VYŠETŘOVÁNÍ KYBERNETICKÝCH ÚTOKŮ A KYBERNETICKÉ TRESTNÉ ČINNOSTI

DOMÉNY LOOK - ALIKE

pplk. Lukáš Vilím

Sekce kybernetické kriminality

Národní centrála proti organizovanému zločinu SKPV

PACHATEL SE SNAŽÍ O OKLAMÁNÍ SVÉ OBĚTI

- Existence domén se **změněnými znaky byly** zaznamenány již v roce 2001.
- záměnou znaků z různých abeced je možné vytvořit doménu na první pohled nerozeznatelnou od té původní. Tento způsob se nazývá **The Homograph Attack.**
- **Pachatelé klonováním původních stránek, vytváří důvěryhodný prostor pro oběti, kde dochází k zadání osobních dat (přihlašovací údaje) do falešných stránek a získané údaje poté slouží k páchání trestné činnosti.**
- Přesvědčivé jméno domény je zásadní pro úspěšnost phishingových útoků.
- K vlákání oběti na podvodné webové stránky často dochází cestou malware.

PHISHINGOVÝ ÚTOK VÝMĚNOU IDN ZNAKŮ V DOMÉNĚ

LEGISLATIVA – TRESTNÍ ZÁKONÍK

§ 209 Podvod

- Kdo 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, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.

§ 234 Neoprávněné opatření, padělání a pozměnění platebního prostředku

- Kdo sobě nebo jinému **bez souhlasu oprávněného držitele opatří, zpřístupní, přijme nebo přechovává platební prostředek jiného**, zejména nepřenosnou platební kartu identifikovatelnou podle jména nebo čísla, elektronické peníze, příkaz k zúčtování, cestovní šek nebo záruční šekovou kartu, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci

§ 180 Neoprávněné nakládání s osobními údaji

- Kdo, byť i z nedbalosti, neoprávněně zveřejní, sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje, které byly o jiném shromážděné v souvislosti s výkonem veřejné moci, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti.

LEGISLATIVA

§ 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo **jinému opatří nebo přechovává**

a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo

b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části,

bude potrestán odnětím svobody až na dvě léta, propadnutím věci nebo zákazem činnosti.

PHISHINGOVÉ ÚTOKY – ČESKÁ POŠTA 2013

Phishingové útoky na Českou poštu neustávají

Česká pošta upozorňuje své klienty na v pořadí **již třetí phishingový útok**. Podvodný email je nyní zasílán z adresy **noreply@ceska-posta.org**. Cílem útoku je získat přihlašovací údaje klientů k jejich bankovním účtům.

E-maily z uvedené adresy nemají s Českou poštou nic společného. Pokud uživatel klikne na stažení souboru, do počítače se mu stáhne malware. Jedná se o nový škodlivý kód TrojanDropper:Win32/Hesperbot.A (detekováno Microsoftem). Tímto virem byly již infikovány počítače v Turecku, Velké Británii, Portugalsku a desítky i v České republice. Pozor by si měli dát i uživatelé mobilních zařízení se systémy Android, Symbian a BlackBerry.

„I když pošta hodně investuje do zabezpečení informačních technologií, těmto útokům se předejít nedá. Jediné, co můžeme udělat, je rychle informovat veřejnost o nebezpečí, které našim zákazníkům hrozí," říká Petr Slavík ředitel odboru bezpečnosti ICT České pošty.

Podvodné e-maily jsou psány ve formě „Informace o zásilce", kde najde zákazník údaje o nedodání zásilky a upozornění na možné sankce.

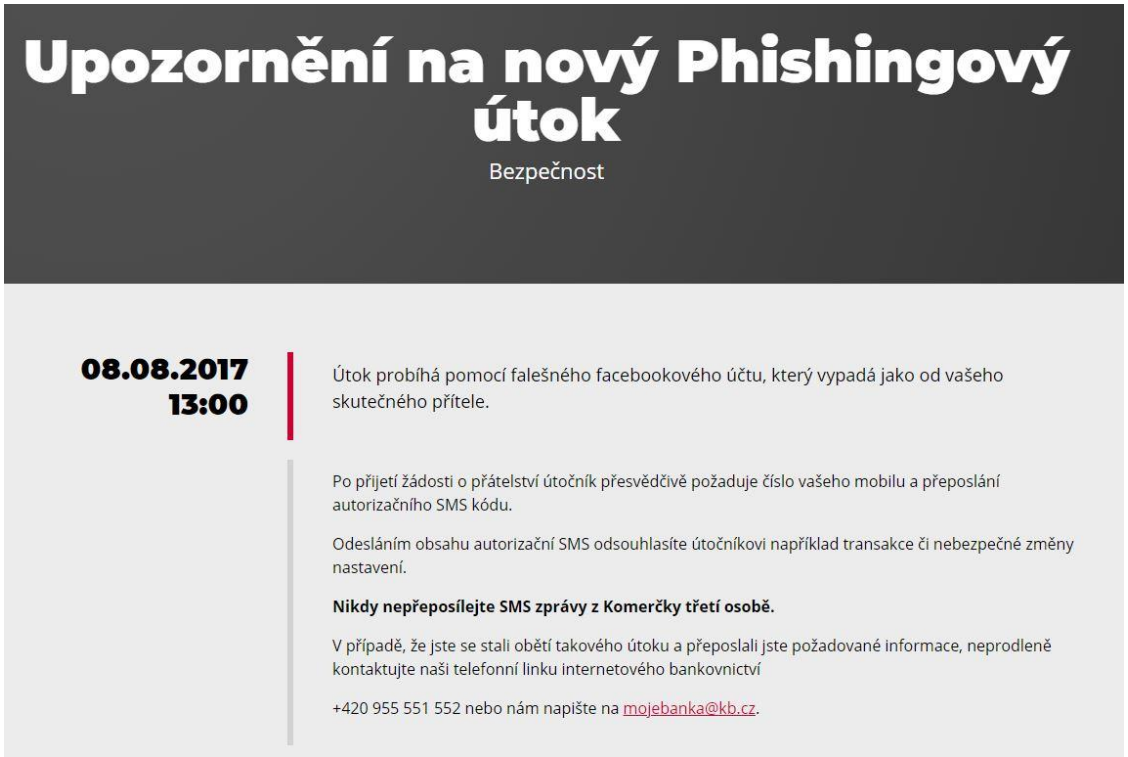
Jestliže takový e-mail obdržíte, děkujeme, že jej odešlete na adresu info@cpost.cz.

Rozhodně na tyto e-maily nereagujte!

Děkujeme.

Datum zveřejnění
12.9.13

KOMERČNÍ BANKA 2017



Upozornění na nový Phishingový útok

Bezpečnost

08.08.2017
13:00

Útok probíhá pomocí falešného facebookového účtu, který vypadá jako od vašeho skutečného přítele.

Po přijetí žádosti o přátelství útočník přesvědčivě požaduje číslo vašeho mobilu a přeposlání autorizačního SMS kódu.

Odesláním obsahu autorizační SMS odsouhlasíte útočníkovi například transakce či nebezpečné změny nastavení.

Nikdy nepřeposílejte SMS zprávy z Komerčky třetí osobě.

V případě, že jste se stali obětí takového útoku a přeposlali jste požadované informace, neprodleně kontaktujte naši telefonní linku internetového bankovnictví

+420 955 551 552 nebo nám napište na mojebanka@kb.cz.

ČESKÁ SPOŘITELNA 2017

Vážení klienti,

upozorňujeme **na novou podobu podvodného e-mailu** (tzv. phishingu), kterou jsme v posledních dnech zaznamenali a která se snaží vzbudit dojem, že byla odeslána Českou spořitelnou. Podvodníci se jejím prostřednictvím snaží vylákat vaše přihlašovací údaje na podvodné přihlašovací stránce.

Buďte k podezřelým e-mailům velmi obezřetní, vždy se do SERVIS 24 přihlašujte ze stránek banky (www.csas.cz), případně přímo ze stránek www.servis24.cz. Zároveň buďte velmi obezřetní před zadáním jakéhokoliv SMS kódu a vždy pečlivě čtěte autorizační SMS zprávy.

Pokud máte podezření, že jste podvodný e-mail obdrželi, v žádném případě nereagujte na jeho obsah, neklikejte na odkaz, který je jeho součástí, a zprávu nám přepošlete na e-mailovou adresu phishing@csas.cz. Jestliže jste již na odkaz klikli a vyplnili požadované údaje, ihned kontaktujte klientskou linku České spořitelny na bezplatném telefonním čísle 800 207 207.

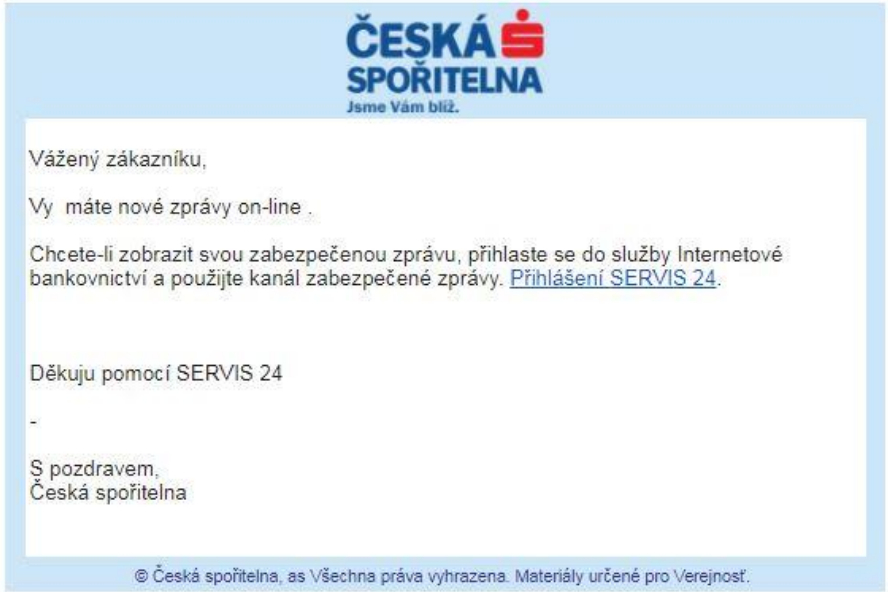
Pokud budete dodržovat tyto zásady bezpečného používání internetbankingu (www.csas.cz/bezpecnostnidesatero), minimalizujete tak možnost zneužití vašich finančních prostředků.

Česká spořitelna

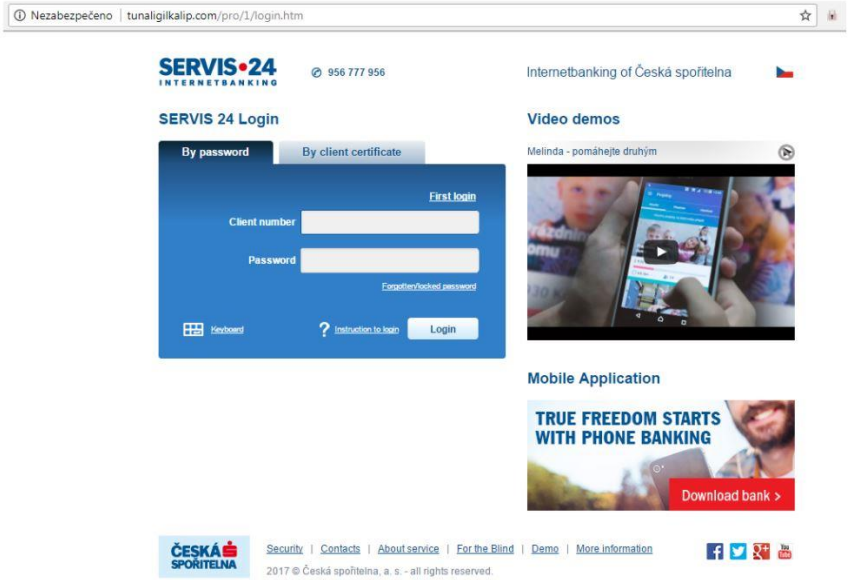
Ukázka podvodného e-mailu:

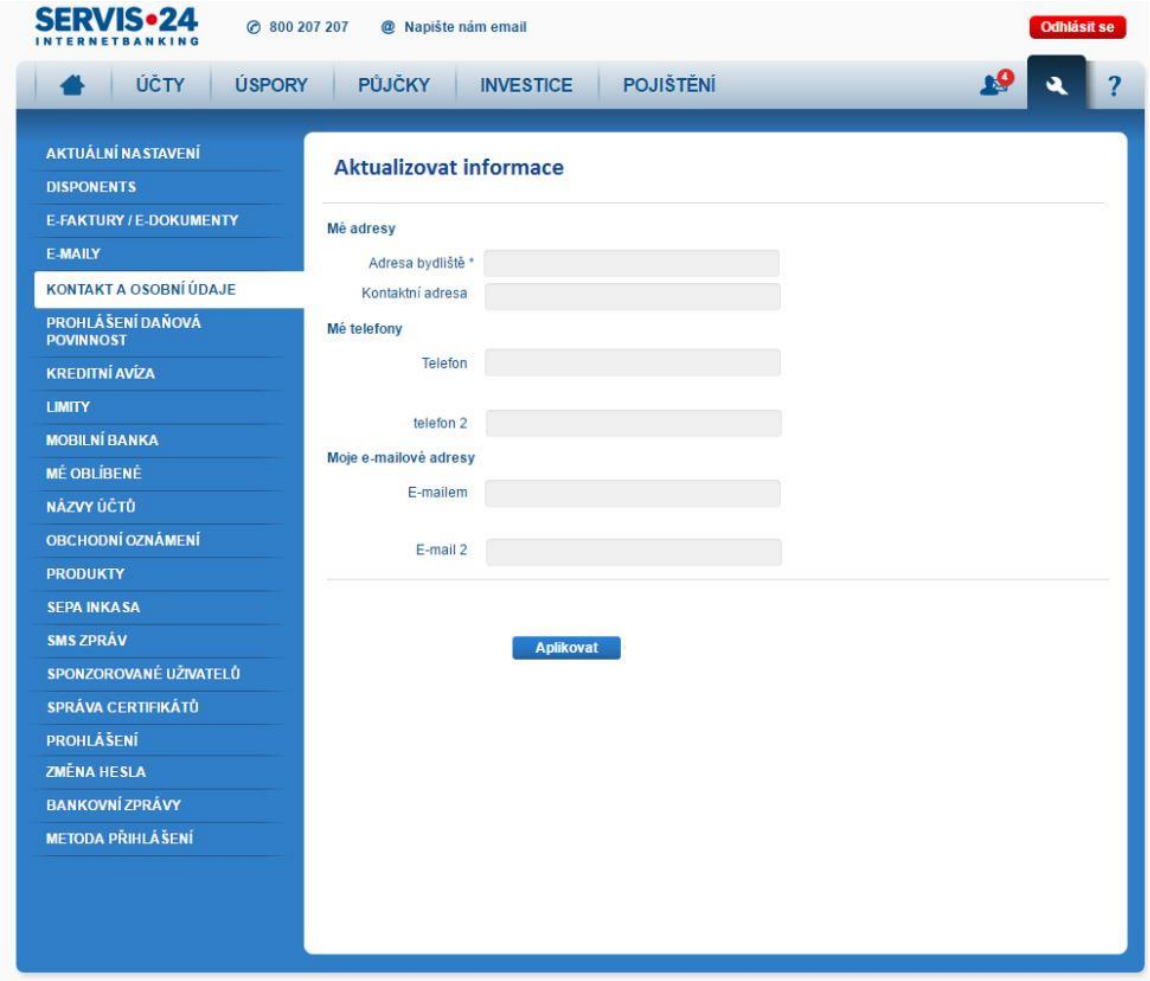
UKÁZKA PODVODNÉHO MAILU

Předmět:Důležité oznámení
Datum: Tue, 11 Jul 2017 04:11:19
Od:Česká spořitelna <messages.notification@csas.cz>

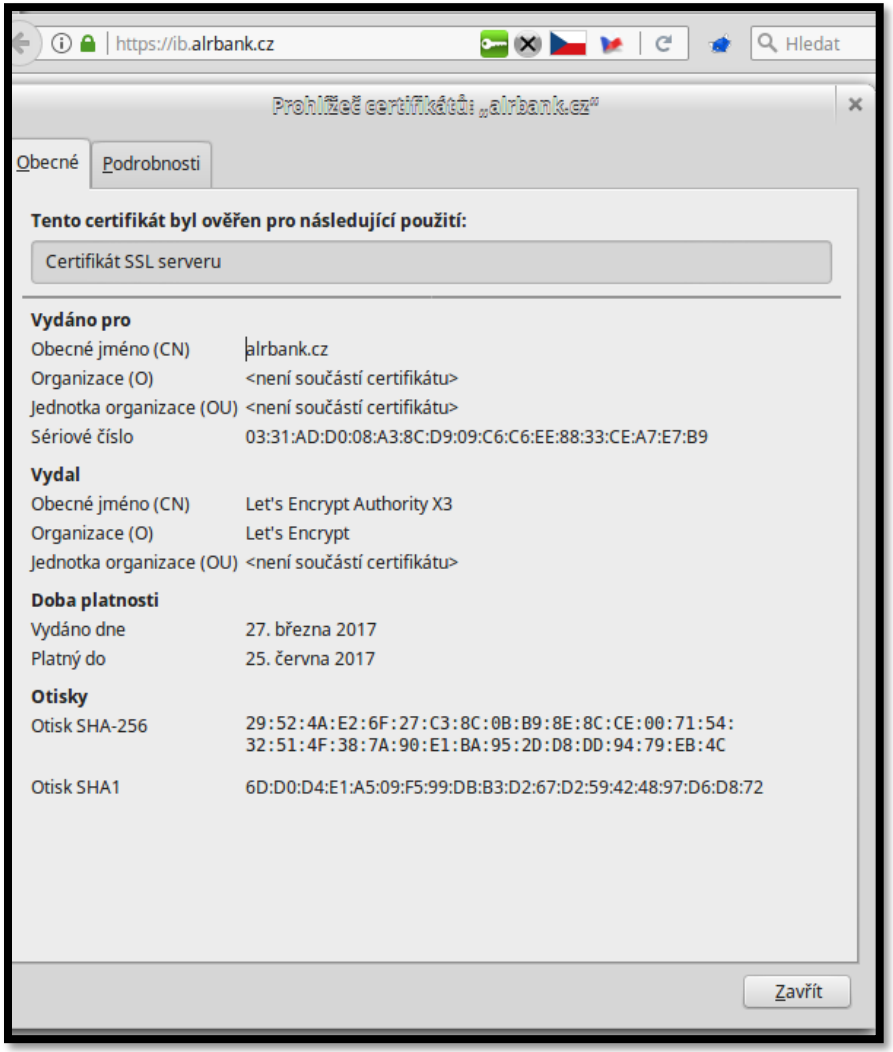


PODVODNÁ STRÁNKA




SERVIS•24
INTERNETBANKING
800 207 207
Napište nám email
Odhlásit se
ÚČTY
ÚSPORY
PŮJČKY
INVESTICE
POJIŠTĚNÍ
AKTUÁLNÍ NASTAVENÍ
DISPONENTS
E-FAKTURY / E-DOKUMENTY
E-MAILY
KONTAKT A OSOBNÍ ÚDAJE
PROHLÁŠENÍ DAŇOVÁ POVINNOST
KREDITNÍ AVÍZA
LIMITY
MOBILNÍ BANKA
MÉ OBLÍBENÉ
NÁZVY ÚČTŮ
OBCHODNÍ OZNÁMENÍ
PRODUKTY
SEPA INKASA
SMS ZPRÁV
SPONZOROVANÉ UŽIVATELŮ
SPRÁVA CERTIFIKÁTŮ
PROHLÁŠENÍ
ZMĚNA HESLA
BANKOVNÍ ZPRÁVY
METODA PŘIHLÁŠENÍ
Aktualizovat informace
Mé adresy
Adresa bydliště *
Kontaktní adresa
Mé telefony
Telefon
telefon 2
Moje e-mailové adresy
E-mailem
E-mail 2
Aplikovat

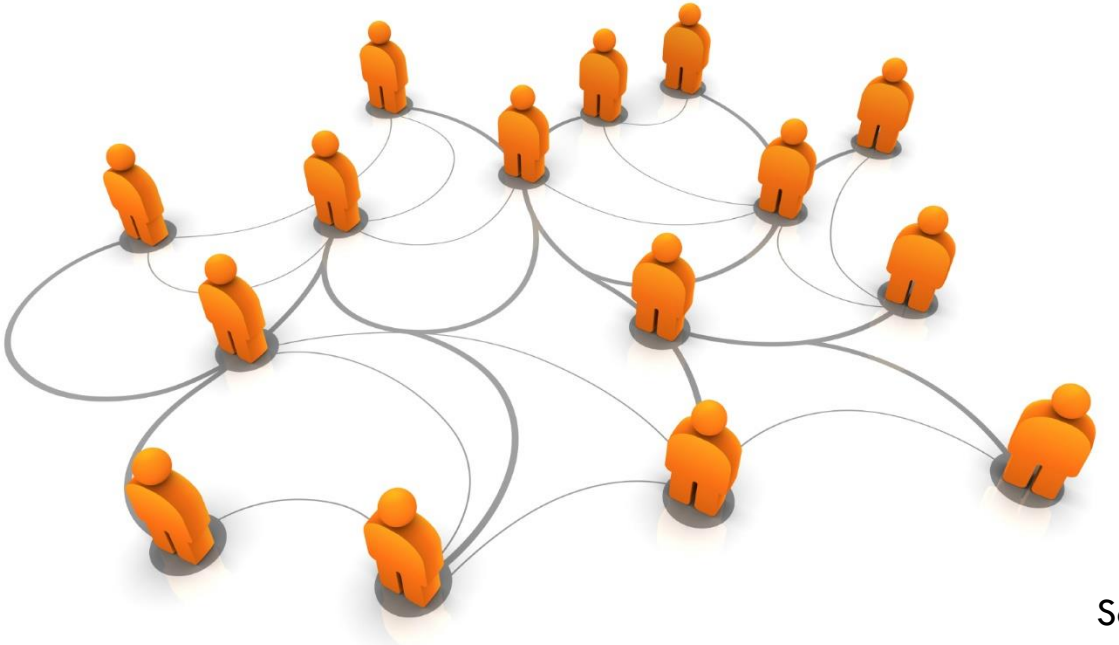
AIRBANK.CZ - 2017:



ZAJIŠŤOVÁNÍ DŮKAZŮ

- registrace domény (kdo si objednal doménu)
- uchování dat u společnosti a jejich vyžádání (data hosting), 7b tr.ř. (8/1, 8/5 tr.ř.))
- ČR nebo zahraničí (kontaktní body dle Úmluvy o kybernetické kriminalitě)
  - ✓ §78 tr.ř. povinnost k předložení nebo vydání věci - vydání dat důležitých pro trestní řízení
  - ✓ zahraničí EVP nebo MJS (MLAT - Mutual legal assistance treaty)

DĚKUJI ZA POZORNOST



pplk. Lukáš Vilím

Sekce kybernetické kriminality