Nový email???

Co mě může čekat v poště …

Obsah

1. Spam ... 3
1.1. Co je to spam? ... 3
1.2. Co není spam? ... 3
1.3. Používané metody ... 3
1.4. Jak se spamům bránit? ... 4
1.5. Zákony proti spamu ... 5
2. HOAX ... 6
2.1. Co je HOAX? ... 6
2.2. Jak HOAX poznáme ... 6
2.3. Co patří mezi HOAX? ... 6
2.4. Příklady HOAXu ... 8
2.5. Čím HOAX škodí? ... 9
2.6. Jak na HOAX reagovat? ... 10
2.7. Jak se chránit? ... 10
3. PHISHING ... 10
3.1. Co je to PHISHING? ... 10
3.2. Základní znaky PHISHINGového emailu ... 11
3.3. Jak poznat podvodné stránky? ... 12
3.4. Jak se bránit? ... 12
4. SCAM 419 ... 14
4.1. Co je to SCAM 419 ... 14
4.2. Jak se bránit? ... 14
5. Malware ... 15
6. Netiketa ... 15

1. Spam

1.1.Co je to spam?

Spam je masově odesílaná nevyžádaná elektronická pošta, tedy e-mail odeslaný na obrovské množství e-mailových schránek. Společným znakem těchto e-mailů je to, že spammeři odesílají zprávy na obrovské množství e-mailů. Nejedná se o žádnou cílenou reklamu na vytipovaný okruh lidí, ale o masové rozesílání dané zprávy (reklamy) komukoli. Dalším společným znakem spamu je, že adresa odesílatele je podvržená. Bývá nahrazena neexistujícím odesílatelem nebo nahrazena e-mailem příjemce. Rozesílání spamu je chápáno jako obtěžování, tedy kdyby spammeři odesílali spamy ze své e-mailové adresy, bylo by snadné je dohledat a odpojit od internetu. Hlavním důvodem rozesílání spamu je zisk.

Původně se používalo především pro nevyžádané reklamní e-maily, postupem času tento fenomén postihl i ostatní druhy internetové komunikace – např. diskuzní fóra, komentáře nebo instant messaging (MSN, ICQ, …).

1.2.Co není spam?

Ačkoliv by pravděpodobně neměl být označován přímo jako spam, tak se jím v případě neopatrného používání může lehce stát. Většina stránek se vás ptá, zda nechcete poskytnout váš email. Zůstanete informování o dění na jejich stránkách, o novinkách, anebo pořádaných akcích.

Jakmile oslovíte několik stránek, budete zásobováni velkým množstvím informativních emailů a nebudete mít čas na běžnou práci. Dalším oříškem jsou rozdílné zákony pro jednotlivé firmy rozmístěné kdekoliv na internetu. Podle jejich zákona mohou mít právo na další šíření emailové databáze, anebo předání vašeho emailu další firmě. Proto si dávejte pozor na umístění firmy vlastnící web.

Většinou není problém jedním kliknutím nebo jedním emailem další zasílání informačních emailů zastavit. Taková možnost by měla být u každého informačního mailu uvedena přímo. Pokud to lze tímto způsobem řešit, není důvod nastavovat filtrační pravidla pro mazání emailů tohoto typu, anebo dokonce vše řešit soudem.

1.3.Používané metody

- **Email**
  Existuje na internetu několik prostředků, které lze svým způsobem použít pro rozesílání spamu. Nejčastěji využívaným, a tím pádem i diskutovaným prostředkem, je elektronická pošta. Na internetu lze nalézt mnoho programů, které umožní i pouhému laikovi odesílat hromadné emaily. Pokud s tím není adresát jakkoliv srozuměn, tak se jedná o jednání porušující zákon.
- **Komunikační programy**

Dalším prostředkem pro rozesílání nevyžádaných zpráv jsou komunikační programy - Instant Messenger - typu ICQ. Díky databázi přístupné přes internet nebo přímo z klienta komunikátoru, lze vyhledat potřebnou cílovou skupinu. Nalezené kontakty uložit a použít pro obeslání libovolné nabídky.

- **Diskusní fóra**
  Nejméně diskutovanou oblastí, ze tří zmiňovaných, jsou diskusní fóra nebo komentáře pod článkem. Pokud se zaměříte na některý z hodně navštěvovaných serverů, zasáhnete široké masy lidí. Většinou vám nic nebrání mnoha příspěvky pod nejnovější články oslovit čtenáře s aktuálními informacemi - nejlépe vůbec se netýkajícími tématu.

1.4.Jak se spamům bránit?

Pokuste se řídit těmito zásadami:

- Zbytečně nezveřejňovat svou e-mailovou adresu na internetu, tj. neregistrovat se v podezřelých, neznámých formulářích nebo soutěžích. (Na internetu jsou roboti, kteří sbírají e-mailové adresy za účelem rozesílání spamu.)
- Na konci zprávy bývá tlačítko Odhlásit (Unsubscribe). Správně by vás po kliknutí na odhlášení měla tato funkce skutečně odhlásit, ale pokud se jedná o podvodný e-mail, často se přihlásíte jen k odebírání dalších spamových zprav. Pokud si tedy nejste stoprocentně jisti, že jde o newsletter či obchodní sdělení, k jehož zasílání jste dali dříve souhlas, neklikejte.
- Přemýšlejte, buďte ostražití a neotevírejte jakoukoli příchozí spamovou zprávu.
- Většina spamů je odesílána z uživatelova počítače bez jeho vědomí, protože je jeho počítač napaden virem. Doporučuje se tedy používat aktualizovaný operační systém + firewall + aktualizovaný antivir, jinak může rozesílat spam i váš počítač.

Obecně však neexistuje žádná jednoduchá rada, která vám umožní zbavit se spamu nadobro. Obrana před nevyžádanou poštou a její zasílání na straně druhé jsou nekončícím bojem. Rozeslané emaily vyvolají obranné mechanismy, které jsou nasazeny do protiútoku. Odesílatelé jako odvetu své způsoby opět trochu změní, aby se jejich emaily dostaly i přes tato nová opatření a kruh se uzavírá. Jen dostatečná softwarová podpora a pozadí v zákonech může tento stav změnit.

Dalším problémem kompletní obrany je subjektivní hodnocení nevyžádané pošty. Někoho může zaslaný email zaujmout, může jej mít dokonce objednán. Na druhou stranu někomu už bude připadat jako neúnosná mez, která jej donutí s existencí na internetu skoncovat.

Pokud jste zahlceni spamem nejjednodušší řešení je **vytvoření nového emailového účtu**. Jedná se o radikální krok, který vám nepomůže, pokud nezměníte trochu své chování. Musíte pochopit, kdy se stává pro odesílatele nevyžádané pošty váš email zajímavý. Jinak se můžete dostat do stádia, kdy budete měnit email každých pár týdnů a to nebude vůbec praktické.

Největší nevýhodou při změně adresy je ztráta stávajících kontaktů, které jste měli. Většině pravděpodobně dáte vědět, ale nemusíte mít kompletní seznam. Nenastavujte si na staré adrese automatickou odpověď s novou adresou! Takto by se jen případní spammeři dozvěděli, kde vás mají dál hledat.

Nejen velikost emailové schránky je důležitá při vytvoření nové adresy. Dnes již téměř každý nabízí různé stupně ochrany proti nevyžádané poště. Dále je zde ještě možnost toto filtrování doplnit při stahování pošty na váš počítač (pokud je možno poštu stahovat). Ve většině emailových klientů jsou integrovány různé antispamové filtry.

Opatrně si vybírejte označení emailové adresy před zavináčem. Běžně se stává, že jsou na nasbírané domény rozesílány emaily podle slovníku. Použije se nějaký rozsáhlý soubor jmen a označení, která lidi používají na internetu ať již jako přezdívky nebo v jiných emailových adresách. Z toho jsou generovány další adresy přímým použitím nebo různým vzájemným kombinováním. Nebojte se použít roztodivné kombinace nejrůznějších znaků. Emailovou adresu si dnes již nemusí nikdo pamatovat. Jednou si ji uloží do adresáře a potom již používá napsané označení, které si k adrese přiřadil. V programu Outlook se po zadání adresy do adresáře uživatel při běžné komunikaci s danou adresou již nesetká.

Další obranou před nevyžádanou poštou je založení několika emailových adres pro různé účely. Jeden typ můžete mít pro příspěvky do diskusních fór, registrační email nebo obchodní jednání. Asi nejpraktičtější je mít tři typy emailových adres:

a) pro důvěryhodnou skupinu - pracovní komunikace, blízcí příbuzní
b) polo důvěrná komunikace - zákazníci, vzdálení příbuzní
c) pro ostatní použití - diskusní skupiny, zveřejnění na internetu, oslovení úplně neznámých

1.5.Zákony proti spamu

Nynější zákony

Od 7. září 2004 začal platit nový **Zákon o některých službách informační společnosti** (č. 480/2004 Sb.), který problematiku spamu upravuje a vyžaduje prokazatelný souhlas příjemce zprávy. Dohledem nad dodržováním zákona byl pověřen Úřad pro ochranu osobních údajů. Tento zákon byl postupně novelizován, a to v letech 2005, 2006 a naposledy v roce 2007.

Zákon byl vytvořen podle směrnice Evropského společenství č. 2000/31/ES. Spam definuje jako obchodní sdělení, což jsou všechny formy sdělení určeného k přímé či nepřímé podpoře zboží či služeb nebo image podniku fyzické či právnické osoby. Zákon řeší nejen internetový spam, ale také jiné formy elektronické komunikace (SMS, telemarketing).

Podle zákona se za obchodní sdělení nepovažují údaje umožňující přímý přístup k informacím o činnosti fyzické či právnické osoby nebo podniku, zejména doménové jméno nebo adresa elektronické pošty; za obchodní sdělení se dále nepovažují údaje týkající se zboží, služeb nebo image fyzické či právnické osoby nebo podniku, získané uživatelem nezávisle.

Obchodní sdělení může prodejce zaslat, když:

a) je adresátem jeho zákazník,
    a. který zasílání podobných sdělení v minulosti neodmítl,
    b. sdělení týká obdobného zboží či služeb,
b) adresát obchodníkovi poskytl informovaný souhlas.

2. HOAX

2.1.Co je HOAX?

Anglické slovo HOAX [:houks:] v překladu znamená: *Falešnou zprávu, Mystifikaci, Novinářskou kachnu, Podvod, Poplašnou zprávu, Výmysl, Žert, kanadský žertík.*

V počítačovém světě slovem HOAX nejčastěji označujeme **poplašnou zprávu**, která varuje před neexistujícím nebezpečným virem.

2.2.Jak HOAX poznáme

Typický text poplašné zprávy obsahuje většinou tyto body:

- **Popis nebezpečí (viru)**
  Smyšlené nebezpečí (vir) bývá stručně popsané, v případě viru bývá uváděný i způsob šíření.
- **Ničivé účinky viru**
  Zde záleží převážně na autorově fantazii. Ničivé účinky mohou být celkem obyčejné, třeba zformátování disku nebo už míň důvěryhodné - zběsilý útěk myši do ledničky, roztočení HDD opačným směrem, výbuch počítače…Autoři hororů zde mohou hledat inspiraci.
- **Důvěryhodné zdroje varují**
  Ve většině případů se pisatel poplašné zprávy snaží přesvědčit, že varování přišlo od důvěryhodných zdrojů ("IBM a FBI varují" nebo "Microsoft upozorňuje" atd.)
- **Výzva k dalšímu rozeslání**
  Tento bod HOAX vždy obsahuje! Mnoho nezkušených uživatelů se nechá zprávou napálit a bez přemýšlení výzvu uposlechnou. Právě proto se tyto nesmysly lavinovitě šíří.

Jako HOAX můžeme také označit šířenou zprávu, která obsahuje nepřesné, zkreslující informace, účelově upravené polopravdy nebo směsku polopravd a lží.

V praxi můžeme použít následující pravidlo:

Jestliže zpráva obsahuje výzvu k hromadnému rozeslání na další adresy, je to podezřelé a s největší pravděpodobností HOAX. Občas to také může být původně opravdová prosba o pomoc, ale i ty svého největšího šíření dosáhnou v době, kdy jsou již neaktuální.

Pokud podobnou zprávu obdržíte a nemáte jistotu, můžete si prohlédnout některý ze seznamů HOAXů a určitě tam obdobu doručené zprávy najdete. Také pravděpodobnost, že byste stopnutím podezřelého e-mailu někomu uškodili, je minimální. Šířením hoaxů a jiných řetězových e-mailů se uživatel proviňuje proti pravidlům **Netikety - pravidel chování na Internetu**.

2.3.Co patří mezi HOAX?

Mezi HOAX můžeme zařadit:

- **Varování před smyšlenými viry a různými útoky na počítač**
  Nejčastější typ poplašných e-mailů.

Pozor na injekční jehly!

ČR (vír) - Dávejte pozor, na co si sedáte! Jde o zdraví i o život! Takové varování putuje po internetu. V textu jsou pak popsány případy, kdy se například návštěvníci kina při usednutí píchli o nastražené injekční stříkačky. Na jehle byl papír se vzkazem: »Právě jsi byl nakažen virem HIV!« Tyto případy se údajně staly v zahraničí i v Praze! Pisatelé v e-mailu tvrdí, že testované jehly opravdu obsahovaly virus HIV nebo žloutenky.

024920/2

- **Popis jiného nereálného nebezpečí**

Zprávy varují před vymyšleným nebezpečím z běžného života - mimo oblast výpočetní techniky. Často obsahují směs lží a polopravd, které nezasvěcený člověk nemůže s jistotou posoudit.

- **Falešné prosby o pomoc**

Kdysi skutečná prosba o pomoc, většinou se masově rozšíří až po její aktuálnosti. Typickým příkladem jsou prosby o darování krve pro nemocného člověka. Trapný pokus o žert, který útočí na základní lidské city.

- **Fámy o mobilních telefonech**
  Vymyšlené, zkreslené nebo neúplné informace o mobilních telefonech. Většinou bývají také masově šířené.
- **Petice a výzvy**
  Smyšlená petice jako žert. Nedomyšlená snaha boje za určitou věc. Petice šířená e-mailem často neobsahuje potřebné údaje podepisujících se (pokud je lze takto označit), aby petice byla platná. Naopak, jestliže ke jménu připojíte další osobní údaje, dáváte je k dispozici komukoliv, kdo e-mail dostane. Zpráva s vašimi údaji se šíří pyramidovitě v mnoha různých variantách na další adresy. Kdykoliv může být změněn i text údajné petice a váš podpis může být pod něčím, s čím nesouhlasíte.
- **Pyramidové hry a různé nabídky na snadné výdělky**
  Většinou to jsou různé obdoby pyramidových her. Podle našich zákonů jsou pyramidové hry zakázány, proto se je organizátoři snaží maskovat jako prodej různých produktů. Tyto nabídky mají stejný základ: koupím produkt od zapojeného účastníka, tím již zapojené členy posunu o pozici výš a snažím se přesvědčit jiné, aby produkt koupili a moji pozici také vylepšili. Pokud je trh nasycen - a to díky pyramidovému způsobu je poměrně rychle - poslední mají minimální šanci, že někdo další se připojí, a jsou to pouze jejich peníze, které pomohly alespoň částečně vrátit náklady zapojeným předchůdcům. Nabídky na odměnu nebo slevu na služby za hromadné rozeslání e-mailů. Pořádně si rozmyslete, jestli je slíbená odměna dostatečnou kompenzací za obtěžování vašich přátel. Žertovná zpráva, ve které se slibuje za její další rozeslání lákavá odměna.
- **Řetězové dopisy štěstí**
  Čínské modlitby a různé dopisy štěstí šířené z pověrčivosti nebo z neznalosti.
- **Žertovné zprávy**
  Různé žertovné zprávy, které si posílají kamarádi a známí. Zde bych pouze připomněl, že ne všichni mají stejný smysl pro humor, a proto není vhodné je hromadně šířit na všechny adresy.

Také sem můžeme zařadit vyloženě podvodné emaily:

- **Nigerijské podvodné e-maily (SCAM 419)**
  Podvodníci rozesílají e-maily s lákavými nabídkami na velkou sumu peněz. Údajnými odesílateli jsou například vdovy po bohatém podnikateli, které žádají o pomoc při převodu peněz ze země. Jako odměna za pomoc je slíbeno až několik miliónů dolarů. Hlavní trik podvodu je v tom, že

nachytaná oběť je nucena postupně platit několikatisícové poplatky na údajné výdaje spojené s převodem peněz, který je stále pod různými záminkami odkládán.

- **Podvodné loterie**
  Uživatelům je rozeslán e-mail, že vyhráli vysokou cenu v mezinárodní loterii. Do údajného slosování se dostali například výběrem e-mailových adres z celého světa a právě ta jejich vyhrála. Když se šťastlivec o svoji výhru přihlásí, dozví se, že musí před vyplacením výhry zaplatit manipulační poplatek ve výši několika desítek až tisíce EUR. Tento poplatek samozřejmě není možné strhnout z vyplácené výhry. I když naivní šťastlivec zaplatí, žádnou výhru neobdrží. Vymáhání výhry je nereálné a šance na vrácení peněz nulová.
- **PHISHING**
  Na velké množství adres jsou rozeslány podvodné dopisy, které na první pohled vypadají jako informace z určité banky. Tyto dopisy plně využívají tzv. sociální inženýrství. Příjemce je informován o údajné nutnosti vyplnit údaje v připraveném formuláři, jinak mu může být zablokován účet, nebo jinak omezena možnost využití svých finančních prostředníků. V e-mailu bývá uveden odkaz na připravené stránky s formulářem, které jakoby odkazovaly na server banky. Ve skutečnosti je uživatel přesměrován na cizí server, ale vytvořený ve stejném stylu, jako jsou stránky příslušné instituce. Chycený uživatel nepozná rozdíl a může vyplnit předvolená políčka, kde jsou po něm požadovány důvěrné informace - čísla účtu, kódy k internetovému bankovnictví, pin pro platbu atd. Takto získané údaje mohou podvodníci velice snadno zneužít.

2.4.Příklady HOAXu

- **Vajíčko uvařené mobilem**
  „Umísti syrové vajíčko do porcelánového stojánku. Na jeho protější strany dej dva mobilní telefony. Zavolej z jednoho telefonu na druhý a zůstaň na lince. Během prvních 15 minut se nic neděje. Po 25 minutách je skořápka vajíčka horká. Po 40 minutách se bílek uvaří, je pevný. Po 65 minutách je i žloutek plně uvařen."

- **Bill Gates se rozhodl podělit o své bohatství**
  „Ahoj všichni, prosím Vás, neberte to na lehkou váhu. Bill Gates se rozhodl podělit se o své bohatství. Pokud tohle budete ignorovat, později Vás to může mrzet. Microsoft a AOL jsou teď největší Internetové společnosti a aby se ujistili, ze Internet Explorer zůstává nejrozšířenějším programem, rozeběhli e-mailový beta test. Jestli přepošlete tento mail svým přátelům, Microsoft to zjisti (pokud jste uživatele Microsoft Windows) do dvou týdnů. Za každého člověka, kterému tento mail přepošlete, Vám Microsoft zaplati $ 245, za každého člověka, kterému to pošlete a on také, Vám Microsoft zaplati dalších $ 243, a za každého třetího člověka, který tuto zprávu obdrží, Vám zaplati $ 241. Do dvou týdnů se Vás Microsoft bude kontaktovat, aby obdržel Vaší adresu a pak Vám posle sek.
  S pozdravem Chinu!
  Myslel jsem si, že je to blbost, ale po dvou týdnech, co jsem tento mail obdržel a přeposlal dále, mě Microsoft kontaktoval kvůli adrese a během par dnu mi přisel sek na $ 24 800. Musíte odpovědět drive, než tato akce skončí. Jestli si tohle může někdo dovolit, pak je to Bill Gates. Pro něj jsou to výdaje na marketing. Prosím přepošlete to co nejvíce lidem. Dostanete minimálně US$ 10 000."

2.5.Čím HOAX škodí?

Mnohým se může zdát, že šíření HOAXů nemůže být škodlivé. HOAX vám pevný disk nezformátuje, ani nesmaže či neukradne soukromá data. Dokonce vám nezničí ani počítač. Přesto v jeho souvislosti lze mluvit o nebezpečí. Při bližším pohledu na problém zjistíme následující:

- **Obtěžuje příjemce**
  Opakovaný příjem nesmyslných zpráv je pro mnohé uživatele nepříjemné, zejména v době epidemie, kdy se v e-mailových schránkách objevuje stejná zpráva několikrát denně.
- **Zbytečné zatěžování linek a serverů**
  Přestože výkonnost serverů a rychlost vzájemného propojení se zvyšuje, je také nutné si uvědomit, že zatížení sítí také narůstá. Vyšší nároky na sítě jsou dány nejen narůstajícím počtem uživatelů, ale také stále větším počtem šířících se škodlivých kódů a hlavně různého spamu. **V dnešní době tvoří spam přes 90% veškeré e-mailové komunikace!** Proč zbytečně tento počet navyšovat zbytečnými HOAXy a řetězovými zprávami.

Velké množství HOAXů rozesílají uživatelé tím nejhorším způsobem, tzn. předat dál a na všechny adresy. Tak dochází k postupnému přidávání adres k textu zprávy a samozřejmě narůstá velikost zprávy, často až do velikosti přesahující 100 kB. Pro porovnání, běžný e-mail mívá velikost 2-6 kB, e-mail s přiloženým dvoustránkovým doc dokumentem přibližně 65 kB. V součtu pak jejich velikost může dosáhnout i mnoha MB.

- **Šířením HOAXu můžete vyzradit důvěrné informace**
  Jestliže se HOAX přeposílá výše uvedeným způsobem (na všechny adresy), **dává se k dispozici obrovský seznam e-mailových adres náhodným příjemcům**. Kvůli lavinovitému šíření zprávy nemůžete vědět, komu v dalších úrovních bude e-mail doručen. **Seznam adres je rájem pro spamery**, kteří pak mohou na získané adresy posílat nevyžádané e-maily. Někteří uživatelé se nestačí divit, jak mohli spammeři získat jejich adresu, kterou svěřili pouze několika známým. Ve skutečnosti stačí, aby se hromadně rozeslaný e-mail dostal na počítač infikovaný škodlivým kódem, který z něj dokáže vysbírat adresy a dále je zneužít.

Další nepříjemná situace by mohla nastat, kdyby se Váš seznam adres klientů a obchodních partnerů dostal ke konkurenci.

V případě různých petic nebo smyšlených podpisových akcí se požaduje vyplnění různých osobních údajů včetně adresy a rodného čísla. Opět nikdy nemůžete vědět, kdo si Vámi vyplněné informace přečte a jakým způsobem je zneužije.

- **Může přímo poškodit jinou osobu nebo společnost**
  Některé HOAXy nebo řetězové zprávy uvádí **úplné kontakty nebo třeba jen telefonní čísla na osobu, která sice se zprávou nemá nic společného, ale přesto se na ni v textu odvolává.** Typickým příkladem je nabídka štěňátek, kdy jsou uvedeny telefonní čísla, kam případní zájemci mohou volat. Často jsou to kontakty na lidi, kteří nikdy žádného psa neměli, ale třeba z pomsty nebo škodolibosti někdo vypustí e-mail do světa. V takovém případě je telefon postiženého prakticky už nepoužitelný.
  Také šíření nepravdivých, polopravdivých nebo zkreslených informací o různých společnostech jim mohou způsobit různé nepříjemnosti. Například poškození dobrého jména, ale také

zbytečné zahlcení zákaznických linek, kam lidé na základě falešné zprávy zbytečně volají. Také skutečné prosby o pomoc mají své stinné stránky. Většinou se rozšíří až po té, co již nejsou aktuální, ale lidé se na uvedné kontakty stále ozývají.

- **Ztráta důvěryhodnosti**
  Odesláním HOAXu obchodním partnerům svoji prestiž určitě nezvýšíte. Šíření poplašných zpráv státními úředníky není dobrou vizitkou úřadu a vrcholem je rozeslání falešného varování před virem zaměstnancem firmy, která se zabývá výpočetní technikou nebo programováním (i to se opravdu stává).
- **Pozor na automatické podpisy**
  Automatické podpisy z vás mohou udělat autora HOAXu! Již mnohokrát se stalo, že uživatel přeposlal HOAX nebo řetězový e-mail a poštovní klient k textu zprávy připojil jeho podpis i s adresou a telefonním kontaktem. Takto upravená zpráva vypadá, že se přímo týká podepsané osoby a případné následky může nést podepsaná osoba.

2.6.Jak na HOAX reagovat?

Jestliže nemáte jistotu, zda obdržená zpráva je HOAX, prohlédněte si nejdříve některý ze seznamů HOAXů. Také je možné zadat i ve vyhledávačích klíčová slova typická pro příslušnou zprávu. Je velice pravděpodobné, že stejný nebo obdobný text najdete. V takovém případě můžete e-mail s klidným svědomím vymazat.

Také je možné slušně odpovědět pouze odesílateli a upozornit ho například tímto textem, že zpráva, kterou Vám poslal je HOAX:

Zpráva, kterou jste nám zaslali, je HOAX - poplašná zprava, která obsahuje nepravdivé nebo zkreslené informace!
Podrobné informace o Vámi zaslaném HOAXu, databázi rozšířených řetězových zpráv a odkazy na další podobné stránky najdete na adrese: http://www.hoax.cz/

2.7.Jak se chránit?

- Nikdy nevěřte všem informacím, které vám z neznámého zdroje přijdou na e-mail.
- Nikdy nesdělujte své osobní informace (PIN, rodné číslo apod.).
- Nikdy nedůvěřujte zprávám, které vám posílá e-mailem vaše bankovní instituce (bankovní instituce s klienty v případě důležitého sdělení tímto způsobem zpravidla nekomunikují).
- Všechny informace si vždy ověřujte.

3. PHISHING

3.1.Co je to PHISHING?

PHISHING je druh internetového podvodu, kterým se podvodníci snaží z uživatelů internetového bankovnictví vylákat přístupové údaje k účtům a zneužít je pro svoje obohacení. K získání těchto důvěrných informací využívají podvodné e-maily, které na první pohled vypadají, že jsou odeslány přímo z banky a snaží se přesvědčit uživatele, aby kliknul na odkaz. Jestliže neopatrný uživatel na tento falešný odkaz klikne, dostane se na podvodné stránky, kde jsou po něm požadovány,

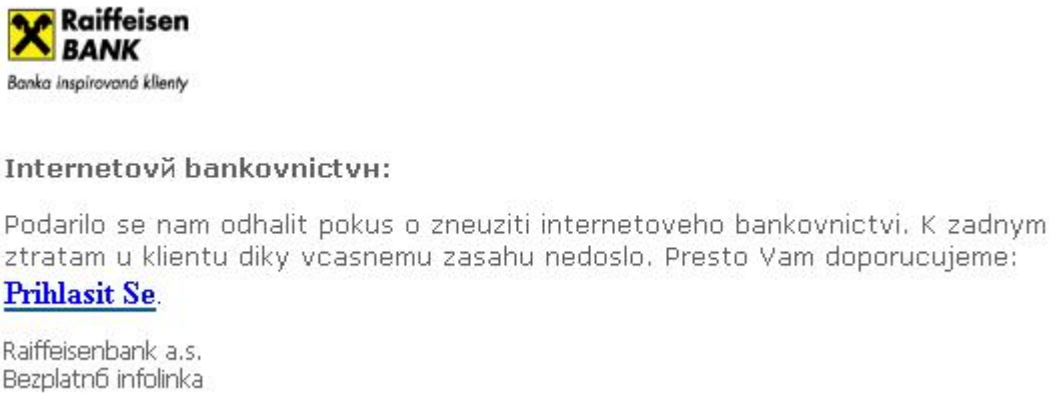
přístupové údaje k účtům, platebním kartám nebo jiné důvěrné informace. Pokud je uživatel naivně vyplní, získají tato data podvodníci, kteří je následně využijí pro svůj prospěch.

Nejčastěji jsou to údaje k platebním kartám včetně PINu nebo různé přihlašovací údaje k účtům. Nemusí jít jenom o účty přímo bankovní, ale také ostatních organizací, kde dochází k manipulaci s penězi nebo je možné jakýmkoliv způsobem zneužit jejich služeb. Příkladem může být PayPal, eBay, Skype, Google.

3.2.Základní znaky PHISHINGového emailu

- Snaží se vyvolat dojem, že byl odeslán organizací, z jejíchž klientů se snaží vylákat důvěrné informace. Toho se snaží docílit grafickou podobou e-mailu a zfalšováním adresy odesílatele.
- 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 jako elektronický bulletin pro klienty.
- V textu zprávy je link, který na první pohled většinou vypadá, že směřuje na stránky organizace (banky). Při jeho bližším prozkoumání zjistíte, že ve skutečnosti odkazuje na jiné místo, kde jsou umístěné podvodné stránky.

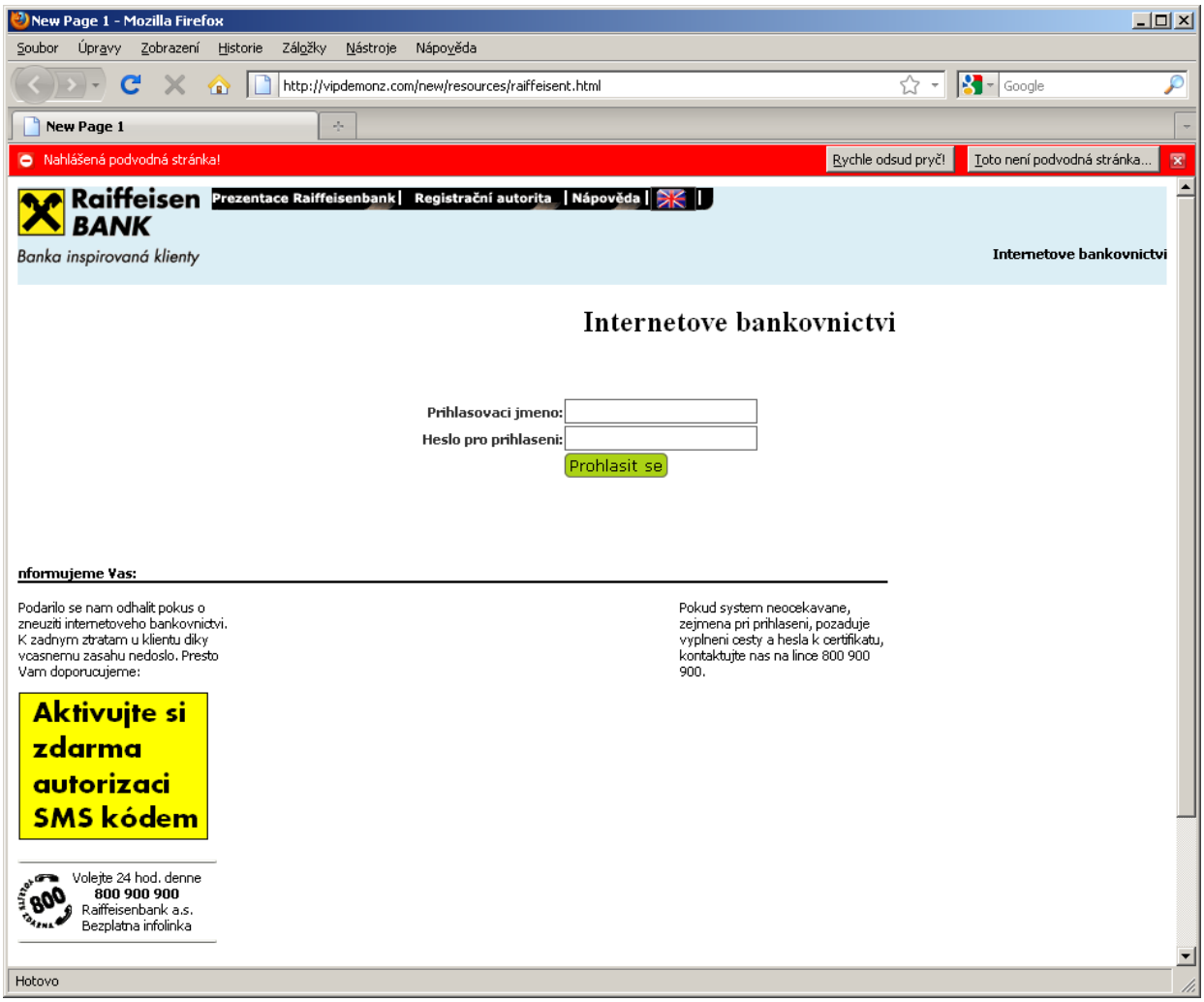
Jestliže vám chodí jménem banky e-maily, které obsahují link, na stránky vyžadující vaše přihlašovací údaje, či údaje ke kartě, je to phishingová zpráva. Banka takové zprávy nikdy nerozesílá a nemá důvod tyto informace od vás požadovat! Pokud uživatel klikne na odkaz v e-mailu, dostane se na falešné stránky podvodníků, které jsou vytvořeny ve stejném stylu, jako originální stránky organizace (banky). Na podvodných stránkách je připraven formulář, kde jsou požadovány důvěrné informace - čísla účtu, kódy k internetovému bankovnictví, PIN k platební kartě, přihlašovací údaje ke službám a podobně.



Podvodné stránky bývají umístěny na napadnutých, špatně zabezpečených serverech. Proto ve většině případů bývá v internetovém prohlížeči v poli pro zadání adresy uvedená jiná adresa, která nemá s příslušnou organizací nic společného. Toto je jeden z poznávacích bodů, že se uživatel dostal na podvodnou stránku. Někdy se podvodníci snaží pomocí různých triků tento údaj v adresním řádku zamaskovat.

3.3.Jak poznat podvodné stránky?

- **Formulář vybízí k vyplnění důvěrných informací, které by banka neměla požadovat.**
- **V adresním řádku prohlížeče se zobrazuje adresa, která nepatří organizaci, jejichž stránky se snaží napodobit.** Uvedená adresa se může snažit originální napodobit, ale vždy bude jiná, případně může začínat číselným kódem IP adresy. Vyskytly se i případy, kdy se podvodníci snaží tuto skutečnost maskovat.
- **Ve většině případů komunikace probíhá po běžném, nezabezpečeném protokolu** (adresa začíná http://).



Adresa pro údajné internetové bankovnictví: „http://vipdemonz.com/new/resources/raiffeisent.html"

3.4.Jak se bránit?

- **Na odkazy v e-mailu neklikejte!** Přesměrují vás na podvodné stránky, které se vás mohou snažit oklamat a pokusit se vylákat důvěryhodné informace, ale také mohou obsahovat škodlivé kódy, které se vám pokusí instalovat do počítače.
- **Jestliže potřebujete vstoupit na stránky internetového bankovnictví nebo na stránky příslušné organizace, raději napište internetovou adresu do prohlížeče sami!**

- **Dejte pozor na překlepy!** Podvodníci si mohou dočasně zaregistrovat adresu, která se bude pouze nepatrnou změnou písmen lišit od pravé. Při překlepu se nepozorný uživatel může dostat na falešné stránky.
- **Pokud se vaše elektronické bankovnictví chová nestandardně nebo jsou po vás požadovány jiné údaje než obvykle, nezadávejte je! Ukončete svoji činnost a kontaktujte zákaznické centrum banky!** Existuje další trik podvodníků, tzv. ***pharming***. Ten umožňuje přesměrovat uživatele na podvodné stránky, aniž by si toho všimnul a to i za předpokladu, že dodrží oba předchozí body.
- **Používejte aktualizovaný operační systém.** V aktualizacích bývají opravené objevené bezpečnostní chyby, které jinak mohou být zneužity. Většina systémů umí, při správném nastavení, kontrolovat aktualizace sama.
- **Používejte antivirový program. Aktualizujte ho!** Existují kvalitní antivirové programy, které jsou pro domácí použití zdarma, případně si můžete zakoupit i komerční produkty. Pokud je počítač připojený k Internetu, dokáže si antivirový program (při správném nastavení) stáhnout aktualizaci sám. Neaktualizovaný antivir nemusí včas odhalit nové viry.
- **Používejte antispywarové programy, využívejte firewall.** Antispywarové programy dokáží odhalit další druhy škodlivého software. O jejich aktualizaci platí totéž, co v předchozích případech. Firewall chrání před nežádoucím přístupem zvenčí nebo může zabránit odchozímu spojení pochybných programů do Internetu.
- **Nespouštějte neznámé programy, které vám přijdou e-mailem, ani na které e-mail odkazuje!** Dodržujte nejvyšší opatrnost, přestože zpráva může vypadat, že je od vašich nejbližších přátel. Typickým příkladem z poslední doby jsou různé podvržené odkazy na elektronické pohlednice. Ve skutečnosti se nekalé živly snaží z odkazované stránky nainstalovat do počítače škodlivý program. Také programy, které se vám na různých stránkách snaží vnutit, mohou mnohdy škodit. Například kromě popisované funkčnosti mohou obsahovat i trojské koně, které pracují ve prospěch svých tvůrců.
- **K elektronickému bankovnictví nebo ke svým účtům (nejen bankovním) se nepřihlašujte z veřejně přístupných nebo nedůvěryhodných počítačů, které nemáte pod kontrolou.** Mohou být na nich nainstalovány různé programy pro monitorování činnosti a vaše důvěrné informace nebo přístupové kódy se mohou dostat k neoprávněným osobám. Toto se týká nejen počítačů v internetových kavárnách, ale také třeba i u známých, kde jsou instalovány programy z různých zdrojů a nemáte jistotu jejich zabezpečení.
- **Jestliže nemůžete mít pro svoji práci svůj počítač, který nesdílíte s ostatními členy rodiny, mějte každý svůj účet. Uživatelům nepřidělujte práva administrátora!** Získáte tím částečnou ochranu před nežádoucími úpravami systému.
- **Používejte svůj rozum a zdravý úsudek! Pamatujte, útočníci jsou vždy o krok napřed a stále zkoušejí nové triky, jak vás nachytat!** I přes veškeré technologické zabezpečení se může objevit jednoduchý trik, kterým se vás mohou snažit obelstít. Jestliže nebudete dodržovat základní bezpečnostní pravidla a nepřemýšlet nad svojí činností, můžete se stát další obětí.

4. SCAM 419

4.1.Co je to SCAM 419

SCAM 419 je označení pro druh podvodu u nás známého spíše jako **Nigerijské dopisy**. Tyto podvody nejsou žádnou novinkou, existovaly již dříve buď ve formě dopisu, nebo jako faxy. Rozvojem e-mailové komunikace se podvody masově rozšířily, ale princip zůstává stejný. Osloví vás neznámý člověk, že zdědil, získal nebo dokonce spravuje něčí majetek ve výši několika desítek miliónů dolarů a potřebuje pomoc při jeho převodu ze země. Za to je slíbená tučná odměna ve výši několika desítek procent z celkové částky. **Princip podvodu spočívá v tom, že oběť musí neustále platit nečekané administrativní poplatky a převod majetku se stále oddaluje.**

S rozvojem internetových a elektronických služeb vymýšlejí podvodníci stále nové triky, jak vylákat z neopatrných uživatelů peníze. **Někdy jsou to falešné nabídky neexistujícího zboží v internetových aukcích, podvodné inzeráty na prodej levného automobilu nebo pronájem bytů.** Podvodníci se **neštítí zneužívat různá neštěstí** nebo přírodní katastrofy k nachytání dalších obětí.

Některé podvody bývají v principu jednoduše provedeny, ale velmi často bývají propracovány i do drobných detailů, jako jsou profesionálně vytvořeny webové stránky neexistujících společností a bankovních institucí. Obětem bývají zasílány i podvržené falešné dokumenty a certifikáty. **K získání peněz a zametení stop slouží tzv. bílí koně** (nebo také mules, arrow). Ti vyberou peníze z účtu, kam je oběť pod různými záminkami poslala a převedou na jiný účet. Bílí koně **bývají nalákáni nabídkou na zajímavou a jednoduchou práci, která spočívá pouze v občasném převedení peněz**. Tyto nabídky opět většinou chodí jako nevyžádaná pošta. U bílých koní stopa většinou končí a jsou to právě oni, kdo pyká za podvod, jehož byli i nevědomky spolupachateli.

V případě, že se přesto někdo stane objetí trestného činu - pošle podvodníkům peníze, může samozřejmě podat trestní oznámení orgánům činným v trestním řízení (státní zastupitelství PČR) nejlépe v místě jeho bydliště. **Z dosavadních zkušeností lze konstatovat, že téměř neexistuje šance, aby poškozená osoba získala zpět své peníze.**

4.2.Jak se bránit?

Jak se chovat, když do schránky přijde pochybný e-mail?

- **Pokud má e-mail podezřelý předmět, neotevírejte jej.** Jestliže předmět zprávy láká na dech beroucí výhru 50 milionů v loterii nebo výhru v soutěži, které jste se nezúčastnili, jde v 99,99 % případech o podvod.
- **Pokud odesílatel e-mailu neláká na výhru, ale nabízí obrovské sumy za jednoduché úkoly nebo tvrdí, že vás miluje, ačkoliv jste jej nikdy neviděl/a, půjde nejspíš také o podvod.** Procento uživatelů, kteří naletí na tyto na první pohled očividné podvody, je stále příliš vysoké.
- **Pokud e-mail nedopatřením otevřete, neodpovídejte na něj.** Jen tím potvrdíte existenci své e-mailové adresy. Podvodník vás začne emocionálně vydírat a objem spamu ve vaší poštovní schránce se následně zaručeně znásobí.
- **Neklikejte na žádné odkazy ve zprávě.** Riskujete stažení škodlivého softwaru, který může krást citlivá data z vašeho počítače.

- **I důvěryhodně vypadající e-mail nemusí být pravý.** Většina nigerijských dopisů se prozradí špatnou češtinou a pravopisnými chybami. Avšak i bezchybný e-mail informující o velké výhře nebo nutnosti převodu peněz je více než podezřelý.
- **Pokud si nejste jisti, zda jde skutečně o podvodný e-mail a jak se chovat, pokud jste na něj již odpověděli, obraťte se na odborníky.** Známý je například server www.419hell.com, který shromažďuje tipy od obětí i bezpečnostních odborníků.

5. Malware

MALWARE je všeobecné označení pro škodlivý kód. Nejčastěji to může být počítačový vir, červ nebo stále častěji Trojský kůň. Dříve se podobná havěť šířila přímo e-mailem, ale v dnešní době se stále více využívá sociální inženýrství, kdy v textu e-mailu je pouze odkaz na tento škodlivý kód pod záminkou, že odkaz směřuje na zajímavý obrázek, video nebo e-pohlednici. Pokud neopatrný uživatel na odkaz klikne, stáhne si namísto slibovaných obrázků škodlivý kód.

Obranou je kromě dobrého antispamového filtru, kvalitního antivirového programu a včas aktualizovaného systému hlavně rozum. Tvůrci malware jsou vždy o krok před výrobci antivirů, kteří reagují na nové hrozby.

6. Netiketa

Netiketa je jakási pomyslná sbírka pravidel a zásad, která by se měla dodržovat v internetovém světě. Slovo netiketa je odvozeno z anglického net (= síť; častá zkratka pro internet) a slova etiketa.

Mnoho lidí si myslí, že při vstupu do internetového světa mají naprostou anonymitu. Což je velký omyl – téměř vždycky se dá pomocí různých metod internetový uživatel vystopovat. Většina uživatelů si to neuvědomuje, takže permanentně vstupuje do nebezpečí tím, že na chatech nebo diskuzích ostatní uživatele urážejí, vysmívají se jim nebo se o nich vyjadřují vulgárně. Z těchto konfliktů pak vznikají tzv. flame war, které mnohdy přerostou v osobní hackerské spory, ohrožující počítače všech účastníků.

Je třeba si uvědomit, že v internetovém světě bychom se měli chovat podobně jako ve světě reálném, tedy jako civilizovaní lidé. Za tím účelem existuje netiketa, pravidla slušného chování na Internetu.

Pravidla

1. Nezapomínejte, že na druhém konci jsou lidé a ne počítač. To, co napíšete do počítače, byste možná dotyčnému nikdy neřekli do očí.

2. Dodržujte obvyklá pravidla slušnosti normálního života. Co je nevhodné v obvyklém životě, je samozřejmě nevhodné i na internetu.
3. Zjistěte si taktně, s kým mluvíte. Internet je přístupný lidem z celého světa, a v každé zemi platí jiná morálka. Co je dovolené na americkém chatu, nemusí být dovolené na arabském, a to platí o všech podobných skupinách. Politika, náboženství a podobné problémy by proto měly být diskutovány s maximálním taktem a v mezích slušnosti.
4. Berte ohled na druhé. Ne každý má tak dobré internetové připojení jako vy. Někteří se připojují z domu přes vytáčené připojení a draze za to platí. Neposílejte proto zbytečně velké e-mailové zprávy a posíláte-li přílohy, komprimujte je. Při posílání velkých obrázků např. na diskusní server využívejte funkci náhledu obrázku.
5. Je vhodné psát s diakritikou. Vyvarujete se tak nedorozumění. Nekomolte rodnou řeč. Toto je obzvlášť důležité, protože se jinak dopustíte faux-pas. Pokud jste z nějakého důvodu nuceni psát bez diakritiky, snažte se používat správný pravopis. Nebuďte grobián, nezveřejňujte nepravdivé, nebo i pravdivé, ale choulostivé informace.
6. Pomáhejte v diskuzích. Pokud má někdo v diskuzi nějaký problém, odpovězte mu, pokud znáte odpověď. Někdo jiný zase pomůže vám. Platí zásada: „Napřed poslouchej, pak piš.“
7. Respektujte soukromí jiných. Pokud vám omylem přišla zpráva, která vám nepatří, je vhodné ji smazat a taktně upozornit odesilatele na jeho chybu.
8. Nezneužívejte svou moc či své vědomosti. Pokud jste správce serveru, máte sice přístup k poště ostatních, ale nemusíte ji neustále kontrolovat jenom tak z nudy, a pokud umíte hackovat, nemusíte to pořád zkoušet.
9. Odpouštějte ostatním chyby. I vy je děláte. Nevysmívejte se jim a nenadávejte za ně.
10. Nešiřte hoaxy. Zahlcují internet. Pokud vám přijde hoax, zdvořile upozorněte jeho odesilatele, že takové jednání je nevhodné.
11. Nerozesílejte spam a reklamu.
12. Neporušujte autorská práva.