ČESKÁ SPOŘITELNA

HOAX

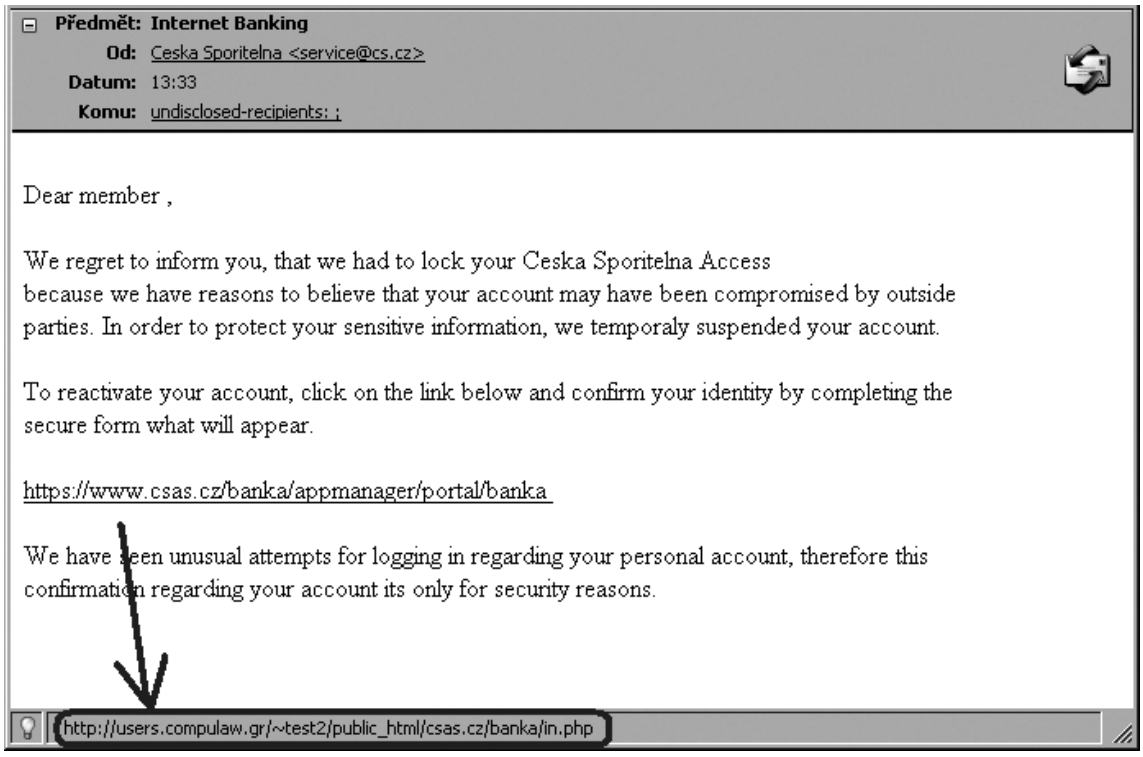
Znáte základní finty počítačové kriminality? Neskočte na ně!

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.

Jak poznám, že jsem na stránkách skutečného internetového bankovnictví?
Poznáte to tak, že se při přihlášení i při dalších operacích nebude dít nic nestandardního.

– Do služby Internetbankingu České spořitelny 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. Je to sice trochu pracnější, ale bezpečnější.
– Adresa stránky vždy začíná „https://“, písmeno „s“ před dvojtečkou znamená, že se jedná 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 bankovnictvní chová nestandardně nebo máte nějaké podezření, nezadávejte žádné důvěrné informace a ukončete aplikaci. Následně kontaktujte klientské centrum Vaší banky.

Aktuálně
Bezpečnostní monitoring České spořitelny nedávno odhalil nový typ trojského koně, který se snaží z počítačů klientů několika bank získat přihlašovací údaje do internetového bankovnictví. Vzhledem k rychlému odhalení je pravděpodobné, že údaje žádného klienta nebyly zneužity.

Kdo jsou kyberzločinci?
Je to jednotlivec nebo častěji skupina lidí, která pro peníze či s cílem obecně škodit provádí nejrůznější aktivity. Například rozesílání nevyžádaných e-mailů, distribuci malware, infiltraci a následné zneužití špatně zabezpečených webových serverů. Do počítačů běžných uživatelů internetu se tak mohou dostat spamy s nejrůznějším obsahem včetně virů a trojských koní. Ty pak škodí a samovolně se aktivují v uživatelově počítači. Boj proti takovým jednotlivcům či skupinám je trochu jako „chytat vítr“. Vzhledem k tomu, že internet nezná hranice, pochází tyto skupiny z různých koutů světa – převážně ze zemí bývalého Sovětského svazu, Číny, ale také z amerického kontinentu.

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 maximální bezpečnosti pár stokorun navíc a pořiďte si elektronický certifikát na čipové kartě. Investice do vyššího zabezpečení vašeho účtu, například čipové karty a čtečky kolem cca 1 500 Kč, se ve srovnání s náklady na bezpečnostní zámek do Vašeho bytu nebo zabezpečení auta nejeví jako příliš vysoká.

Zvažte též důvěryhodnost serveru, na kterém máte umístěnu Vaši e-mailovou schránku. Tento server sice nemá nic společného s bankovním serverem, na kterém je provozováno internetové bankovnictví, ani s jiným serverem banky. Pokud máte schránku zaplavenou nevyžádanými e-maily (spamy), správce e-mailového serveru se zřejmě řádně nestará o aktualizaci spamových a jiných filtrů. V takovém případě pak nezbývá nic jiného, než se zamyslet nad případnou změnou poskytovatele e-mailových služeb.

Informace na internetu:
Česky:
http://www.csas.cz/phishing
http://www.hoax.cz/ (http://www.phishing.cz/)
http://www.spyware.cz/

Anglicky:
http://www.antiphishing.org/
http://en.wikipedia.org/wiki/Phishing
http://en.wikipedia.org/wiki/Pharming
http://www.castlecops.com/

Praha 19. března 2008

Vydala Česká spořitelna ve spolupráci s www.hoax.cz.