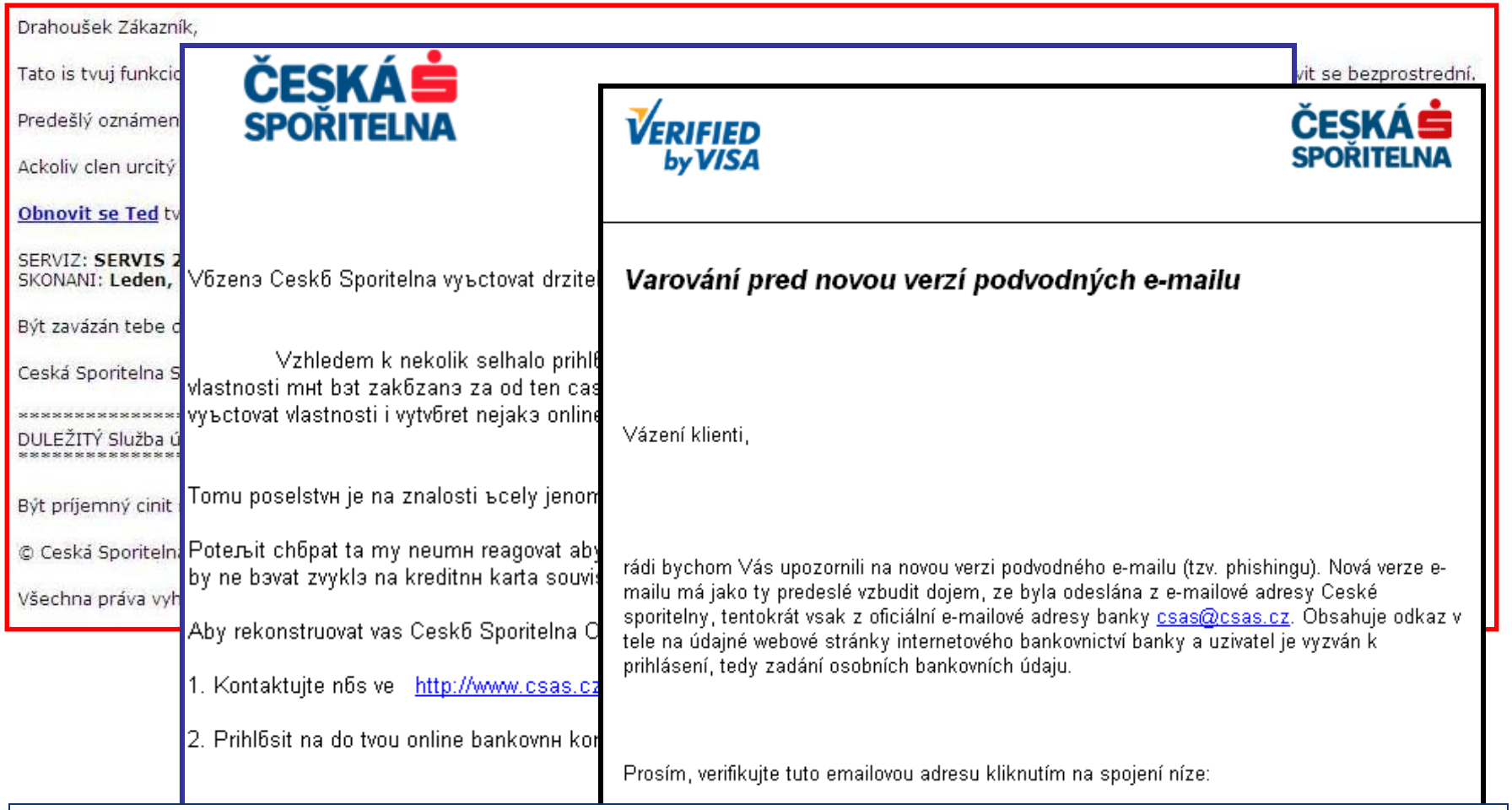
David Pikálek
Česká spořitelna, a.s.
Přímé bankovnictví

ČESKÁ SPOŘITELNA
Jsme Vám blíž.

Agenda

1. **Zkušenost roku 2008 v ČR**
    1. Phishing
    2. Pharming
2. **Aktuální trendy v bezpečnosti ADK**
    1. ČR
    2. Evropa a USA
3. **Plány ČS v oblasti bezpečnosti**

Ukázka phishingu na ČS



Útočníci se u phishingu hodně rychle učí

Dopad phishingu na ČS

Následky phishingové vlny z jara 2008:

1) **nedošlo k žádnému zneužití peněz přes internetové bankovnictví**
2) **několik stovek klientů vyzradilo údaje o svých platebních kartách**
   a) někteří včetně PINu
   b) u poloviny karet došlo k pokusu o zneužití
   c) k reálným transakcím došlo u 10% karet
   d) průměrná škoda na kartu byla 13 000 Kč
   e) díky úspěšným reklamacím byly téměř všechny peníze klientům vráceny
3) **zahlcené klientské centrum – ve špičce až 3000 telefonátů a 8500 e-mailů denně**
4) **osvěta klientů – intenzivní komunikace bank, ČNB i policie vedla k výraznému zlepšení povědomí klientů o možných hrozbách a připomněla, jak se bezpečně chovat na internetu**

Phishing se nejvíce zaměřuje na platební karty

Pharming

V roce 2008 se na českém trhu objevily dva hlavní typy pharmingu:

1) získání přihlašovacích a autorizačních údajů do internet bankingu

a) klientův počítač je infikován trojským koněm nebo jiným škodlivým SW
b) trojský kůň čeká, až klient použije své internetové bankovnictví
c) přesměrování na falešné stránky s cílem získat dodatečné bezpečnostní prvky (např. Bezpečnostní kód)
d) pokus o zneužití peněz na účtu klienta

2) získání údajů o platební kartě

a) klientův počítač je infikován trojským koněm nebo jiným škodlivým SW
b) trojský kůň čeká, až klient použije svou platební kartu
c) přesměrování na falešné stránky s cílem získat dodatečné bezpečnostní prvky (CVV/CVC a/nebo PIN)
d) pokus o zneužití peněz na účtu klienta

Pharming se vloni týkal asi 50 klientů ČS, ani jeden nebyl úspěšný

Jak bojovat proti phishingu a pharmingu

Hlavní nástroje:

1) **Prevence - proaktivní komunikace**
   - přímá komunikace na klienty
   - osvěta v médiích
2) **Koordinace**
   - ČNB a Bankovní asociace
   - Policie ČR
   - technologické firmy (výrobci antivirů, antispamové databáze…)
3) **Nové metody zabezpečení**
   - dvoufaktorové metody
   - fraud management systémy

Znáte základní finty počítačové kriminality? Neskočte jim na ně!

Problematika bezpečného využívání Internetu pro potřeby plateb a dalších operací se stává stále aktuálnější nejen v České republice. Otevřené prostředí internetu láká ke zneužití. Počítačová kriminalita je závažný trestný čin. Jaké jsou základní typy podvodů a jak se jim bránit?

Co je phishing?
Phishing je podvodný e-mail, který má za cíl vylákat od příjemce citlivé údaje, jako jsou čísla karet včetně kódu ze zadní strany karty (kód nad magnetickým proužkem, tzv. CVV/CVC ochranný kód, který se používá jen při placení po internetu), dále například přístupové údaje pro internetové bankovnictví (klientské číslo, heslo i další bezpečnostní údaje), a následně je zneužít.

Jak poznám podvodný e-mail?
Pokud Vám najednou chodí jménem banky e-maily, které obsahují internetovou adresu nebo odkaz na stránky vyžadující vaše přihlašovací údaje či údaje ke kartě, je to phishingová zpráva. Banka takové zprávy nikdy nerozesílá a nemá důvod tyto informace od Vás požadovat.

- Do služby Internetbankingu se nikdy nepřihlašujte z internetových adres uvedených v e-mailu!
- Při vstupu na stránky internetového bankovnictví vždy vypište internetovou adresu služby do pole URL adresy prohlížeče na nově otevřené internetové stránce.
- Adresa stránky vždy začíná „https://“, písmeno „s“ před dvojtečkou znamená, že jde o zabezpečenou komunikaci internetového prohlížeče se serverem.
- Při přihlášení nejsou požadovány žádné další údaje, které nebyly dříve požadovány. Také se nekoná žádné duplicitní potvrzování osobních údajů.

Další techniky kyberzločinců
Pharming – technika podvodu, při které se útočníci snaží pomocí upraveného překladu internetových adres přesměrovat uživatele internetového bankovnictví na připravené podvodné stránky. Uživatel se tak dostane na předem připravenou kopii stránek, jejímž účelem je opětovně zjistit citlivé osobní údaje a následně je zneužít.

Trojský kůň – typickým příkladem je keyloger, který se snaží vysledovat přihlašovací údaje zadávané uživatelem. Zjištěné informace pak předává svým tvůrcům.
Malware – všeobecné označení pro škodlivé programy. Napadené počítače mohou sloužit ke sběru adres, šíření spamu, včetně phishingových e-mailů a šíření dalšího malware.

Všechny podvodné techniky se snaží obejít bezpečnostní technologie a bez vědomí uživatele se samovolně instalovat do počítače. Například při brouzdání po internetu, spouštění pochybných příloh v e-mailu nebo instalaci neověřených programů. Pokud se Vaše internetové bankovnictví chová nestandardně nebo máte nějaké podezření, nezadávejte žádné důvěrné informace a ukončete aplikaci. Následně kontaktujte klientské centrum vaší banky.

Jak se jim bránit?
Důležité je dodržovat bezpečnostní pravidla:
- Aktualizovat operační systém v počítači. Většina systémů umí při správném nastavení tyto aktualizace pravidelně kontrolovat, stahovat a instalovat.
- Používat kvalitní antivirový program a hlavně ho pravidelně aktualizovat.
- Vhodné je mít nainstalovaný program pro ochranu před spyware.
- Své přihlašovací údaje i údaje z platební karty pečlivě chránit.
- Pro obsluhu účtu přes internet nepoužívat veřejně přístupné počítače, umístěné například v různých internetových kavárnách.
- Pokud již k prozrazení citlivých osobních údajů dojde, kontaktujte neprodleně vaši banku.
- Chcete-li mít jistotu, investujte do certifikátu na čipové kartě. Zdá se Vám částka kolem 1 500 Kč vysoká? Ale bezpečnostní zámek do Vašeho bytu nebo zabezpečení auta také něco stojí.

Česká spořitelna ve spolupráci s www.hoax.cz.

ČESKÁ SPOŘITELNA

ČESKÁ SPOŘITELNA

Letáky – na pobočkách a ke stažení na webu

ČESKÁ SPOŘITELNA

Chodí Vám podivné e-maily? Možná je to phishing!

Co je phishing?
Phishing jsou podvodné e-mailové zprávy, které mají vzbudit dojem, že byly odeslány z e-mailové adresy České spořitelny. Zpráva je obvykle psána anglicky nebo špatnou češtinou, obsahuje link na údajné stránky České spořitelny a vyzývá k potvrzení osobních bankovních údajů. Phishingová zpráva může vypadat jako informace o neprovedení platby, výzva k aktualizaci bezpečnostních údajů, či dokonce jako výzkum klientské spokojenosti. Cílem podvodného e-mailu může být získání a následné zneužití klientského čísla a hesla adresáta (identifikační a autentizační údaje), bezpečnostního kódu nebo například čísla platební karty, PIN kódu či dalších bezpečnostních údajů.

Jak se dostala moje e-mailová adresa k někomu, kdo phishing rozesílá? Nejde o únik dat?
V žádném případě nejde o únik dat. Jde o typický případ spamu. Útočníci obvykle e-mailové adresy příjemců náhodně generují nebo je kupují na černém trhu. Česká spořitelna úspěšně chrání e-mailové adresy svých klientů, stejně jako ostatní citlivé údaje, a nikdy je neposkytuje třetím stranám.

Co dělá Česká spořitelna proti phishingu?
Česká spořitelna monitoruje všechny pokusy o phishing. Česká spořitelna podala trestní oznámení a úzce spolupracuje s policií v úsilí najít pachatele a zabránit mu v pokračování podobných útoků. Spolu s technickými specialisty podniká i kroky, jak blokovat aktivity útočníků v zahraničí. Důležitá je rovněž prevence, kdy Česká spořitelna opakovaně informuje klienty, jak phishing poznají a co dělat v případě, že na něj reagovali.

Co má dělat klient v případě, že obdržel phishingový e-mail?
Phishing obvykle vypadá jako zpráva odeslaná z České spořitelny – může se vydávat za informaci o neprovedení platby, výzvu k aktualizaci bezpečnostních údajů, či dokonce za výzkum klientské spokojenosti. Má v sobě také odkazy na podvržené stránky vyžadující zadání klientských bezpečnostních údajů (klientské číslo a heslo, bezpečnostní kód, PIN). Česká spořitelna žádnou takovou zprávu nerozesílá – s klienty nikdy prostřednictvím e-mailu nekomunikuje o tak zásadních záležitostech, jako je např. zabezpečení, a nevyzývá e-mailem k zadání těchto údajů.

Nemám tedy na zprávu reagovat?
Na zprávu v žádném případě nereagujte, smažte ji a na link neklikejte. V případě, že se tak stalo, hrozí, že poskytnete citlivé údaje útočníkům k dalšímu zneužití. Pokud jste na zprávu reagovali, doporučujeme ihned kontaktovat naše klientské centrum na telefonním čísle 800 207 207 pro zablokování služby a vygenerování nových přihlašovacích údajů. Pokud jste podvodný e-mail dostali, budeme rádi, když nám ho pošlete na adresu csas@csas.cz. Pomůžete tak dalšímu posilování prevence proti zneužití internetového bankovnictví.

Je internetbanking stále ještě bezpečný?
Internetbanking České spořitelny je zcela bezpečná a komfortní služba pro klienty za předpokladu, že dodržují základní bezpečnostní pravidla, zejména dbají bezpečnostních doporučení banky, nepřihlašují se do služby z neznámých nebo veřejně dostupných počítačů, chrání své přihlašovací údaje, nestahují do svých počítačů soubory z neznámých zdrojů a věnují pozornost aktuálnímu antivirovému nastavení na svém počítači.

Další informace najdete na www.csas.cz nebo je získáte telefonicky na bezplatné lince 800 207 207.
Dotazy prosím posílejte na adresu: csas@csas.cz.

V Praze 10. 3. 2008

Česká spořitelna, a. s.

ČESKÁ SPOŘITELNA

HOAX

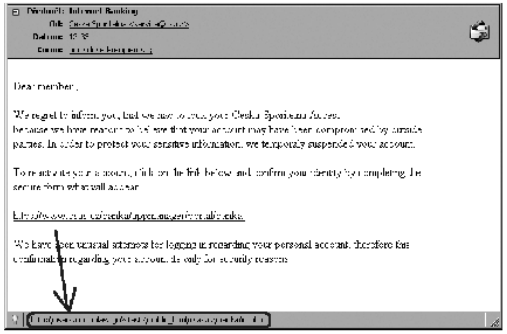
Znáte základní finty počítačové kriminality? Neskočte na ně!

Problematika bezpečného využívání internetu pro potřeby plateb a dalších operací se stává stále aktuálnější nejen v České republice. Otevřené prostředí internetu láká ke zneužití. Počítačová kriminalita je závažný trestný čin. Jaké jsou základní typy podvodů a jak se jim bránit?

Co je phishing?
Phishing je podvodný e-mail, který má za cíl vylákat od příjemce citlivé údaje, jako jsou čísla karet včetně kódu ze zadní strany karty (kód nad magnetickým proužkem, tzv. CVV/CVC ochranný kód, který se používá jen při placení u internetových obchodníků), dále například přístupové údaje pro internetové bankovnictví (klientské číslo, heslo i další bezpečnostní údaje), a následně je zneužít.

Základní znaky phishingového e-mailu:
- Snaží se vzbudit dojem, že byl odeslán z e-mailové adresy banky. Skutečná adresa odesílatele je pro příjemce maskována důvěryhodnou adresou.
- Text může vypadat jako informace o neprovedení platby, výzva k aktualizaci bezpečnostních údajů, oznámení o dočasném zablokování účtu či platební karty, výzkum klientské spokojenosti, nebo dokonce jako elektronický bulletin pro klienty.
- V textu zprávy je internetová adresa, která na první pohled vypadá, že směřuje na internetové stránky banky. Při jeho bližším prozkoumání zjistíte, že ve skutečnosti odkazuje na jiné místo, kde jsou umístěné podvodné stránky.
- Často je napsán anglicky, ale poslední dobou se objevuje i v české verzi ve stále lepší kvalitě bez pravopisných chyb.

Aktuálně
Phishing trápí české klienty, zejména klienty České spořitelny, již od začátku letošního roku.
Pozor na všechny e-mailové zprávy, které Vám chodí a budí dojem, že je rozesílá Česká spořitelna.



Po najetí myší na odkaz v textu e-mailu se ukáže skutečná adresa cílové stránky.

Jak poznám podvodný e-mail?
Phishing poznáte snadno. Pokud Vám najednou chodí jménem banky e-maily, které obsahují internetovou adresu nebo odkaz na stránky vyžadující vaše přihlašovací údaje či údaje ke kartě, je to phishingová zpráva. Banka takové zprávy nikdy nerozesílá a nemá důvod tyto informace od vás požadovat.

ČESKÁ SPOŘITELNA

Komunikace

a) Interní:

Maily všem 12,000 zaměstnancům

Průběžné info na Intranetu

b) Externí

Internet

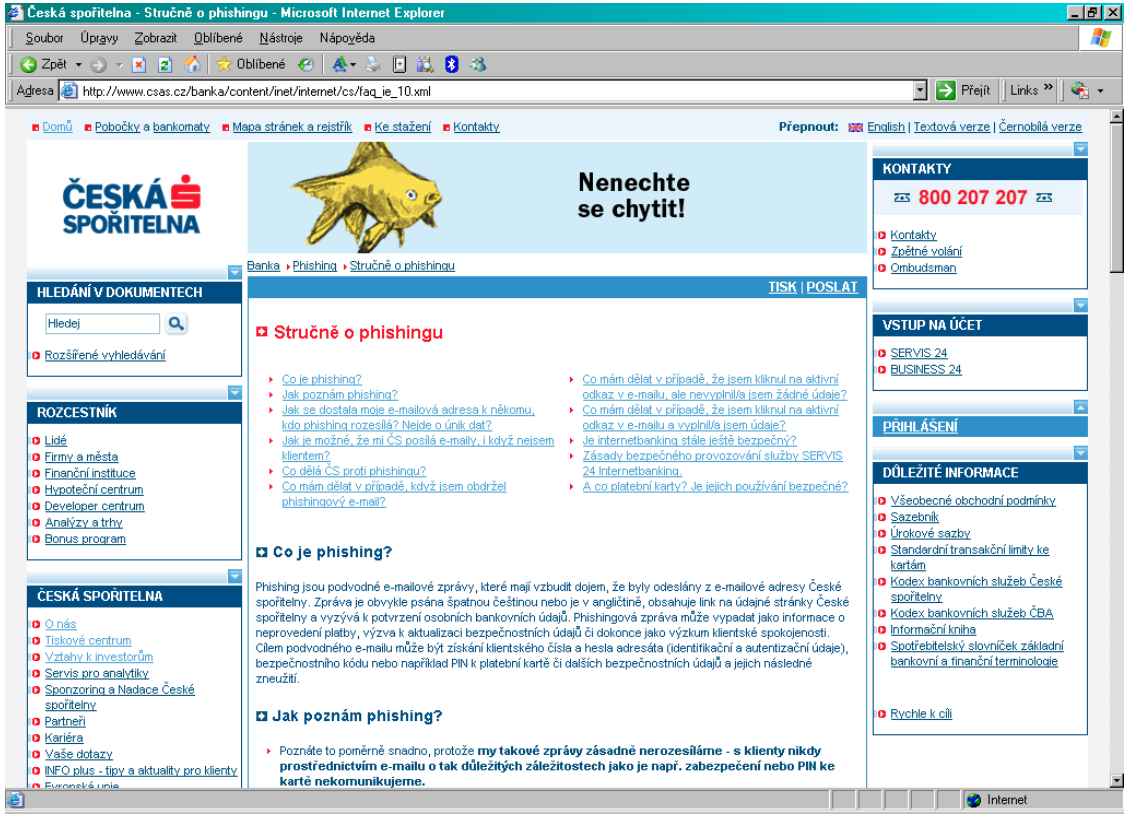
Tiskové zprávy

Rozhovory

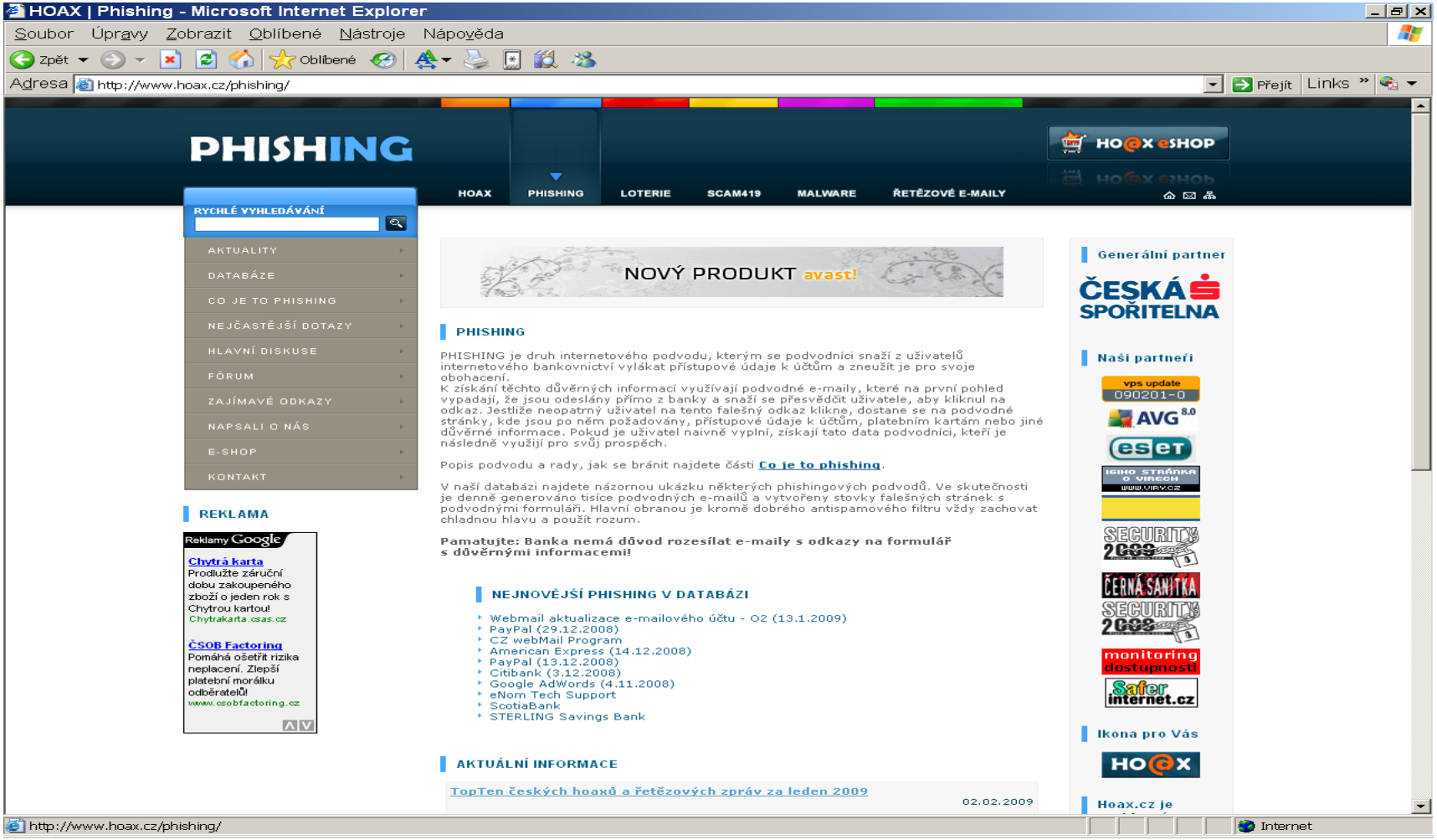
Inzerce v tisku

Odborná konference

Spolupráce s experty



Participace na osvětě



Agenda

1. **Zkušenost roku 2008 v ČR**
    1. Phishing
    2. Pharming
2. **Aktuální trendy v bezpečnosti ADK**
    1. ČR
    2. Evropa a USA
3. **Plány ČS v oblasti bezpečnosti**

Nový trend – trojské koně

- Roste počet nových variant
- Roste počet používaných hostů

- (zdroj RSA)

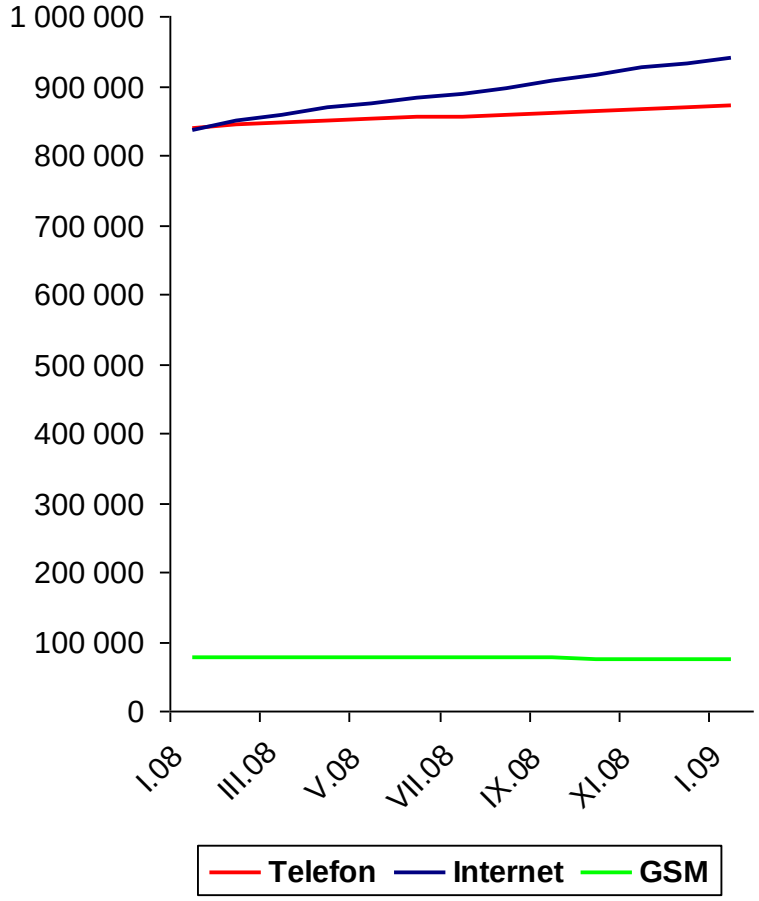
Mění se cíl útoků

Vývoj způsobu útoku:	Nástroje ochrany:
Viry šířené na médiích	On-demand souborové antiviry
Makroviry	Real-time souborové antiviry
Červy	Personální firewally
Phishing	Antispam filtry
Pharming	Hodnocení důvěryhodnosti
Trojské koně	???

Úspěšnost detekce trojských koní antivirovými nástroji byla v roce 2009 průměrně 19% (zdroj RSA)

Co klienti používají v ČS

Počty uživatelů přímého bankovnictví



Aktuální trendy:

1) **Počet uživatelů ADK roste**
   - z 2,8 milionů běžných účtů v ČS má přímé bankovnictví přes 1,2 milionu z nich (43%)
   - meziroční růst počtu klientů s ADK zpomalil na 9%
   - nejpopulárnějším kanálem se stal internet banking s 940 000 uživateli
2) **Transakce jedině přes internet**
   - každý pracovní den ČS zpracuje v průměru 270 000 on-line příkazů v objemu skoro osm miliard korun
   - 80% transakcí klienti v ČS zadají přes přímé bankovnictví

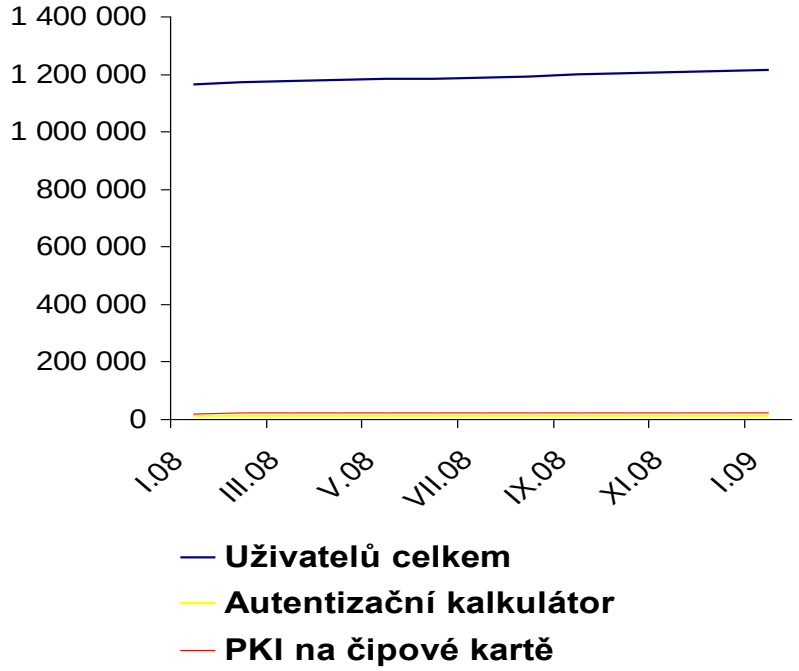
ČESKÁ SPOŘITELNA

Srovnání bezpečnostních metod v ČS

Bezpečnostní metody:

1) **používané metody**
   - SMS
   - PKI a čipová karta
   - Autentizační kalkulátor
2) **preference klientů**
   - nejčastěji používanou metodou zabezpečení jsou autorizační SMS
   - méně než tři procenta klientů používají vyšší formy zabezpečení (kalkulátor nebo PKI)

Počty uživatelů přímého bankovnictví



Klienti jednoznačně preferují jednoduchost před vyšší bezpečností

Trendy v EU

Řešení bezpečnosti:

- Většina bank používá různé varianty ověření statickým heslem nebo OTP z tabulky
- Trendem je posilování bezpečnosti dodatečnými prvky nebo dvoufaktorovými metodami

Banka	ID/heslo	vylepšené heslo	SMS	Token	CAP/DPA	PKI
Citigroup	ne	TAN	ne	Digipass	připravuje	ne
Deutsche Bank	ne	TAN, Code Card/Number card	ne	ne	připravuje	ne
ABN-AMRO	ano	ne	ne	ano	ano	ano
HSBC	ne	heslo + kontrolní otázky	ne	ano	ne	ne
UBS	ne	ne	ne	ne	ano	ne
Dexia	ano	GRID karta, TAN	ano	ano	ano	ne
Barclays Bank	ne	PIN + náhodné pozice z hesla	ne	ne	ano	ne
Fortis	ano	ne	ne	ne	ano	ne
Royal Bank of Scotland	ne	náhodně vybraná písmena z hesla	ne	ne	ano	ne
ING Direct	ano	ne	ne	ne	ne	ne
BNP Paribas					ano	
BAWAG P.S.K.	ne	ne	ne	ne	ano	ano

Většina bank zavádí nebo zvažuje metodu EMV CAP/DPA

ČESKÁ SPOŘITELNA

Trendy v ČR

Řešení bezpečnosti:

- Řeší zvlášť **autentizaci** uživatele a **autorizaci** pokynů
- Používání bezpečnostních metod se liší mezi bankami

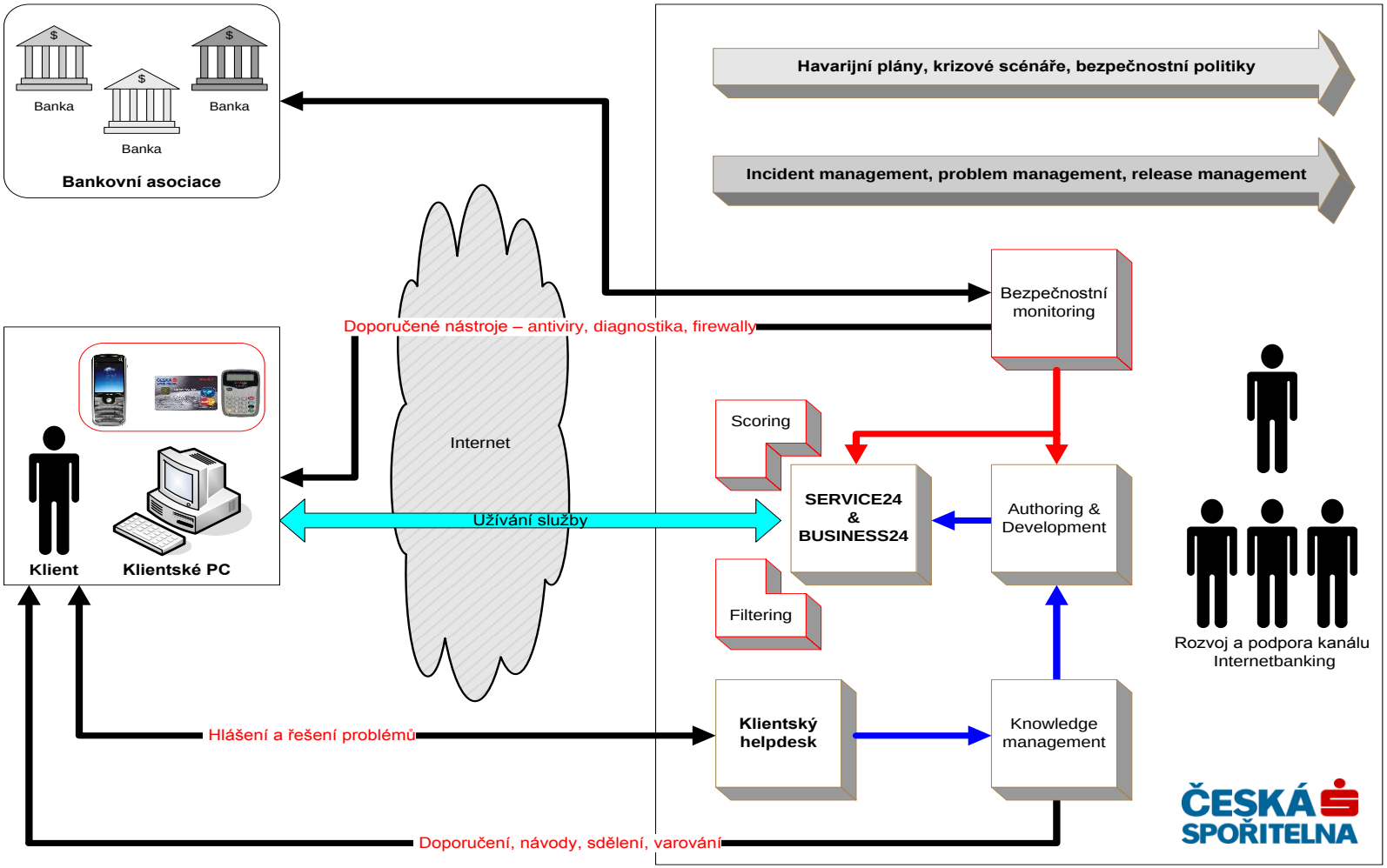
	PW	TOKEN	PKI	SMS	GRID	Summary
CITIBANK	+/-	-/+	-/-	-/-	-/-	+/+
RAIFFEISEN	+/-	-/-	-/-	-/+	-/-	+/+
POŠTOVNÍ SPOŘITELNA	+/-	-/-	-/-	-/+	-/-	+/+
ČSOB	+/-	-/+	+/+	+/-	-/-	++/++
KB	-/-	-/-	+/+	-/+	-/-	+/++
HVB	+/-	+/-	-/+	-/+	-/-	++/++
E-BANKA	-/-	+/+	+/+	+/+	-/-	+++/+++
ČESKÁ SPOŘITELNA	+/-	+/+	+/+	-/+	-/-	+++/+++

Banky nemají společný přístup k řešení bezpečnosti

Agenda

1. **Zkušenost roku 2008 v ČR**
    1. Phishing
    2. Pharming
2. **Aktuální trendy v bezpečnosti ADK**
    1. ČR
    2. Evropa a USA
3. **Plány ČS v oblasti bezpečnosti**

Komplexní bezpečnost



Nové bezpečnostní metody

Kritéria pro výběr:

- Bezpečnost, odolnost proti útokům
- Použitelnost pro různé kanály přímého bankovnictví
- Komfort, jednoduchost používání
- Náročnost z pohledu banky

Hodnocené metody:

- Heslo, vylepšené heslo, generátor OTP, HW token, SMS OTP, digitální podpis

Výsledek:

- Kritériím nejlépe vyhovují metody: **SmartSIM** a **EMV CAP/DPA**
- SmartSIM je SIMToolkit aplikace ovládaná v mobilním telefonu
- EMV CAP/DPA je aplikace na platební kartě ovládaná off-line čtečkou s klávesnicí

Další kroky:

- Ve skupině ERSTE byla za standard zvolena metoda EMV CAP/DPA
- V tomto roce příprava projektu, v roce 2011 chceme implementovat

ČS připravuje zavedení nových bezpečnostních metod

Ochrana klientského PC

Doporučení bank:

- Požadavky na správné verze systému a komponent
- Personální firewall
- Antivirový program
- Pravidelná aktualizace systému a všech programů
- Opatrnost při používání e-mailu a Internetu

Pomoc banky:

- Včasné informace o nových hrozbách

- **Nástroj**, kterým si uživatel PC otestuje
- Použití nástroje má být dobrovolné
- Výstupem je jednoduchá informace:
  - PC je/není kompatibilní s aplikací ČS Internetbankingu
  - PC má/nemá známou bezpečnostní zranitelnost
- V případě nalezení problému nástroj nabídne návod k řešení

Většina uživatelů si není jistá nastavením a bezpečností vlastního PC

ČESKÁ SPOŘITELNA

Ochrana banky

Banka je povinná sledovat podezřelé aktivity na účtech klientů

Řešení:

- Více automatizovaných nástrojů
- Hodnotí důvěryhodnost transakcí podle různých příznaků
  - Blacklisty, whitelisty
  - Pravidelné transakce v obvyklé výši
  - Používání známé/prověřené stanice
  - Přihlášení z neobvyklé lokace, v neobvyklou dobu
  - … Další sledované vzorce podvodného chování
- Je zavedený **řízený proces sledování**
- Výstupem nástrojů je varování na transakce s vyšším rizikem
- Pracovníci banky transakce dále prověřují
- Poslední možností je ověření transakce s klientem

Shrnutí

1. **Útoky využívající phishing či pharming jsou stále sofistikovanější**

2. **Novým trendem jsou útoky trojských koní**

3. **Klíčové aktivity minimalizující riziko**
   1. Prevence - komunikace
   2. Koordinace
   3. Nové bezpečnostní metody (u klienta i v bankách)

4. **Erste Bank Group bude rozvíjet zejména EMV CAP/DPA a tokeny**