Elektronická pošta – e-mail (7. třída)

Počítačové viry v mikroskopu

Stažení škodlivého software do počítače – Malware

Malvare dělíme:

- *Počítačové viry a červy*

Jako virus se označuje program, který se dokáže sám šířit bez vědomí uživatele. Pro množení se vkládá do jiných spustitelných souborů či dokumentů. Tyto soubory se nalézají v příloze e-mailu a pro aktivaci viru je třeba tuto přílohu otevřít. Počítačový červ je modernější a ke svému šíření již soubory či dokumenty nepotřebuje. K aktivaci počítačového červa stačí pouhé přečtení zprávy anebo kliknutí na odkaz v textu zprávy – ten vás přesměruje na webovou stránku, kde na vás už počítačový červ čeká.

- *Trojské koně*

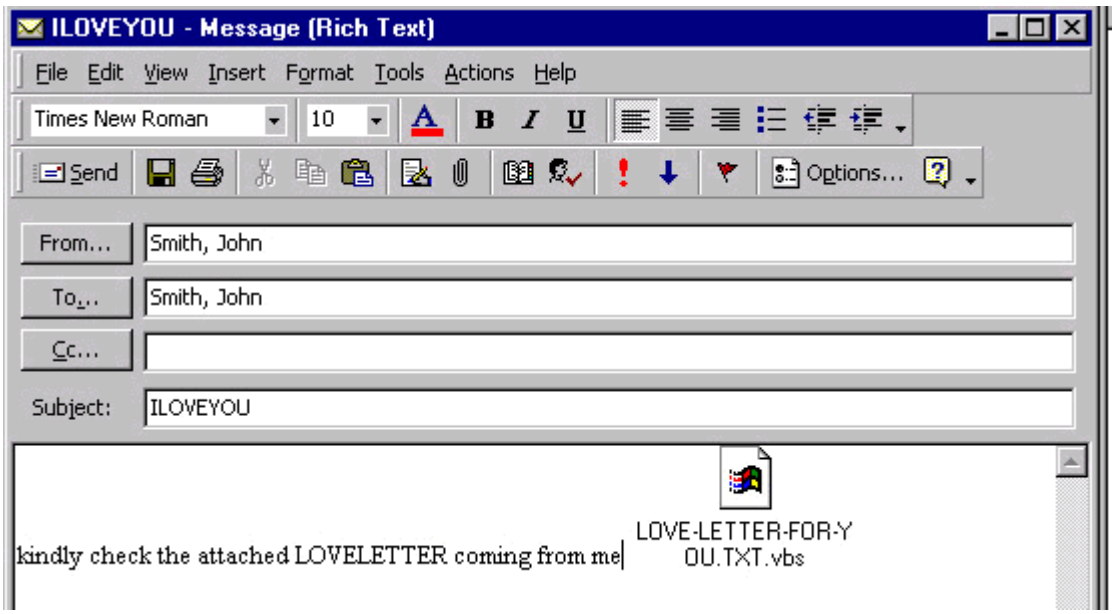
Trojský kůň je uživateli skrytá část programu s funkcí, se kterou uživatel nesouhlasí (typicky je to činnost škodlivá). Často bývá skrytý v souborech, které si stahujete z Internetu z neověřených zdrojů – nelegální kopie her, cracky – jak craknout neoriginální hru….

- *Spyware*

Spyware je program, který využívá internetu k odesílání informací z počítače bez vědomí jeho uživatele. Těmito informacemi mohou být fotografie, čísla platebních karet, přihlašovací údaje…

- *Adware*

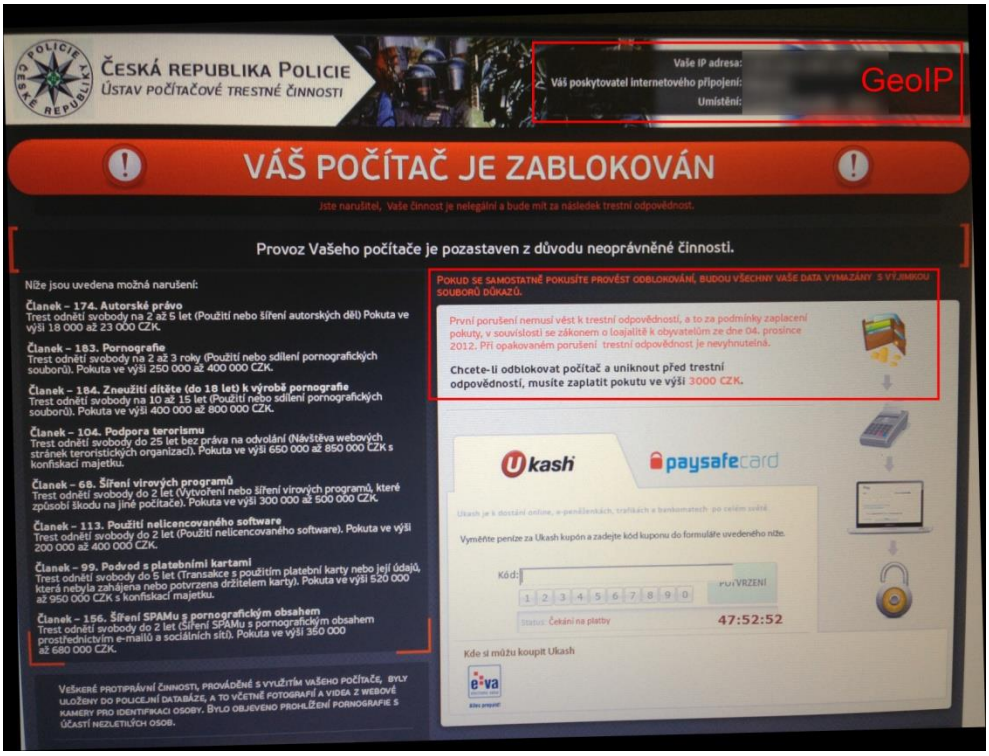
Adware je označení pro produkty znepříjemňující práci s nějakou reklamou. Ta může mít různou úroveň agresivity - od běžných bannerů až po neustále vyskakující pop-up okna nebo ikony v oznamovací oblasti. Další nepříjemnou věcí je např. změna domovské stránky ve Windows Internet Exploreru, aniž by o to uživatel měl zájem.



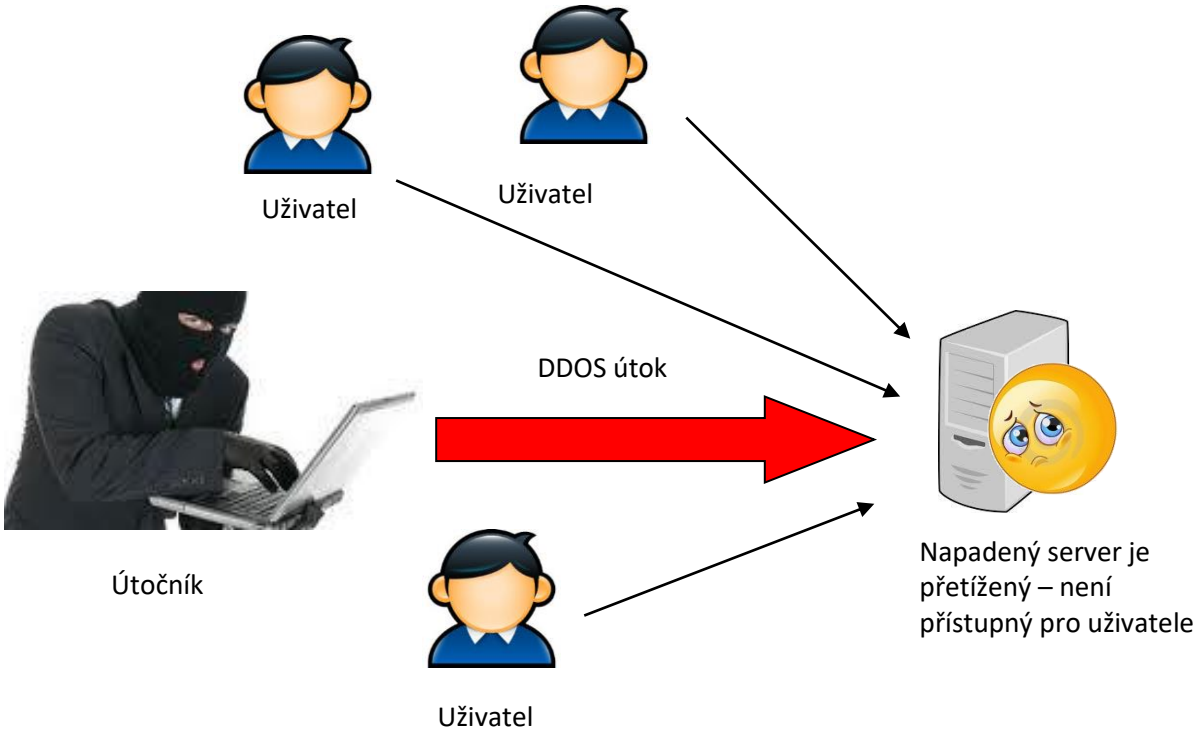
Na obrázku je e-mail, který v přiloženém souboru skrývá nejničivější virus všech dob – virus **I love you.** Virus způsobil škodu za 5 bilionů $ a infikoval asi 10 % všech počítačů připojených na Internet.

Jak může malware přinést prospěch svému tvůrci?

- Zablokování počítače a následné vyžadování poplatku za jeho odblokování.



- DDOS útoky – zablokování vybrané webové stránky tím, že se na ní v jednom okamžiku přihlásí velké množství počítačů napadených malware a následné vydírání majitele webové stránky (buď zaplatíš anebo budeš mít webovou stránku nefunkční).



- Umístí na váš počítač webové stránky, které nabízí prodej drog, dětské pornografie….
- Umístí na váš počítač poštovní schránku, ze které rozesílá nevyžádanou poštu - spam
- Spyware – odesílá z vašeho počítače informace
- Mining – těžba kryptoměn na vašem počítači

Jak poznám, že mám v počítači malware?

- **provedu kontrolu počítače antivirovým programem**
- výrazně se zpomalí práce celého počítače
- start počítače trvá o poznání déle
- operační systém je nestabilní (“zasekává se“)
- při práci s Internetem vyskakují okna s reklamou (pop-up okna)
- v oznamovací oblasti se objeví ikony, které vás neustále obtěžují (reklamou)
- změní se domovská stránka Windows Internet Exploreru (a nejde nastavit vlastní)

Tyto příznaky **mohou (ale nemusí)** znamenat, že máte v počítači Malware.

Jak si ochráním počítač před malware?

- v počítači musí být nainstalován komplexní antivirový balík
- operační systém musí mít nainstalované všechny aktualizace
- ostatní software musí mít nainstalované také všechny aktualizace
- v počítači musí být funkční brána Firewall
- veškery stažený software před instalací zkontroluji na přítomnost malware
- před použitím zkontroluji všechny externí paměťová zařízení (flashdisky)
- podezřelé e-maily patří do koše – nestahuji z nich přílohu a neklikám na odkazy
- nešířím spam
- používám pouze legální software z prověřených zdrojů
- pravidelně provádím údržbu počítače

Morrisův červ byl jeden z prvních počítačových červů, který ke svému šíření využíval Internet. Byl vytvořen tehdy 23letým studentem R. T. Morrisem. K jeho vypuštění došlo 2. listopadu 1988. Červ napadl asi 10 % tehdejších počítačů, výrazně zpomalil jejich činnost a způsobil tak škody ve výši až 10 mil. dolarů. Autor byl odsouzen k tříletému podmíněnému trestu, 400 hodinám veřejně prospěšných prací a pokutě ve výši 10 000 amerických dolarů

Virus I love you byl dosud nejničivějším virem všech dob. Způsobil škodu za 5 bilionů $ a infikoval asi 10 % všech počítačů připojených na Internet. Virus po aktivaci vyhledával v počítači čísla a hesla kreditních karet a zasílal je e-mailem zpět útočníkovi. Následně poškodil operační systém napadeného počítače a vyřadil ho tak z provozu. Vypuštěn byl 4. května 2000. Jeho autorem byli sourozenci Onel de Guzman, Irene de Guzman a její přítel Reomel Lamores z Filipín. Nikdy nebyli odsouzeni.

Rozesílání nevyžádané pošty - spam

Nevyžádaná pošta tvoří většinu e-mailů, které míří do vaší schránky (přes 90 %). Jako spam označujeme většinou zprávu, která obsahuje nevyžádanou, nechtěnou reklamu. Většinu spamu do vaší poštovní schránky zachytí filtry, které blokují nevyžádanou poštu. Spam zbytečně zatěžuje Internet a uživatele obtěžuje reklamou.

Jak může spam přinést prospěch svému tvůrci?

- Spam obsahuje reklamu, za šíření reklamy zadavatel reklamy zaplatí (například 0,1 Kč za jeden e-mail, ale e-mailů s reklamou mohou být miliony….).
- Spam může být zdrojem malware.

ekm.mrkaceknn@pru…	Nebankovni uver do vyse 10 000 Kc za 15 minut. » Dobry den, Schazi Vam penize pred vyplatou? Zkuste online pujcku do vyse…
gerardo.juarez@reju…	Be number 1 in her heart » Do you wish to impress your woman this night? http://disloyal.qwswcdqq.eu/
vreisen@acagents.c…	Time for perfect satisfaction in bed » Make your gf happy http://acrobatic.ypjdeqss.eu/
dx1all@computervar.it	Get rid of your problems in bed » http://interval.zmmlwzae.eu/ The only way to regain your intimate life
mark@chlngr.com	Jealous RightEDmed » http://nurtriko.net/essential.php?vetoceq

Jak si ochráním počítač před spamem?

- v počítači musí být nainstalován komplexní antivirový balík
- nevyžádanou poštu označím jako spam (a bude doručována do složky spam)
- nešířím spam
- zvážím, komu poskytnu svůj e-mail (čím více ho používáte, tím více spamu dostáváte)

Název spam pochází ze značky amerických konzerv lančmítu. Slovo vzniklo jako zkratka ze slov spiced ham - okořeněná šunka a tyto konzervy se vyrábí od 30. let 20. století dodnes. V současnosti ale výrobce trvá na psaní velkým písmem - SPAM. V období 2. světové války byla hojně rozšířená a stále méně oblíbená ve Velké Británii.

Hoax (anglické slovo hoax označuje podvod, mystifikaci či žert) je nevyžádaná e-mailová zpráva, která uživatele varuje před nějakým virem, prosí o pomoc, informuje o nebezpečí, snaží se ho pobavit apod. Hoax většinou obsahuje i výzvu žádající další rozeslání hoaxu mezi přátele, příp. na co největší množství dalších adres, proto se někdy označuje také jako řetězový e-mail.

Hoaxy nabývají několika typických forem:

- Falešný poplach – původní význam slova hoax. Zpráva manipuluje s informacemi a snaží se uživatele přimět hlavně k dalšímu šíření (Ve školní jídelně se množí případy úplavice. Vedení školy se to snaží zatajit. Ve vlastním zájmu nechoďte na obědy. Rozešli tuto zprávu všem spolužákům!)
- Zábavné – dříve se řetězové dopisy šířily jen klasickou poštou, dnes se přesunuly na internet. Tyto využívají uživatelovy touhy být vtipný nebo jeho pověrčivosti a vyhrožují (Nepřepošleš-li, budeš mít smůlu.). Naopak poslušnému uživateli slibují všechno možné.
- Prosby – hoax většinou působí na city a prosí příjemce o darování krve, hledání ztracené osoby, případně přímo vylákává peníze. Některé z těchto zpráv původně opravdu rozeslali lidé ve svízelné životní situaci, ale hoaxy často přežívají mnohem déle, než měl autor v úmyslu.

Čím škodí:

- Opakovaný příjem nesmyslných zpráv je pro mnohé uživatele nepříjemný.
- Některé hoaxy poskytují nebezpečné rady, např. jak se zbavit domnělého viru smazáním nějakého souboru. Uživatel, který takové rady slepě následuje, může svému počítači naopak ublížit.
- Uživatel v dobrém úmyslu pošle peníze, ty však skončí na účtu podvodníka.

Ochrana před Hoaxy:

- Pokud dostaneme takovýto e-mail, je dobré kontaktovat odesílatele, a pokusit se ho poučit o zbytečnosti a nezřídka kdy také o škodlivosti jeho počínání.
- Zastavím šíření hoaxů, nepřeposílám je dále.
- Při brouzdání po Internetu, chatování a používání Facebooku přemýšlejte. Zjistěte si z více zdrojů, zda se jedná o skutečnou zprávu a hlavně, nepodlehněte nátlaku s prosbou o co největší rozeslání mezi ostatní přátele.
- Více informací naleznete na: https://www.hoax.cz/
- Podívejte se na: https://www.youtube.com/watch?v=SPKMBL-BOk0

Slovem ***Phishing*** označujeme podvodné e-mailové útoky na uživatele Internetu, jejichž cílem je vylákat důvěrné informace.

Nejčastěji jsou to údaje k platebním kartám včetně PINu nebo různé přihlašovací údaje k účtům.

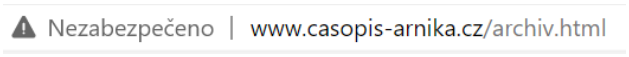
Základní znaky phishingového e-mailu:

- Snaží se vyvolat dojem, že byl odeslán organizací, z jejichž 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, informace o nedoručení zásilky (například DPD), informace o nutnosti zaplacení celního poplatku.

- V textu zprávy je odkaz, 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.

Jak poznáme 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.
- Ve většině případů komunikace probíhá po běžném, nezabezpečeném připojení:
  Nezabezpečený protokol: http://

- Komunikace s bankou musí probíhat po zabezpečeném připojení:
  Zabezpečený protokol https://

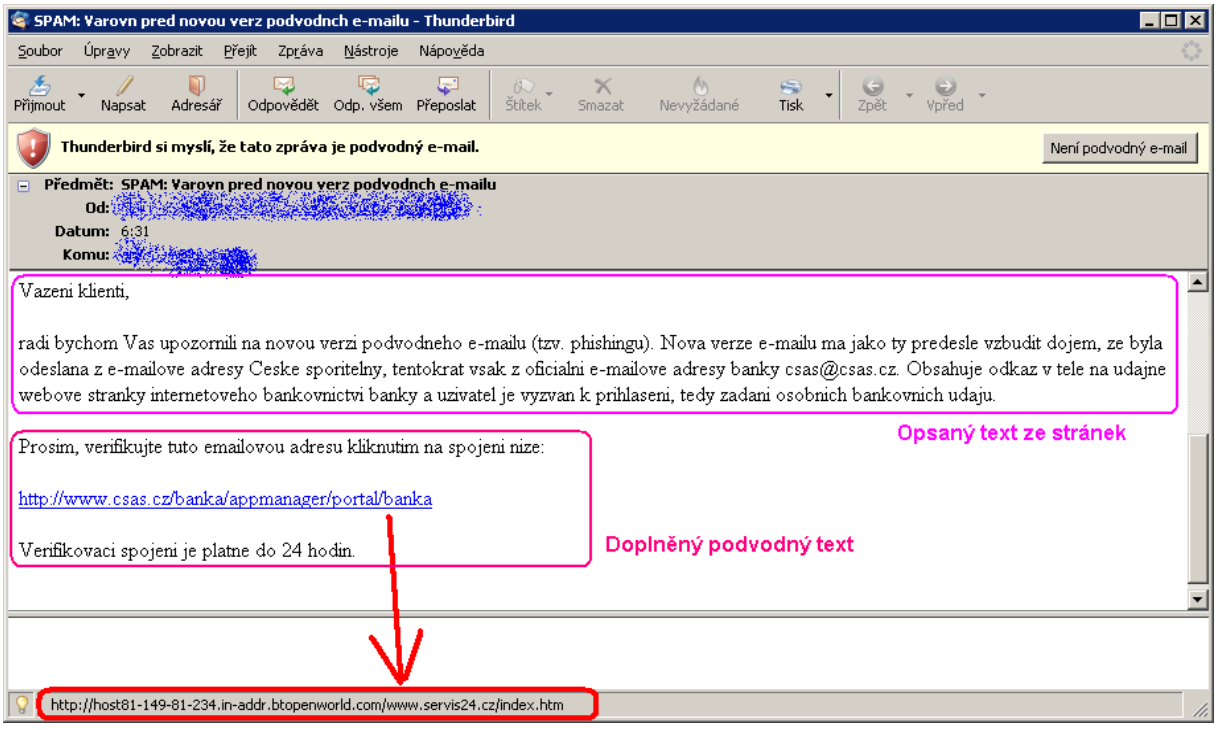
  

- Kliknutím na se musí zobrazit **platný certifikát**

Jak se bránit:

- Jestliže vám chodí jménem banky e-maily, které obsahují 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! Zprávu vymažte.
- Používejte komplexní antivirový balíček, ten většinou dovede Phishing odhalit.
- Podívejte se na: https://www.youtube.com/watch?v=iDCdJ8FUakY

Příklad: Phishing, který se tváří jako varování před phishingem.



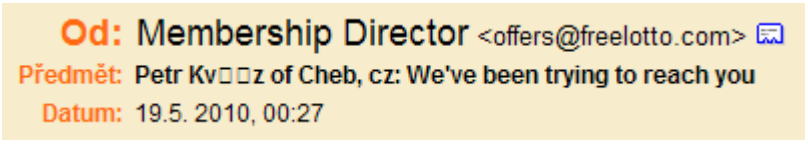
Podvodné loterie

Uživatelům jsou rozeslány e-maily, s oznámením vysoké výhry v nějaké mezinárodní loterii. Do údajného slosování se oslovení uživatelé dostali například výběrem e-mailových adres z celého světa a právě ta jejich vyhrála.

Čím škodí:

- Když se šťastlivec o svoji výhru přihlásí, dozví se kromě gratulace, že musí před vyplacením výhry **zaplatit manipulační poplatek** několika desítek až tisíce EUR. Tento poplatek samozřejmě není možné strhnout z vyplácené výhry. Někdy po zaplacení prvního poplatku jsou požadovány další, mnohem větší částky.
- V krajním případě jsou **požadovány od "výherce" důvěrné informace** nebo přístupové údaje k účtům například pod záminkou problému s převodem slibované výhry. Takto získané informace mohou podvodníci dále snadno zneužít.

Příklad: Chceme tě obohatit - Petr Kvíz z Chebu získal v loterii 11 260 000 $



Proč podvodníci oslovili právě Vás?

Nevytipovali si Vás jako osobu, pouze se jim do seznamu dostala Vaše e-mailová adresa a tak nyní máte smůlu. Pravděpodobně i v budoucnu Vás budou bombardovat dalšími podvody a jiným spamem.

Jakým způsobem mám na podvodné e-maily reagovat?

- Nejjednodušší a snad nejsprávnější je tyto e-maily rovnou vymazat.
- Podívejte se na: https://www.youtube.com/watch?v=74iJHk69lhs

Nigerijské dopisy

Po celém světě jsou na náhodné adresy rozeslány prosby o pomoc s převodem obrovské částky peněz nebo jiného velkého množství cenin - většinou z Nigerie (odtud název).

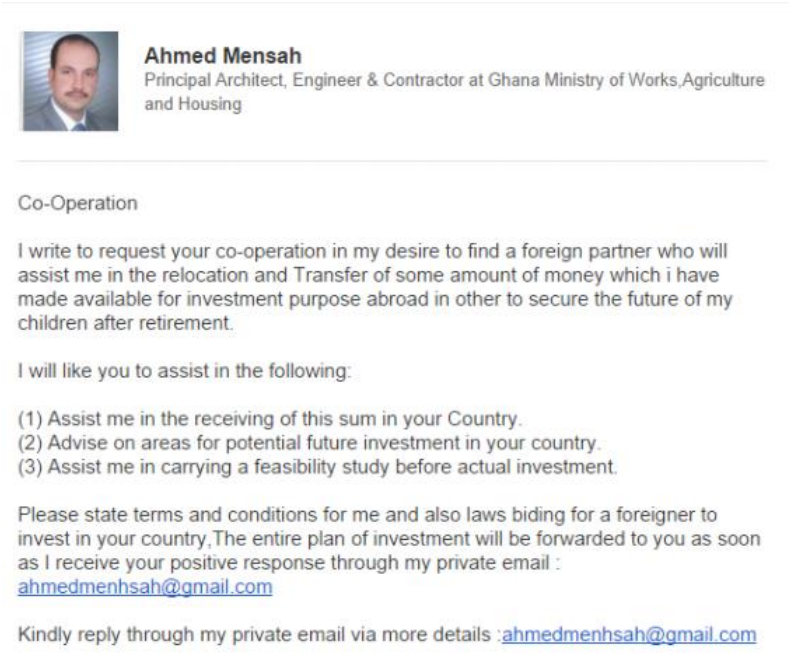
Údajným odesílatelem bývá například vdova po bohatém podnikateli nebo vysokém státním úředníkovi. Někdy například i bankovní úředník, který údajně objevil vysoké bankovní konto po milionářovi, který před několika lety zemřel a nemá žádné příbuzné. Všichni tito podvržení autoři důvěrně prosí o pomoc při vývozu tohoto majetku. Za odměnu je slibována několika procentní odměna, která by však měla činit až několik miliónů dolarů!

Pokud se někdo nachytá a s podvodníky se kontaktuje, bývají jim předloženy různé falešné doklady a nechybí ani odkazy na podvržené stránky finančních institucí, kde si naivní důvěřivec může zkontrolovat vymyšlené informace.

Čím škodí:

- Princip podvodu spočívá v tom, že z **oběti jsou lákány peníze na nečekané nepředvídané údaje**, úplatky úředníku a podobně. Pod vidinou velké odměny je oběť ochotna platit.
- Výjimkou nejsou ani **internetové seznamovací inzeráty**, pomocí kterých si podvodníci hledají své oběti. Poté co získají jejich důvěru, požadují pro nastávajícího ženicha nebo nevěstu například zaplacení letenky, léků, domu (kde budou spolu šťastně bydlet…)
- https://www.seznamzpravy.cz/clanek/ja-tebja-ljublju-jak-ruske-krasky-lovi-ceske-zenichy-a-obiraji-je-o-penize-142435?autoplay=1

Příklad:



Ahmed Mensah
Principal Architect, Engineer & Contractor at Ghana Ministry of Works,Agriculture and Housing

Co-Operation

I write to request your co-operation in my desire to find a foreign partner who will assist me in the relocation and Transfer of some amount of money which i have made available for investment purpose abroad in other to secure the future of my children after retirement.

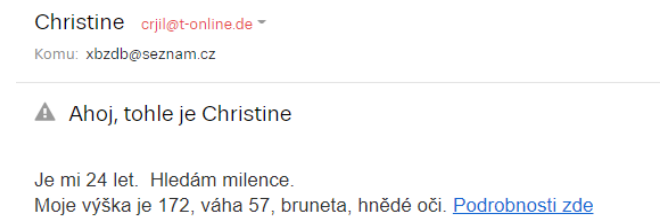
I will like you to assist in the following:

(1) Assist me in the receiving of this sum in your Country.
(2) Advise on areas for potential future investment in your country.
(3) Assist me in carrying a feasibility study before actual investment.

Please state terms and conditions for me and also laws biding for a foreigner to invest in your country,The entire plan of investment will be forwarded to you as soon as I receive your positive response through my private email :
ahmedmenhsah@gmail.com

Kindly reply through my private email via more details :ahmedmenhsah@gmail.com

Příklad:



Christine crjil@t-online.de
Komu: xbzdb@seznam.cz

Ahoj, tohle je Christine

Je mi 24 let. Hledám milence.
Moje výška je 172, váha 57, bruneta, hnědé oči. Podrobnosti zde

Falešné vydírání

Autor podvodného vyděračského e-mailu se vydává za hackera, kterému se údajně **podařilo nahrát do počítače škodlivý program a zneužít webkameru**.

V některých případech bývá i v textu e-mailu heslo, které uživatelé opravdu používali na některých webových službách v kombinaci s e-mailovou adresou. Je možné, že pachatelé získali údaje buď předcházejícím phishingovým útokem nebo využili nějakou databázi získaných hesel. Ta se dá také jako placená služba získat.

Tím, že je v podvodném e-mailu uvedené skutečně používané heslo, je příjemce zprávy více motivován k platbě.

Čím škodí:

Nabízí příjemci e-mailu, že záznamy nezveřejnění, pokud nedostane požadovanou částku (tentokrát "pouhých" 1000 USD) v bitcoinech.

Příklad:

Ahoj!

Mám pro tebe velice špatné zprávy.

03/08/2018 - v tento den jsem napadl váš operacní systém a získal vám plný prístup k vašemu úctu.

Pred mesícem jsem chtel uzamknout zarízení a požádat o to, aby se BTC odblokovalo.

Ale podívala jsem se na místa, která pravidelne navštevujete, a já jsem byl šokován tím, co jsem videl !!!

Udelal jsem screenshot z webových stránek pro dospelé, kde se bavíte (chápete, o co jde, jo?).

Poté jsem provedl screenshot svých radostí (pomocí fotoaparátu vašeho prístroje) a prilepil je.

Ukázalo se to úžasné! Jste tak velkolepý! Vím, že byste nechteli zobrazovat tyto screenshoty svým prátelum,

príbuzní nebo kolegové. Myslím, že 1000 dolaru je velmi, velmi malá cástka pro mé mlcení. Krome toho vás na vás špehuji

tak dlouho, protože strávil spoustu casu! Platit pouze v Bitcoins! Moje penaženka BTC: 1CpsNMwbkk1XGxFQoPX9npzKXjXYiee8gp

Máte-li potíže s tímto - Zeptejte se spolecnosti Google "jak uskutecnit platbu na peneženku peneženky". Je to snadné.

Po obdržení výše uvedené cástky budou všechna data automaticky odstranena.

Muj virus se také znicí z vašeho operacního systému.

Jak se bránit?

- Uživatelé by si rozhodně měli změnit svá hesla a dodržovat pravidlo, že pro každý účet nebo službu by měli mít různé heslo.
- Vyděračský e-mail patří rovnou do koše. Jakákoliv platba podpoří podvodníky v jejich další činnosti.

Falešné internetové obchody

Falešné internetové obchody většinou nabízí zboží za neuvěřitelně nízké ceny. Zákazník si zboží objedná a zaplatí. Bohužel se zakoupeného zboží nikdy nedočká.

Tady je rada jednoduchá – **nakupujte pouze u prověřených** (doporučených, vyzkoušených) obchodů, a pokud si nejste jistí, nikdy neplaťte za objednané zboží předem.

Příklad: Pokud vám z internetového obchodu přijde podobný e-mail, vězte, že jde o snahu vylákat z vás peníze předem a objednané zboží samozřejmě nedodat.

„Dobrý den, děkujeme za Vaši objednávku. Vaše objednané zboží je skladem a připraveno k okamžité distribuci. Bohužel se jedná o poslední kus za tuto akční cenu a díky situaci na trhu kdy si lidé nevyzvedávají naše dobírky na poště, jedná se o 40 procent za poslední měsíc, jsme nuceni změnit způsob platby na bankovní převod v rámci zachování příznivých cen. Děkuji za pochopení a po úhradě prosím o informaci a zboží bude doručeno do 24 hodin. Jako bonus a satisfakci Vám nabízíme slevu na uvedený výrobek ve výši 5 %, o kterou jsme ponížili vystavenou fakturu. Děkujeme za pochopení a hezký den, Petr Březina, prodejce.“

1) co označuje termín malware
2) jak se od sebe odlišuje počítačový virus a počítačový červ
3) jakým způsobem prostřednictvím e-mailu mohu aktivovat počítačový virus
4) jakým způsobem prostřednictvím e-mailu mohu aktivovat počítačového červa
5) popište činnost Trojského koně
6) vysvětlete termín spyware
7) jakým způsobem se v počítači může projevit adware
8) jakým způsobem může malware přinést prospěch svému tvůrci
9) popište DDOS útok
10) jak poznám, že mám v počítači malware
11) jak může DDOS útok přinést prospěch svému tvůrci
12) jak zabezpečíte svůj počítač před DDOS útokem
13) zda mi zajistí komplexní antivirový balík 100% ochranu před malware
14) jak zajistím 100 % ochranu počítače před malware
15) jaká je hlavní nevýhoda antivirového programu Windows Defender
16) jakým způsobem škodí falešný antivirový program
17) proč jsou nutné aktualizace operačního systému Windows
18) co je to řetězový e-mail
19) jakým způsobem škodil nejničivější virus všech dob
20) co označuje termín spam
21) jakým způsobem může spam přinést prospěch svému tvůrci
22) jak poznám spam
23) jak se mohu před spamem bránit
24) co označuje termín hoax
25) jaký je typický znak hoaxu
26) jakým způsobem může mě hoax škodit
27) zkuste napsat vlastní hoax
28) jak se bránit před hoaxem
29) co označuje termín phishing
30) jak poznáme podvodné stránky
31) jak se od sebe liší zabezpečený a nezabezpečený protokol, podle kterého probíhá komunikace na Internetu
32) jakým způsobem může phishing přinést prospěch svému tvůrci

33) jakým způsobem může podvodná loterie přinést prospěch svému tvůrci
34) co to jsou takzvané žluté linky
35) co označujeme termínem Nigerijské dopisy
36) jakým způsobem mohou Nigerijské dopisy přinést prospěch svému tvůrci
37) jak může autor Nigerijského dopisu mít zisk z falešného seznamovacího inzerátu
38) jakým způsobem správně nakupovat zboží a služby na Internetu