Zde si můžete stáhnout poslední verzi tohoto článku.

Bezpečnost v digitálním věku

Ing. Boleslav Vraný
www.bolekvrany.cz
13. května 2004

Vysázeno v systému LaTeX

Obsah

Kapitola 1

Status

Tento dokument vznikl na žádost kamaráda sepsat naše rozhovory pro širší okruh čtenářů. Jde o soukromý pohled jednoho poněkud poučenějšího uživatele PC na tuto oblast a je určen pro mírné poučení uživatelů méně poučených. Tento dokument si v žádném případě nedělá nárok na obsahovou správnost nebo úplnost; jak již bylo řečeno, je to jen soukromý pohled na věc, který však některé lidi zajímal a možná bude někomu ku prospěchu. Co zde uvádím, odpovídá mým znalostem ke dni vydání tohoto dokumentu, 13. května 2004.

Rád bych ještě upozornil na to, že vzhledem k obrovské různorodosti hardwaru, instalovaných operačních systémů a programů atd., navíc ještě doplněné o činnost virů, hackerů atd. nelze zcela předvídat, co se stane, ani když použijete tu nejneškodnější radu z tohoto textu. Např. se může stát, že po instalaci některých bezpečnostních záplat přestanou některé programy fungovat. Neodbornými zásahy do přístupových práv nebo neodborně provedeným odvirováním si můžete zcela zneprovoznit počítač atd. Proto platí: Máte-li správce počítače, obraťte se na něj s žádostí o aplikaci těchto rad. Nemáte-li správce, pak než něco uděláte, zálohujte, zejména data. Ta jsou to nejcennější, co máte. Nejste-li si jisti, obraťte se na odborníky. Peníze zaplacené za zvýšení bezpečnosti Vašeho počítače jsou rozhodně dobře investované.

Ze shora uvedných důvodů se já sám se výslovně zříkám odpovědnosti za všechny škody, které by Vám mohly aplikací rad popsaných v tomto textu vzniknout, ať už přímo nebo nepřímo. Vše děláte na vlastní riziko.

Je také třeba upozornit na fakt, že dokument se zabývá technickými možnostmi ochrany. Některé tyto možnosti (např. šifrování) však mohou být v některých zemích nelegální a zakázané zákonem. Před jejich použitím si tedy ověřte jejich legálnost ve vaší zemi. Opět se výslovně zříkám jakékoliv odpovědnosti za vše, co Vám způsobí použití těchto technických prostředků v rozporu se zákonem.

Dokument můžete libovolně šířit tak dlouho, dokud ho budete šířit celý a v nezměněné podobě. Šíření změněných dokumentů je výslovně zakázáno.

Kapitola 2

Psychologické útoky

Jedním z technicky nejsnadnějších a přitom velmi účinných útoků je útok psychologický. Spočívá v tom, že jste pod vhodnou záminkou vyzváni k zadání citlivých údajů nebo účasti v různých zajímavých transakcích.

2.1 Vylákání údajů

Příkladem, který vás může stát desítky tisíc korun, může být např. takzvaný **fishing**. Spočívá v tom, že dostanete e-mailem dotazník, který vás nabádá k vyplnění čísla platební karty, pinu, doby platnosti a dalších údajů, údajně proto, že odesílatel (tvářící se jako např. společnost VISA) je potřebuje k vyřešení nějakého problému s vaší platební kartou. Poté, co tyto údaje v dobré víře odešlete, mohou být zneužity skutečným autorem mailu k vašemu okradení. Podobně vypadá i celá řada dalších dopisů, které se např. tváří, jako že jsou od administrátora vaší lokální sítě, a vyzývají k zaslání vašeho hesla, protože potřebuje cosi vyřešit s vaším (síťovým) účtem. K tomu lze říci jen to: Jsou to všechno podvody. **Banka samozřejmě číslo vaší platební karty zná, zná i její dobu platnosti a vše další. PIN banka NIKDY znát nepotřebuje. Podobně administrátor sítě sice vaše heslo nezná a obvykle nemůže zjistit, ale obvykle může manipulovat s vašimi nastaveními a daty a vůbec vším, co se týká vašeho síťového účtu, bez jeho znalosti.** Proto pokud vám takový mail přijde, ignorujte ho. Bez vyjímek.

Mnoho virů se dnes šíří tak, že vám přijde mail s přílohou, kterou musíte vy sami ručně spustit. Teprve poté, co toto uděláte, bude váš počítač zavirován. Vrcholem tohoto přístupu je virus, který se šíří v zaheslované příloze, takže pronikne sebelepším antivirem, a v textu zprávy je uvedeno něco jako „Otevřete přílohu a pro její rozbalení zadejte heslo XYZ“. Jakkoliv se to může zdát neuvěřitelné, tento virus se skutečně šíří a to pouze a jenom díky tomu, že uživatelé, kterým přijde, si neuvědomí, že zpráva je podezřelá. Podobně existuje virus, který se šíří jako příloha mailu, který se tváří jako upozornění poslané Microsoftem a obsahující poslední bezpečnostní záplaty. I tento virus si pravděpodobně musíte sami ručně spustit a sami ručně nainstalovat v dobré víře, že jde o skutečné bezpečnostní záplaty.

Zde je třeba si uvědomit jednu věc: zfalšovat odesilatele e-mailu vůbec není problém. Proto to, že v kolonce odesilatel je napsán váš známý nebo společnosti jako VISA nebo

Microsoft neznamená, že tito jsou skuteční odesilatelé. Jak už bylo řečeno, správce sítě nebo VISA nepotřebuje, abyste zadávali své heslo nebo pin do jakéhosi formuláře, mohou veškeré opravy dělat bez jeho znalosti. Podobně Microsoft ani žádná jiná solidní společnost nerozesílá lidem záplaty ani jakékoliv jiné upgrady mailem sama od sebe. Je možné, že dostanete mail skutečně od Microsoftu a skutečně obsahující bezpečnostní záplaty - ale to jen a pouze tehdy, pokud jste se zaregistrovali do příslušných mailing listů apod. Pokud jste nikdy nic takového nedělali, **veškeré takové maily mažte, protože jsou to bez vyjímky viry. Skutečné slušné společnosti neposílají nevyžádané maily milionům uživatelů, ale jen těm, kteří se výslovně zaregistrovali a vyjádřili své přání takové maily dostávat.**

Dostanete-li mail známého, je také dobré si ho před spuštěním příloh prohlédnout. Většina vašich známých asi budou Češi. Myslíte, že vám budou psát dopisy anglicky? (Naprostá většina zavirovaných mailů je anglicky.) Podobně vám asi nebudou naprosto cizí lidé s česky znějícími jmény psát anglické maily s textem jako „See my photos“ („Podívej se na moje fotky“). Současné mailové viry postupují tak, že z napadeného počítače rozesílají stovky a tisíce mailů se svými kopiemi. Přitom jako adresu odesilatele obvykle použijí buď adresu toho, z jehož počítače se rozesílají, a nebo náhodně vybranou adresu z jeho adresáře. Tedy pokud vám přijde mail, který je jakkoliv podezřelý, je lépe ho neotevírat a odesilatele se zeptat, zda ho skutečně odeslal on a zda vám skutečně dnes ráno posílal fotky ze včerejší párty, jak se píše v mailu.¡br¿

2.2 Nigerijské dopisy

Dalším značně rozšířeným příkladem jsou takzvané nigerijské dopisy. Jejich struktura je v podstatě následující:

> Vážená paní, vážený pane,
>
> jsem pracovníkem banky v ... . Před 20 lety si u nás americký občan John Smith uložil 20.000.000 USD (dvacet milionů dolarů). Pokud by si tyto peníze nevybral do 31.12. tohoto roku, vklad propadne naší zkorumpované vládě. Proto jsme hledali jeho nebo jeho příbuzné, ale ani on, ani jeho přímí příbuzní již nežijí. Nalezli jsme pouze jeho nejlepšího přítele, který však nemá nárok na dědictví. Protože nechceme, aby tyto peníze propadly naší vládě, rozhodli jsme se je tajnou operací převést tomuto jeho příteli. Bohužel k tomu potřebujeme nějaký účet mimo naši banku, který k transakci použijeme. Dovolujeme si proto s důvěrou obrátit na Vás a požádat Vás, zda byste nám neposkytl(a) svůj účet. Za tuto laskavost dostanete provizi ve výši 10% z převedené částky, tedy 2.000.000 USD (dva miliony dolarů). Máte-li zájem .....

Tyto dopisy jsou samozřejmě podrvh. Není příliš pravděpodobné, že někdo, kdo by vážně chtěl převádět 20 milionů USD z Nigérie, by se skutečně obrátil zrovna na vás. Pokud tedy váš otec není velmi dobrým známým šéfa nigerijské národní banky, o čemž pochybuji. Pokud na tento dopis naletíte, mohou následovat v podstatě tři scénáře. První spočívá v tom, že budete vyzváni, abyste poslali pár (desítek či stovek) tisíc na

dořešení nějakých drobných detailů celé transakce. Samozřejmě že poté, co je pošlete, celá transakce skončí a žádných 20milionů Vám nepřijde. Druhý scénář spočívá v tom, že Vám bude napsáno, že je třeba dojednat nějaké detaily a kvůli tomu musíte do Nigérie. Poté, co tam odletíte (je možné, že peníze na cestu tam dostanete od podvodníků), budete víceméně uneseni a budete se muset ze svého zajetí vykoupit tím, že na účet těchto podvodníků převedete nemalou částku. Teprve poté budete propuštěni a budete se moci za své peníze vrátit domů, chudší o pár set tisíc. Třetí možností je, že váš účet bude zneužit k nelegálním transakcím jako je praní špinavých peněz.

Mimochodem proč se těmto dopisům říká nigerijské - jednak první takové dopisy, ještě v dobách, kdy nebyl internet, chodily v papírové podobě právě z Nigérie. A jednak proto, protože jako země, v níž si dotyčný pán uložil své dolary, typicky vystupuje Nigérie, případně je tam nějak jinak zmíněna. Není to nutné, ale je to velmi časté.

2.3 Hoaxy

Na internetu se šíří celá řada planých poplachů (**hoaxů**). Krásnou ukázkou je zpráva, která mi chodí pravidelně cca každých půl roku, a která tvrdí, že nějaká holčička nutně potřebuje asi 100.000USD na operaci rakoviny. A její otec, který nemá peníze, sháněl sponzory. Sehnal firmy AOL a Netscape, které se zavázaly, že za každý mail s touto zprávou, který pošlete svým přátelům, zaplatí na příslušné konto 1 cent. Tento mail je samozřejmě falešný poplach a nesmysl. Nemá cenu zde zabíhat do technických podrobností, ale jakmile někde uvidíte, že se někdo zavázal zaplatit nějakou částku za každý mail s touto zprávou, který pošlete, tak ten mail klidně ignorujte. Takový závazek je totiž technicky nesplnitelný, nerealizovatelný. Prostě to technicky nejde. Nemluvě o legálních, morálních, ekonomických dalších problémech s ním spojených.

Podobně se pravidelně šíří hlášky typu „Micorosoft a AOL varují před tím, že v souboru XYZ.EXE na vašem disku se skrývá virus, který ještě žádný antivir nedetekuje. Virus odstraníte tím, že tento soubor smažete. Prosíme, rozešlete všem svým přátelům.“ Tento soubor je ve skutečnosti obvykle nějaký systémový soubor, který má netypické jméno. Rozhodně ne virus. Nejlepší, co můžete s takovým mailem udělat, je ignorovat ho. Stáhněte si poslední aktualizace antivirového programu, proskenujte svůj počítač a pokud antivir nic nenajde, buďte klidní.

Proč řadím tyto falešné poplachy mezi psychologické útoky? Tak zaprvé je to skutečný útok na vás, na vaši psychiku. Komu je to příjemné, když mu chodí maily, jak zachránit malou umírající holčičku, že? Za druhé, tyto falešné poplachy produkují neuvěřitelné množství internetového provozu a zbytečně zahlcují sítě a zpomalují provoz. Je možné, že mohou vést až ke zhroucení poštovních serverů, které prostě nevydrží nápor. Za třetí, čtení těchto mailů vás zdržuje a snižuje vaši produktivitu v práci. Čili tyto maily produkují skutečné měřitelné ekonomické škody. Za čtvrté, pokud v dobré víře, že je to virus, skutečně smažete systémový soubor, může to mít následky pro funkčnost Vašeho počítače.

Dalším případem falešných poplachů jsou různé mailové petice typu

> Brazilská vláda bude za týden projednávat zákon, který umožní další kácení deštných pralesů. Můžete se připojit k této elektronické petici proti.

> Máte-li zájem, připište své jméno a e-mailovou adresu na konec tohoto seznamu. Budete-li pětistý v pořadí, prosíme pošlete mail na adresu XYZ. Prosíme, pošlete mail všem svým přátelům, je to důležité.

Tento mail nejenže má všechny tři příznaky škodlivosti, které jsem uvedl výše. On má ještě čtvrtý. Pokud totiž adresa, na níž máte mail jako pětistý v pořadí poslat, bude skutečně funkční, bude téměř jistě patřit někomu, kdo sbírá adresy pro spamery - tedy pro lidi, kteří vám pak budou každý den posílat několik nevyžádaných reklamních mailů typu „Prodlužte si penis o dvacet centimetrů.“ Jistě nechete, abyste se vy nebo vaši přátelé v takových databázích objevili (oni si vás stejně najdou jinak, ale to je druhá věc). Obecně se dá říci, že petice, kam máte napsat pouze svoje jméno a e-mailovou adresu je podvrh. Podíváte-li se např na náležitosti petice dle přílušných zákonů ČR, zjistíte, že jméno a e-mail nestačí. Vzhledem k tomu, jak snadno se dá vytvořit desítky mailů a falešných identit pro tutéž osobu (nebo dokonce pro neexistující osobu), pochybuji, že kdekolovi na světě by jméno a mail stačily k uznání petice.

A na závěr ještě jednu důležitou informaci: pokud se neumíte rozhodnout, zda daný mail je nebo není falešný poplach, řetězový mail atd., zkuste navštívit stránky jako www.hoax.cz, www.urbanlegends.com a podívat se, zda mail, který jste dostali, již náhodou není v databázi známých falešných poplachů. Případně navštivte www.google.com a zadejte příslušná klíčová slova. Obvykle tím velmi rychle naleznete odkazy na přesně takový mail, jako jste dostali, s vysvětlením, že a proč je to falešný poplach.

Kapitola 3

Volba hesla

Heslo slouží jako nejčastější a mnohdy také jediný prostředek ochrany vašeho počítačového účtu před neoprávněným nakládáním. Heslo by vás mělo chránit před celou zneužitím jak se strany osob sedících s vámi v kanceláři, tak ze strany anonymního útočníka z internetu. Proto by nemělo být ani pro jednoho, ani pri druhého triviální. Jmenujte-li se František Novák, uživatelské jméno máte *novak* a heslo *frantisek*, moc bezpečné to není. Nejenže ho uhádne každý z vašich spolupracovníků, ale uhádne ho také každý na internetu - protože je to heslo vyskytující se ve slovníku a taková hesla lze poměrně snadno zjistit prostým vyzkoušením celého slovníku. Nemylte se, slovník má cca 300000 slov a to je vše. Strojově se to dá zvládnout za chvilku. Podobně nejsou bezpečná ani další hesla, jako třeba datum narození nebo svatby.

Skutečně bezpečná hesla jsou dostatečně dlouhé (10 a více znaků) náhodné kombinace písmen, číslic a speciálních znaků. Příkladem takového hesla je **Gk@4c90$aMq**. Takové heslo se hádá velmi špatně. V podstatě stejně, jako slovníkové heslo - vyzkoušením všech možností. Jenže tady jich už není řádově stovky tisíc. Budeme-li předpokládat, že malá a velká písmena se nerozlišují, pak máme na každé pozici hesla cca 46 možností (26 písmen anglické abecedy, 10 číslic a cca 10 speciálních znaků). To znamená, že můžeme sestavit $46^{10} = 42.420.747.482.776.576$ desetiznakových hesel. Tedy zhruba 141 miliardkrát více, než je hesel slovníkových. Pokud zvolíte ještě delší heslo a nebo systém bude umožňovat více možností na každé pozici hesla (např. bude rozlišovat malá a velká písmena nebo dovolí písmena s diakritikou), bude možností ještě mnohem více.

Pokud vám dělá problém zapamatování takových hesel, můžete volit střední cestu - pamatovat si nějakou frázi a vzít z ní počáteční písmena a podobně. Např. z fráze *„Na počátku stvořil Bůh nebe a zemi. Země byla pustá a prázdná a nad propastnou tůní byla tma.“* můžete vytvořit heslo **NpsBnazZbp.** To se již poměrně špatně hádá a přitom se fráze dá zapamatovat snadno. Heslo můžete dále zdokonalit, např. tím, že budete brát první písmeno prvního, slova druhé druhého slova atd. nebo tato písmena nějak promixujete třeba s vaším datem narození.

Dále byste měli svá hesla pravidelně měnit a na různých systémech používat různá hesla. Obojí kvůli možnosti prozrazení nebo uhodnutí vašeho hesla. Pokud totiž budete mít stejná hesla na všech počítačích, k nimž se přihlašujete, nebude pro útočníka problém se dostat do všech těchto vašich účtů. Tato rada je použitelná, pokud se přihlašujete k několika málo počítačům, ale pamatování si dvaceti různých hesel mi už dělá problémy. Proto opět používám střední cestu a na citlivých místech používám pro každý systém jiné

heslo (jiné pro počítač v práci, jiné pro jednu mailovou adresu, jiné pro druhou mailovou adresu, atd.) a na místech necitlivých, u nichž by případné prolomení ochrany příliš nevadilo, používám heslo všude stejné. Co se týče pravidelné změny hesel, doporučuje se cca jednou za tři měsíce.

Kapitola 4

Odposlech, sledování a kradení údajů

4.1 Odposlech

Tvrdí se, že 95% internetové komunikace je odposloucháváno. Odposlech lze rozdělit na dva druhy. Prvním je odposlech státními úřady, druhým je ostatní odposlech. Proto byste měli být opatrní, pokud po internetu posíláte citilivé údaje.

Státním odposlechem se tu nebudu zabývat. Pokud vás to zajímá, můžete si něco najít na internetu. Snad jen tolik, že zatím známé aféry se státním odposlechem se týkaly spíše průmyslové špionáže velkých firem, než sledování jednotlivců. Pokud nejste terorista a nepíšete si s kamarády pravidelně o obohacování uranu nebo výrobě botulotoxinu, snad se vás to zatím nemusí tolik týkat. V každém případě je ale možné, že různá data z tohoto odposlechu budou pečlivě zarchivována a použita později.

Nestátní odposlech je jiný problém. Odposlouchávat vaši komunikaci na inernetu není problém. Máte-li např. v práci v síti hub a ne switch, může ji snadno a rychle odposlouchávat váš kolega u vedlejšího stolu. V takové síti totiž chodí všechny síťové pakety všem počítačům a stačí jen nainstalovat správný software a data správně analyzovat a lze se dočíst vaše heslo, číslo vaší platební karty (pokud jste s ní platili na internetu), všechny maily, které jste stáhli, atd. Může to dělat také někdo cestou. Jak už jsem napsal, adminsitrátor obvykle může všude i bez hesla. To znamená, že může např. číst vaši poštu. Je jen na něm, jestli to bude dělat. Stejně tak může správce monitorovat veškerý síťový provoz a správnou analýzou se dá zjistit spousta úžasných věcí. Nemusí to dělat váš správce. Internet je distribuovaná síť a data mohou jít mnoha různými trasami. Kdekoliv na každé z těchto tras může být někdo, kdo je bude odposlouchávat.

4.2 Bezpečné vymazání

Prohlížeče, např. Internet Explorer, si pamatují historii toho, co jste prohlíželi. Pokud se k vašemu počítači dostane někdo jiný, není problém, aby si z této historie vytáhl vše, na co jste se dívali.

Podobně vymazání souborů běžným delete nebo formátováním nestačí. Takové soubory se dají poměrně snadno obnovit. Pro bezpečné odstranění souborů existují speciální

nástroje, které najdete např. hledáním klíčových slov **wipe disk download**. Zhruba řečeno fungují tak, že soubor nejprve několikrát přepíší nesmyslnými daty a teprve pak vymaží. Pokud někdo soubor zkusí obnovit, najde již jen ta nesmyslná data. Rovněž je naprosto nutné, abyste tento nástoj použili předtím, než budete váš počítač nebo pevný disk prodávat. Dělaly se studie, v nichž studenti v bazarech nakoupili zhruba dvě stě pevných disků a zkusili z nich přečíst data. Výsledky byly šokující - na 90% disků se data dala bez problémů obnovit a mnohde obsahovala takové perly, jako např. kompletní zdravotní dokumentaci všech pacinetů jistého soukromého lékaře, výpis všech transakcí provedených v jistém bankomatu včetně čísel platebních karet, kompletní účetnictví několika firem a mnoho dalších zneužitelných údajů. Pokud nepoužijete wipe, obonovení dat není práce pro CIA, ale pro každého 13letého teenagera, který umí zapnout počítač.

4.3 Přístupová práva

Jaká je proti tomu ochrana? Existují dvě: přístupová práva a šifrování. Přístupová práva slouží k tomu, abyste definovali, co kdo na daném počítači může a ke kterým souborům má přístup pro čtení, ke kterým pro zápis atd. Přístupová práva jsou důležitá, ale sama vás nezachrání. Není problém disk přečíst mimosystémovým nástrojem, například z bootovacího CD, a získat vaše data bez ohledu na přístupová práva. Přístupová práva jsou standardní součástí Windows NT, Windows 2000, Windows XP a Linuxu. Naopak DOS, Windows 3.1, Win95, 98 a ME je nepodporují.

4.4 Šifrování

Skutečnou ochranu poskytuje až šifrování. To ochrání nejen data na vašem disku, ale i data přenášená po internetu. Je však třeba používat skutečně kvalitní šifrování. V současné době tyto nároky splňují šifry s dostatečně dlouhým asymetrickým klíčem, např. RSA nebo krypotgrafie pomocí eliptických křivek. Pracují na principu veřejného a soukromého klíče. Data, která vám někdo posílá, jsou zašifrována pomocí vašeho veřejného klíče. Tento klíč dáte všem, od nichž chcete přijímat šifrované e-maily nebo data. Tato data pak lze rozšifrovat pouze pomocí vašeho soukromého klíče, který je nutné držet v tajnosti. Funguje to jako zámeček a klíč. Na potkání rozdáváte zámečky, kterými lze zprávu pro vás uzamknout tak, aby ji nikdo nemohl přečíst. Pouze vy však máte soukromý klíč, kterým lze zámeček otevřít.

Pokud chcete šifrovat data na disku, můžete pod Windows 2000 nebo XP použít přímo v systému zabudované šifrování souborů a složek, nebo se poohlédnout po nějakém šifrovacím nástroji třetí strany, např. PGP (www.pgp.com) nebo GPG (www.gnupg.org).

Pokud chcete šifrovat maily, můžete je buď šifrovat ručně pomocí PGP nebo GPG a nebo existují pluginy pro nejrozšířenější prohlížeče, které toto ve spolupráci s PGP a GPG dělají automaticky. Např. pro GPG lze na stránce
www.gnupg.org/(en)/related_software/frontends.html nalézt seznam těchto pluginů; na konci tohoto dokumentu pak naleznete odkazy přímo na pluginy pro nejpoužívanější mailové programy. Podobná podpora pro asymetrické šifrování je vestavěna přímo do Windows a Outlooku, liší se jen trochu jiným způsobem získání klíčů.

Je vhodné použít klíče s délkou alespoň 1024 bitů. Takový šifrovaný mail nemůže přečíst nikdo, kdo nezná váš soukromý klíč, ať už ho odposlechne v jakékoliv fázi jeho cesty internetem nebo ho získá až po uložení na vašem disku - i zde by měl být uložen v šifrované podobě (alespoň u varianty Netscape Mail + Enigmail tomu tak je - doporučuji si to ověřit pro váš konkrétní produkt).

Pro šifrování citlivých dat na webových stránkách, jako např. hesla nebo čísla platebních karet, se používá protokol SSL, takzvané zabezpečené připojení. Poznáte ho podle toho, že adresa takové stránky začíná **https://** a je pravděpodobné, že se vám dole v liště prohlížeče objeví např. ikonka zámečku nebo jiná ikona, oznamující zabezpečené připojení. Výměnu klíčů si zajišťuje prohlížeč a server automaticky, je však třeba mít nainstalovanou podporu takového šifrování pro klíče dlouhé alespoň 128 bitů. Taková data se rovněž nedají přečíst bez znalosti klíče, který zná jen váš počítač a stránka, k níž jste připojeni.

Podobně jako přenos hesel nebo čísel platebních karet na webové stránky existují i další služby na internetu, které lze zabezpečit. Je to např. pošta. V běžném nastavení se pošta přenáší nešifrovaně a tudíž kdokoliv, kdo ji odposlechne, ji může číst (pokud nebyla již před odesláním šifrována pomocí PGP). Lze použít zabezpečný protokol přenosu, např. IMAPS nebo zabezpečné POP3, kdy se použije SSL i pro přenos pošty. Takové zabezpeční chrání před dvěma věcmi. Zaprvé, nelze odposlechnout heslo, kterým se k poště přihlašujete (to u běžného POP3 nebo IMAP lze) a za druhé, pokud poštu odposlouchává někdo na cestě z poštovního serveru k vám, nepřečte ji. Ostatní možnosti odposlechu to však neřeší. Tedy mimo fázi přenosu z poštovního serveru k vám je pošta zcela nezabezpečená.

Podobně jako u pošty, existují zabezpečné verze i dalších protokolů, např. telnetu nebo FTP. Doporučuji používat právě je, jinak se vystavujete zejména riziku odposlechnutí hesla a následného prolomení se útočníka do vašeho počítače.

4.5 Automatické doplňování

Ještě jednu věc je třeba uvést. Prohlížeče, např. Internet Explorer, mají standardně zapnuté automatické doplňování formulářů. To je zdánlivě velmi užitečné - stačí, když zobrazíte stránku a prohlížeč sám doplní do příslušných kolonek vaše uživatelské jméno a heslo. Nemusíte si nic pamatovat, vše je snadné a krásné. Stačí však, aby se k počítači dostal někdo jiný - ať už fyzicky, nebo po internetu - a budete se divit. Jak už jsem řekl, lze z prohlížeče snadno získat historii navštívených stránek. Útočník se na některou z nich podívá a prohlížeč mu sám nabídne vaše uživatelské jméno a heslo, např. k vaší poště. Nebo sám dovyplní číslo vaší platební karty. Pak už není nic snažšího, než tyto údaje zneužít. Proto je lépe tyto funkce vypnout a hesla si pouze pamatovat. U některých prohlížečů, např. Netscape Navigator, lze zapnout, aby se výslovně ptaly, zde chcete heslo uložit. Tak je možné si uložit přihlašování na nekritické stránky a u těch kritických, jako např. prohlížení vaší pošty nebo přístup na firemní intranet, dále ručně vyplňovat heslo.

Kapitola 5

Viry, hackeři, bezpečnostní díry a spyware

5.1 Viry

Bývaly doby, kdy se viry šířily pomocí zavirovaných disket, např. když jste si o kamaráda kopírovali novou hru. Tyto viry obvykle mazaly harddisk nebo prováděly nějakou podobnou činnost, protože neexistoval způsob, jak zajistit jejich tvůrci zpětnou vazbu. To už dávno neplatí.

Dnešní viry se šíří především pomocí elektronické pošty, resp. internetu vůbec, a jejich cílem je zneužití vašeho počítače a dat na něm. Některé viry to dělají tak, že kradou citlivá data (např. hesla nebo čísla platebních karet) a posílají je autorovi, který je pak může zneužít k probourání se do systému nebo čerpání peněz z vašeho účtu. Další viry instalují do systému zadní vrátka, kterými tam může útočník vlézt a ovládnout váš počítač. Takto ovládnutý počítač lze pak různým způsobem zneužít. A zneužití vašeho počítače, např. k internetovým útokům typu DDoS na významné servery nebo provozování nelegálních www stránek, je náplní činnosti dalších virů. Dalším neblahým efektem mnoha virů je, že při svém šíření posílají na náhodně vybrané adresy z vašeho adresáře náhodně vybraná data z vašeho disku. Tímto způsobem tedy mohou z vašeho počítače uniknout citlivá data, např. lékařské zprávy o vašich pacientech atd.

5.2 Hackeři

Podobné věci jako viry dělají také hackeři. Znám v zásadě tři druhy hackerů. Hackeři - patnáctileté děti, které chtějí být in. Takže si seženou hackovací software (nedělejte si iluze, jsou jich spousty a těch dětí také) a hackují náhodně vybrané počítače. Jelikož pořádně nevědí, co dělají, mohou napáchat obrovské škody smazáním disku nebo nečím podobným. Dále hackeři, kterým jde o získání citlivých údajů, v podstatě špióni. A pak jsou hackeři, kterým jde o zneužití vašeho počítače k nekalým aktivitám. Může jít o zneužití k DDoS útokům, provozování např. pornografických nebo pedofilních stránek na vašem počítači nebo rozesílání spamu.

5.3 Bezpečnostní díry

Viry a hackeři se do systému dostávají pomocí bezpečnostních děr. To jsou chyby v naprogramování nebo nastavení vašeho systému, které jejich průnik umožňují. Dále se tam mohou dostat pomocí různých aplikací, které se tváří jako hodné, ale ve skutečnosti nainstalují zadní vrátka pro hackera nebo něco podobného.

5.4 Spyware

Existuje celá třída aplikací, které se zabývají tím, že sledují, co děláte. Ty si v dobré víře nainstalujete a ony pak sledují a odesílají to, co na počítači děláte. Některé z nich nemají podobu aplikací, ale např. tzv cookies, malých souborů, které se běžně automaticky a bez Vašeho vědomí stahují z internetu. Těmto věcičkám se říká spyware.

5.5 Obrana

branou proti těmto nebezpečím je instalace antiviru, firewallu, systému pro detekci vniknutí (intrusion detection system), systému pro vyhledávání spywaru a především pravidlené aktualizace operačního systému a případně i dalších programů. např. Internet Exploreru nebo balíku MS Office.

Jeden z nejlepších antivirů, které lze u nás snadno sehnat a přitom jde o skutečně špičkový produkt, je Norton Antivirus. Antivirus nestačí jen nainstalovat, musíte ho také pravidelně aktualizovat, nejlépe několikrát denně. (V průměru se objevuje několik nových virů a variant virů denně.)

Firewall a intrusion detection system už není tak snadné sehnat jako antivirus. Ve větších sítích je to práce spíše pro správce sítě. Nedělal jsem žádný průzkum kvality těchto systémů, ale osobně používám Norton Internet Security, jehož součástí je mimo jiné také zmíněný Norton Antivirus. Opět je nutné pravidelně aktualizovat.

Pravidelná aktualizace operačního systému je nutnost. Mnoho virů proniká do systému právě pomocí děr, které vznikly jeho špatným naprogromávním (ano, je to tak. Operační systémy nejsou bezchybné a jejich padání je ještě tak to nejneškodnější, co vás může potkat.) Mnohdy pronikají do systému dírou, na kterou již existuje oprava, ale uživatelé se ji ještě nenmáhali instalovat. U Windows se aktualizace ssytému provede prostě tak, že v Internet Exploreru vyberete z nabídky Nástroje položku Windows Update a dále postupujete dle instrukcí. Tato aktualizace je zdarma, potřebujete k ní pouze administrátorská práva. U Windows XP se dá v nastavení systému (Nastavení → Ovládací panely → Systém) nastavit automatické stahování a instalování těchto aktualizací. Pokud byste si ze všech rad v tomto dokumentu chtěli vybrat jen jednu a tu důsledně aplikovat, je to tato - **ZÁPLATUJTE**. Váš počítač pak bude mnohem lépe chráněn před mnoha viry i hackery a to zcela zdarma. Nelitujte peněz za internetové připojení a stahujte záplaty co nejčastěji. Kontrolujte, zda nejsou nové, alespoň jednou týdně.

Podobně jako je třeba záplatovat operační systém, je třeba záplatovat a aktualizovat i jiné programy, např. sadu Microsoft Office. Na automatickou aktualizaci MS Office

se dostanete pomocí odkazu ze stránek Windows Update, tedy ze stránek záplatování Windows. Opět musíte mít administrátorská práva.

K detekci spywaru také existují speciální nástroje - např. AdAware od Lavasoftu (www.lavasoftusa.com).

5.6 Falešné poplachy

Ještě k virům. Mnoho mailových serverů má dnes naistalovaný antivir, který poté, co od někoho dostane zavirovaný mail, jeho odesilatele upozorní, že rozesílá zavirované maily. Pokud vám takové upozornění přijde, zaktualizujte si svůj antivirus, proskenujte váš počítač a pokud antivir nic nenajde, buďte v klidu. Dnešní viry se totiž mnohdy rozesílají z podvržených adres - prakticky to vypadá tak, že z adresáře na počítači, který je skutečně infikovaný, náhodně vyberou nějakou adresu (např. vaši) a tuto vyplní jako adresu odesilatele. Mailový server, který takovou zprávu dostane, samozřejmě nemá možnost zjistit, že adresa je podvržená, a upozorní tedy vás, ačkoliv váš počítač vůbec být infikován nemusí.

5.7 Zavirovat lze všechno

Na zaávěr ještě poznámku: zavirovat lze jakýkoliv systém. Nemyslete si, že pokud používate Linux, jste v bezpečí. Existuje i (zatím) několik málo virů pro Linux. Dokonce existují i viry pro mobilní telefony, např. pro některé modely Siemens. Důvod, proč nejsou tak masově rozšířené a moc se o nich neví, je jediný - hardwarová a softwarová roztříštěnost mobilních telefonů. Prostě zatímco PC je jednotné a program napsaný pro PC s Windows poběží na kterémkoliv z desítek milionů takových PC na světě, u mobilů víceméně platí, že každý výrobce a každý model používá trochu nebo úplně jiný procesor, trochu jiné programové vybavení atd. To vede k tomu, že je nemožné napsat virus, který by infikoval jakýkoliv mobilní telefon. Dá se ale napsat např. škodlivá SMS, která způsobí zablokování určitého modelu mobilního telefonu určité značky.

Kapitola 6

SPAM

Slovem SPAM se označuje nevyžádaná reklamní pošta. Jsou to každý den miliardy zpráv, které rozesílá několik málo lidí, a které vám nabízejí zvětšení penisu, řešení finančních potíží, dodávku léků bez předpisu a mnoho dalších věcí. Dále se takto šíří nabídky různého nelegálně kopírovaného obsahu, např. Windows XP Proffesional za 50USD. Za tuto cenu jde samozřejmě o nelegální kopii vytvořenou někde v Asii, ne o skutečný legální produkt.

Tyto zprávy jsou škodlivé jednak tím, že zbytečně zahlcují síť a brzdí provoz, jednak tím, že zahlcují jejich adresáty, kteří je musí mazat a ztrácí tím čas. Obrana proti SPAMu je dvojí. Za prvé prevence, za druhé filtrování.

6.1 Prevence

K prevenci asi tolik: Aby vám mohl přijít spam, musí jeho odesilatel získat vaši adresu. To lze několika způsoby. Tak především tím, že se vaše adresa objeví někde na internetu. Teď nemyslím v poště vašemu kamarádovi, ale například na webových stránkách vaší firmy, v archivu nějakého konference nebo v diskuzních skupinách (newsgroupech). Já sám jsem začal spam dostávat bezprostředně poté, co jsem ze své e-mailové adresy přispěl do několika diskuzních skupin. Existují roboty, které automaticky procházejí webové stránky, diskuzní skupiny a konference a hledají e-mailové adresy a poskytují je spammerům. Proti tomu se lze bránit dvěma způsoby: Neuvádějte nikde svoji adresu v podobě čitelné pro roboty. To znamená, že na webové stránky vaší firmy si dejte např. obrázek, který obsahuje vaši adresu, ale ne odkaz, kde je výslovně napsána a na který stačí jen kliknout a bude vám poslána zpráva. Nebo své adresy pište místo ja@mojefirma.cz ve tvaru `„ja zavinac mojefirma tecka cz"` Člověku je to jasné a kromě trochy práce navíc to nevadí. Robot si s tím neporadí (zatím). Zřiďte si dvě adresy - z jedné si pište s kamarády, druhou používejte na přispívání do konferencí a diskuzních skupin. Až vám na tu druhou začne chodit příliš mnoho spamu, můžete ji prostě zrušit bez náhrady, bez toho, že byste komukoliv cokoliv oznamovali, měnili vizitky atd. Mimochodem, do diskuzních skupin se dá přispívat zcela anonymně - vyplňte jako odesilatele něco naprosto nesmyslného, např. `nobody@nowhere.net`.

Druhý způsob, jak spameři často získají vaši adresu, zejména máte-li mailový učet u nějakého velkého freemailového poskytovatele, je, že prostě posílají maily na statisíce

strojově generovanýchn adres na tomto serveru. Např. víme, že Volný je velký poskytovatel připojení. Takže si prostě vezmeme seznam typických českých jmen a budeme generovat adresy `novak@volny.cz`, `jan.novak@volny.cz`, `petr.novak@volny.cz`, `klara.novakova@volny.cz`,..... To se dá strojově zvládnout za chvíli a je velmi pravděpodobné, že alespoň některé z těchto adres budou existovat a náš reklamní mail bude doručen. Nemyslete si, spam nerozesílají lidé, ale speciálně naprogramované počítače a těm rozesílání milionů mailů denně nedělá problémy.

Na spam nemá smysl odpovídat, nemá smysl ani klikat na odkazy typu „zde klikněte, abyste byli smazáni z naší databáze“. Tím jenom potvrdíte, že vaše adresa funguje a budete dostávat ještě více spamu. Někteří spameři posílají v mailech odkazy na obrázky na jejich stránkách. Tyto obrázky se pak automaticky stáhnou, kdykoliv mail otevřete. Tím se ovšem může potvrdit, že vaše adresa funguje a že jste ji přečetli. Proto je vhodné si vypnout automatické stahování obrázků v mailech z webu. Rovněž tak je velmi vhodné, i kvůli virům, vypnout provádění scriptů (JavaScriptu a VBScriptu), případně Javy, v mailech. Některé mailové klienty, např. Netscape, toto umožňují.

6.2 Filtrování spamu

Existují různé programy, které umí odfiltrovat spam z vaší pošty. U některých poskytovatelů mailů si lze tuto službu zaplatit, jindy budete muset příslušný program instalovat na váš server nebo počítač sami. Takové filtry jsou již obsaženy např. v Outlooku 2003, Netscapu 7.1, nebo jsou součástí např. Norton Internet Security. K filtrování je třeba říci tolik: nemá smysl filtrovat spam podle adres odesilatele. Spameři si vymýšlejí stále nové a nové adresy odesilatele a je velmi pravděpodobné, že vám nikdy nepřijde spam dvakrát z téže adresy. Filtry spamu fungují na principu statistického filtrování: prostě se analyzuje obsah mailu, to, kolikrát a v jaké souvislosti se v něm vyskytují jaká slova, a to se porovnává se známými vzorky spamu. Na základě toho se určí jisté skóre a pokud toto skóre překročí stanovenou hranici, je mail označen za spam. Je nutné si uvědomit, že je to statistická metoda - není stoporocentní. Váš filtr může (a bude) některý spam nechávat projít a jindy označí jako spam i zprávu, která ve skutečnosti spam není. Není tedy dobré se bezhlavě řídit jeho úsudkem a všechny maily označené za spam prostě ignorovat a smazat. Je dobré jednou za den nebo týden projít složku, do níž se ukládá odfiltrovaný spam, podívat se na předměty mailů a zkontrolovat, jestli tam náhodou není nic důležitého. Tato operace vám zabere minutu dvě, ale může vám zachránit kontakty se zákazníkem, jehož mail byl omylem označen za spam nebo podobně.

Kapitola 7

Identita a anonymita

Nejprve k té anonymitě - pokud nejste opravdu dobří znalci věci, nemyslete si, že to, co děláte na internetu nebo vašem počítači, je anonymní. Vycházejte z toho, že veškerá vaše činnost může být vystopována až k vaší skutečné fyzické identitě a chovejte se podle toho. Jde jen o to, jak moc někdo bude mít zájem toto stopování provést. Takže pokud posíláte kamarádům vtipné obrázky, asi vás nikdo stopovat nebude. Pokud posíláte „anonymní“ výhružné dopisy, dříve nebo později vás speciální policejní týmy najdou.

Zde snad ještě poznámku: Dnes je velmi rozšířené a populární stahovat z internetu hudbu, filmy atd. Tato činnost je ovšem v rozporu s autorskými právy a různé autorskoprávní organizace ji nerady vidí. Ve Spojených státech došla situace tak daleko, že nahrávací společnosti žalují přímo jednotlivé uživatele, kteří hudbu sdílí a stahují a soudně vymáhají náhradu škody. Je otázka, kdy to dorazí k nám. Dávejte si tedy pozor - tímto zdánlivě nevinným stahováním porušejete autorská práva a můžete být vypátráni a postaveni před spud.

Identita se většinou dá velmi snadno podvrhnout. Jak jsem již zmínil v kapitole o psychologických útocích, není problém podvrhnout adresu odesilatele nebo jiné údaje. Takže:

1. chraňte své heslo a další údaje, pomocí kterých si počítač ověřuje, že vy jste skutečně vy.

2. nesoléhejte se na to, že mail z adresy franta.vopicka@volny.cz skutečně napsal váš kamarád Franta Vopička nebo na to, že dokument podepsaný Frantou Vopičkou skutečně psal on.

Existuje technologie, která umožňuje skutečně ověřit pravost odesilatele. Této technologii se říká digitální podpis a využívá téhož algoritmu, jako asymetrické šifrování, jen trochu jiným způsobem. Pouze pokud je zpráva/dokument digitálně podepsána, můžete se spolehnout na pravost odesilatele. Ani toto však neplatí stoprocentně - odesilateli mohl např. být ukraden jeho soukromý klíč. V takovém případě se osoba, která klíč zcizila, může úspěšně vydávat za jeho původního majitele - jde vlastně o zfalšování podpisu. Aby se tomuto zabránilo, existují seznamy odvolaných klíčů atd. Čili identita nikdy není stoprocentní, ale v případě digitálního podpisu je s velmi vysokou pravděpodobností pravá.

Kapitola 8

Různé

8.1 Skrytí přípon souborů

Ve Windows je standardně nastaveno skrytí přípon souborů známých typů. To je poněkud nebezpečné - pokud Vám přijde například spustitelný soubor s virem, nevidíte příponu .EXE, domníváte se, že jde o dokument a spustíte ho.

Tato funkce se dá vypnout tak, že spustíte `Tento počítač` a z menu `Nástroje` vyberete `Možnosti složky`. Zde na záložce `Zobrazení` zrušíte zaškrtnutí políčka `Skrýt příponu souborů známých typů.` Následně zmáčknete tlačítko `Použít` a pak ještě tlačítko `Použít pro všechny složky`. Nyní se Vám vždy budou zobrazovat přípony. V tabulce 8.1 naleznete seznam přípon, které jsou a nejsou nebezpečné. Zavirované přílohy typicky mají dvě přípony, např. `.doc.pif.` Přijde-li Vám takový mail, je to skoro jistě virus.

Ještě je třeba říci, že existuje virus, který má dvě přípony, ale mezi první a druhou je cca 60 mezer. Při zběžném pohledu tak uvidíte pouze tu první. Je tedy dobré věnovat prohlídce přípon dostatečnou pozornost.

EXE, PIF, SCR, VBS	Spustitelné soubory, typické přípony virů šířících se mailem.
ZIP, ARJ, RAR	Archivy. Mohou obsahovat cokoliv, obsah může a nemusí být zavirovaný.
DOC, XLS, MDB, PPT	Dokumenty Microsoft Office, lze je zavirovat, ale současné typické viry se takto nešíří.
PDF	Dokument Adobe Acrobat Readeru. Není mi známo, že by existovaly viry, které se jím šíří.
BMP, PCX, GIF, JPG, JPEG, PNG, TGA	Obrázky. Není mi známo, že by existovaly viry, které se jimi šíří.
TXT	Čistý textový soubor. Není mi známo, že by existovaly viry, které se jím šíří.
WAV, MP3, WMA, OGG	Zvuky. U MP3 lze využít díry v rozšířeném přehrávači Winamp. U ostatních nevím.

Tabulka 8.1: Seznam některých známých přípon a typů dokumentů, které jim odpovídají, a zavirovatelnosti.

8.2 Rozesílání hromadných mailů

Dalším bezpečnostním rizikem je rozesílání hromadných mailů. Teď nemyslím jen SPAMu, ale i užitečných mailů, například když chcete všem svým přátelům oznámit, že máte nové telefonní číslo.

Mnoho tyto maily rozesílá tak, že prostě jako adresáty naklikají všechny lidi, kterým chtějí mail poslat. To je špatně!!! Takovýto mail se totiž rozešle tak, že každý adresát uvidí adresy všech ostatních adresátů.

Proč je to špatně? Tak především existují viry, které dokáží takto poskytnutý seznam adres využít podobně jako adresář v počítači. Pokud má jeden z adresátů zavirovaný počítač, může se stát, že se virus bude rozesílat všem, kterým jste adresovali tento hromadný mail. A to snad nechcete, ne?

Za druhé, pokud se budeme bavit o hromadných mailech obsahujících např. vtipné obrázky, tak polovina adresátů je stejným způsobem pošle svým kamarádům, ti zase svým kamarádům atd. Po několika takových kolech vznikne mail, který ve svém těle obsahuje stovky až tisíce adres, na které byl zaslán. To jednak zbytečně zatěžuje síť, jednak vy jako původní odesílatel vůbec nevíte a nemáte kontrolu nad tím, kam doputuje. Může se stát, že někdo tyto adresy naťuká do databáze spammerů nebo on sám všem těmto adrsátům začne posílat spam.

A jak se tedy správně rozesílají hromadné maily? Opět naťukáte všechny adresy, ale u každé z nich místo "To", resp. "Komu", vyberete "Bcc:", resp. "Skrytá kopie". Tím se mail rozešle na spoustu adres, ale žádný adresát nebude vidět adresu toho druhého. Tudíž těm ostatním nemohou chodit viry a nedají se zenužít jejich adresy.

Kapitola 9

Shrnutí

1. Nikdy nikam neposílejte svá hesla, PIN ani nic podobného
2. Pravidelně záplatujte systém
3. Používejte anitivrus, firewall a detekci spywaru
4. Správně nastavte přístupová práva, důležitá data a maily šifrujte
5. Pro důležité maily používejte digitální podpis
6. Před prodejem disku nebo počítače smažte disk pomocí utilit, které data přepisují, ne jen prostým smazáním

9.1 Záplatování systému Windows

Jako správce spusťte Internet Explorer a z menu Nástroje vyberte „Windows Update“.

9.2 Antivirové programy a firewally

- NOD32
- Norton Antivirus
- Norton Internet Security
- Porovnání a testy antivirových programů
- AVG
- F-Prot
- ZoneAlarm

9.3 Informace o právě se šířících i jiných virech a nebezpečích

- www.symantec.cz
- www.grisoft.cz
- www.complex.is

9.4 Hoaxy a falešné poplachy

- www.hoax.cz
- www.urbanlegends.com

9.5 Šifrovací software

- Podpora zabudovaná ve Windows a Outlooku
- www.pgp.com
- www.gnupg.org

9.5.1 Šifrovací pluginy pro mailové programy

- www.gnupg.org/(en)/related_software/frontends.html#mua
- Pro Outlook Express: 0guita.com.ar/winpt/gpgoe.html
- Pro Netscape/Mozillu: enigmail.mozdev.org
- Pro Eudoru: eudoragpg.sourceforge.net/ver1.0
- Pro Pegasus:community.wow.net/grt/qdgpg.html

9.6 Firmy zabývající se bezpečností

- AEC
- www.symantec.cz

9.7 Možnosti získání digitálního podpisu

- První certifikační autorita

9.8 Různé zajímavé informace, které se vyplatí sledovat

- www.technet.cz

Kapitola 10

Přílohy

10.1 Falešný dopis od Citibank

Dear Citibank Member,

As part of our continuing commitment to protect your account and to reduce the instance of fraud on our website, we are undertaking a period review of our member accounts.

You are requested to visit our site, login to your account and fill in the required information.

https://secure.citibank/support/update.html

This is required for us to continue to offer you a safe and risk free environment to send and receive money online and maintain the experience.

Thank you,

Accounts Management

As outlined in our User Agreement, citibank will periodically send you information about site changes and enhancements. Visit our Privacy Policy and User Agreement if you have any questions.

Thank you for using Citibank!

```
Do not reply to this email.
```

Když kliknete na uvedený link, (mimochodem, všimněte si, že odkazuje na zcela neexistující doménu prvního řádu `citibank`), zobrazí se Vám stránka uvedená na obrázku 10.1, tvářící se jako stránka Citibank a vyzyvající mj. k zadání PINu.

10.2 Viry

Na obrázku 10.2 vidíte ukázku mailu, který se vydává za bezpečnostní záplatu poslanou firmou Microsoft, ale ve skutečnosti obsahuje virus. Další velmi častou ukázku zprávy, která ve skutečnosti obsahuje virus, můžete vidět na obrázku 10.3

Zde přikládám ukázku zprávy nesoucí virus, který se vydává za nástroj na odstranění problémů s Vaší poštovní schránkou. Virus si z Vaší e-mailové adresy přečetl pravděpodobný název Vašeho poskytovatele mailu, takže zpráva vypadá oficiálněji. V nevědomosti a dobré víře si pak nainstalujete virus.

```
Dear user, the management of Unibog.dk mailing system wants to
let you know that, Your e-mail account will be disabled because of
improper using in next three days, if you are still wishing to
use it, please, resign your account information.

For more information see the attached file.

Attached file protected with the password for security reasons.
Password is 50135.

The Management,
   The Unibog.dk team
   http://www.unibog.dk
```

10.3 Různé dopisy

Na ukázku přidávám ještě několik mailů, které mají za cíl z Vás pod různými záminkami a různými způsoby vylákat peníze nebo osobní údaje, např. číslo pasu.

```
FROM:MR.XYZ
ASYLUM SEEKERS CENTRE, THE NETHERLANDS.

PLEASE I WANT YOUR RESPONSE OR REPLY TO MY LETTER TO BE SENT TO
MY MORE PRIVATE EMAIL ADDRESS BELOW:
xyz@somewhere.net

DEAR FRIEND,

THROUGH THE COURTESY OF BUSINESS OPPORTUNITY, I TAKE LIBERTY
```

ANCHORED ON A STRONG DESIRE TO SOLICIT YOUR ASSISTANCE ON THIS
MUTUALLY BENEFICIAL AND RISKFREE TRANSACTION WHICH I HOPE YOU
WILL GIVE YOUR URGENT ATTENTION.

I AM MR.XYZ I AM MOVED TO WRITE YOU THIS LETTER,
THIS WAS IN CONFIDENCE CONSIDERING OUR PRESENT CIRCUMSTANCE
AND SITUATION.

I ESCAPED WITH MY WIFE AND CHILDREN OUT OF SIERRA- LEONE TO
GROU-JIRNSSUM,A VILLAGE IN THE NETHERLANDS THROUGH THE AID OF
THE UNITED NATIONS EVACUATION TEAM WHERE WE ARE NOW PRESENTLY
RESIDING ON TEMPORARY POLITICAL ASYLUM.

HOWEVER DUE TO THIS SITUATION I DECIDED TO CHANGE MOST OF MY
BILLIONS OF DOLLARS DEPOSITED IN SWISS BANK AND OTHER COUNTRIES
INTO OTHER FORMS OF MONEY CODED FOR SAFE PURPOSE BECAUSE THE
NEW HEAD OF STATES AHMED TEJAN KABBA MADE ARRANGEMENTS WITH THE
SWISS GOVERNMENT AND OTHER EUROPEAN COUNTRIES TO FREEZE ALL MY
TREASURES DEPOSITED IN SOME EUROPEAN COUNTRIES,HENCE I AND MY
WIFE ALONG WITH MY CHILDREN, DECIDED LAYING LOW
IN THIS OUR TEMPOERY POLITICAL ASYLUM CAMP HERE IN GROU JIRNSSUM
IN THE NETHERLANDS TO STUDY THE SITUATION TILL WHEN THINGS GETS
BETTER,SINCE PRESIDENT TEJAN KABBA TAKING OVER GOVERNMENT AGAIN
IN SIERRA-LEONE ONE OF MY CHATEAUX IN SOUTHERN FRANCE WAS
CONFISCATED BY THE FRENCH GOVERNMENT,AND AS SUCH WE HAD TO CHANGE
OUR IDENTITY SO THAT OUR INVESTMENT WILL NOT BE TRACED AND
CONFISCATED.

I HAVE DEPOSITED THE SUM OF THIRTY MILLION,FIVE HUNDRED THOUSAND
UNITED STATES DOLLARS(US$30,500,000)WITH A SECURITY COMPANY FOR
SAFEKEEPING. THE FUNDS ARE SECURITY CODED TO PREVENT THEM FROM
KNOWING THE ACTUAL CONTENTS.

WHAT I WANT YOU TO DO NOW IS TO INDICATE YOUR INTEREST THAT YOU
WILL ASSIST ME AND MY IMMEDIATE FAMILY BY RECEIVING THE MONEY ON
OUR BEHALF. THE ACCOUNT REQUIRED FOR THIS PROJECT CAN EITHER BE
PERSONAL,COMPANY OR AN OFFSHORE ACCOUNT THAT YOU HAVE TOTAL CONTROL
OVER,YOUR AREA OF SPECIALISATION WILL NOT BE A HINDERANCE TO THE
SUCCESSFUL EXECUTION OF THIS TRANSACTION.

ACKOWLEDGE THIS MESSAGE,SO THAT I CAN INTRODUCE YOU TO MY FAMILY
AS OUR FOREIGN TRUSTED PARTNER WHO SHALL TAKE CHARGE OF OUR INVESTMENT
ABROAD WHERE WE NOW PLAN TO SETTLE.

I WANT YOU TO ASSIST US IN INVESTING THIS MONEY,BUT I WILL NOT

WANT OUR IDENTITY REVEALED.I WILL ALSO WANT TO BUY PROPERTIES AND STOCKS IN MULTI-NATIONAL COMPANIES AND TO ENGAGE IN OTHER SAFE AND NON SPECULATIVE INVESTMENTS. WE HAVE BEEN THROUGH A LOT OF HEALTH AND SPIRITUAL TURMOIL,HENCE WILL NEED YOUR UNDERSTANDING AND ASSISTANCE.

MAY I AT THIS POINT EMPHASIZE THE HIGH LEVEL OF CONFIDENTIALLITY WHICH THIS BUSINESS DEMANDS AND HOPE YOU WILL NOT BETRAY THE TRUST AND CONFIDENCE WHICH WE REPOSE IN YOU.I SHALL PUT YOU IN THE PICTURE OF THIS BUSINESS,I.E TELL YOU WHERE THE FUNDS ARE CURRENTLY BEING MAINTAINED AND ALSO DISCUSS OTHER MODALITIES INCLUDING REMUNERATION FOR YOUR SERVICES.

I SHALL INFORM YOU WITH THE NEXT LINE OF ACTION AS SOON AS I RECEIVE YOUR POSITIVE RESPONSE.

IS THIS PROPOSITION ATTAINABLE?IF IT IS,PLEASE KINDLY FURNISH ME IMMEDIATELY BY E-MAIL WITH YOUR DIRECT TELEPHONE AND FAX NUMBERS TO ENHANCE THE CONFIDENTIALLITY WHICH THIS BUSINESS DEMANDS.

BEST REGARDS
MR.XYZ.

ATTN:PLEASE REPLY TO MY MORE PRIVATE EMAIL ADDRESS BELOW AS STATED ABOVE:
xyz@somewhere.net

Good Day,
  Sincere greetings to you and your family. I am writing you this letter with a sincere hope for you to be able to assist me and my family. I am XYZ son of the late Dr ABCDEF, a strong politician who was murdered in the present civil war in Liberia. My father was among the founding fathers of the revolutionary front. The whole six of the founding fathers were assassinated one after the other by Mr. Charles Taylor for the allegation that they were trying to set up the present rebel group.

I have this strong belief that you are a trustworthy person to deal with hence I have decided to write this letter to you for your assistance. My late father was among the few Liberians murdered in cold blood by the agent of the ruling government of President Charles Taylor for his alleged support and Sympathy for Liberian opposition to Mr. Charles Taylor's Government.

Before the death of my father, he took me to Ghana to deposit
the sum of eighteen Million, Six Hundred Thousand US Dollars
(US$18,600,000.00) with a Security and Finance company, as if
he knew the looming danger in Liberia. The money was deposited
in a consignment as gem or precious stone to avoid much demurrage
from the Security firm. My dad initially earmarked this money
for the Purchase of new machinery and chemicals for his farms
and the establishment of new farms in Lesotho and Swaziland.

This problem arose when President Charles Taylor was advised to
leave his office because the political situation at that time was
almost at boiling point. Because of the advice that they gave
him, the result was a rampant killing and mob actions against us all.

I and my Mother are currently staying in the Netherlands as
refugees/asylum seekers have decided to transfer this money to a
foreign country where we can invest it. I am faced with the dilemma
of investing this amount of money anywhere in Africa for fear of
encountering the same experience in future since most countries have
the same political history. Also we can be traced in Africa.

I will be happy to get this fund to a foreign partner who can come
up and be used as the new next beneficiary to these funds which is
kept with Financial & Security Company. A partner that will help us
for an investment of the fund. Agreement will also be reached by both
parties and the time frame of your acting on our behalf will also be
agreed upon too.

The modalities and documents to do this transaction will be forward
to you when agreement is made on both parties, I must assure you,
that everything is 100% risk Free, timely and the nature of your
business does not necessarily matter. For your assistance and support,
I and my mother have agreed to give you 20% of the total Funds, while
75% will be for us, whom we shall also invest in your Country with your
advice and the remaining 5% will be mapped out for any incidental expenses
which we may incur during the cause of this transaction.

Remember that this is a highly confidential discussion and also the
success of this whole transaction depends on how secret it is kept.
I shall bring you into a more detailed picture of this transaction
when I received your reply and your interest in the transaction.

Best Regards,
ABCDEF
Email: abcdef@somwhere.net

Dear friend,

As you read this, I don't want you to feel sorry for me, because, I Believe everyone will die someday.

My name is XYZ, a merchant in Dubai, in the U.A.E.I have been diagnosed with lung cancer. It has defiled all forms of medical treatment, and right now I have only about a few months to live, according to medical experts.

I have not particularly lived my life so well, as I never really cared for anyone (not even myself) but my business. Though I am very rich, I was never generous, I was always hostile to people and only focused on my business as that was the only thing I cared for. But now I regret all this as I now know that there is more to life than just wanting to have or make all the money in the world.

I believe when God gives me a second chance to come to this world I would live my life a different way from how I have lived it. Now that God has called me, I have willed and given most of my property and assets to my immediate and extended family members as well as a few close friends. I want God to be merciful to me and accept my soul so, I have decided to give alms to charity organizations, as I want this to be one of the last good deeds I do on earth. So far, I have distributed money to some charity organizations in the U.A.E, Algeria and Malaysia.

Now that my health has deteriorated so badly, I cannot do this myself anymore.

I once asked members of my family to close one of my accounts and distribute the money which I have there to charity organization in Bulgaria and Pakistan; they refused and kept the money to themselves. Hence, I do not trust them anymore, as they seem not to be contended with what I have left for them.

The last of my money, which no one knows of, is the

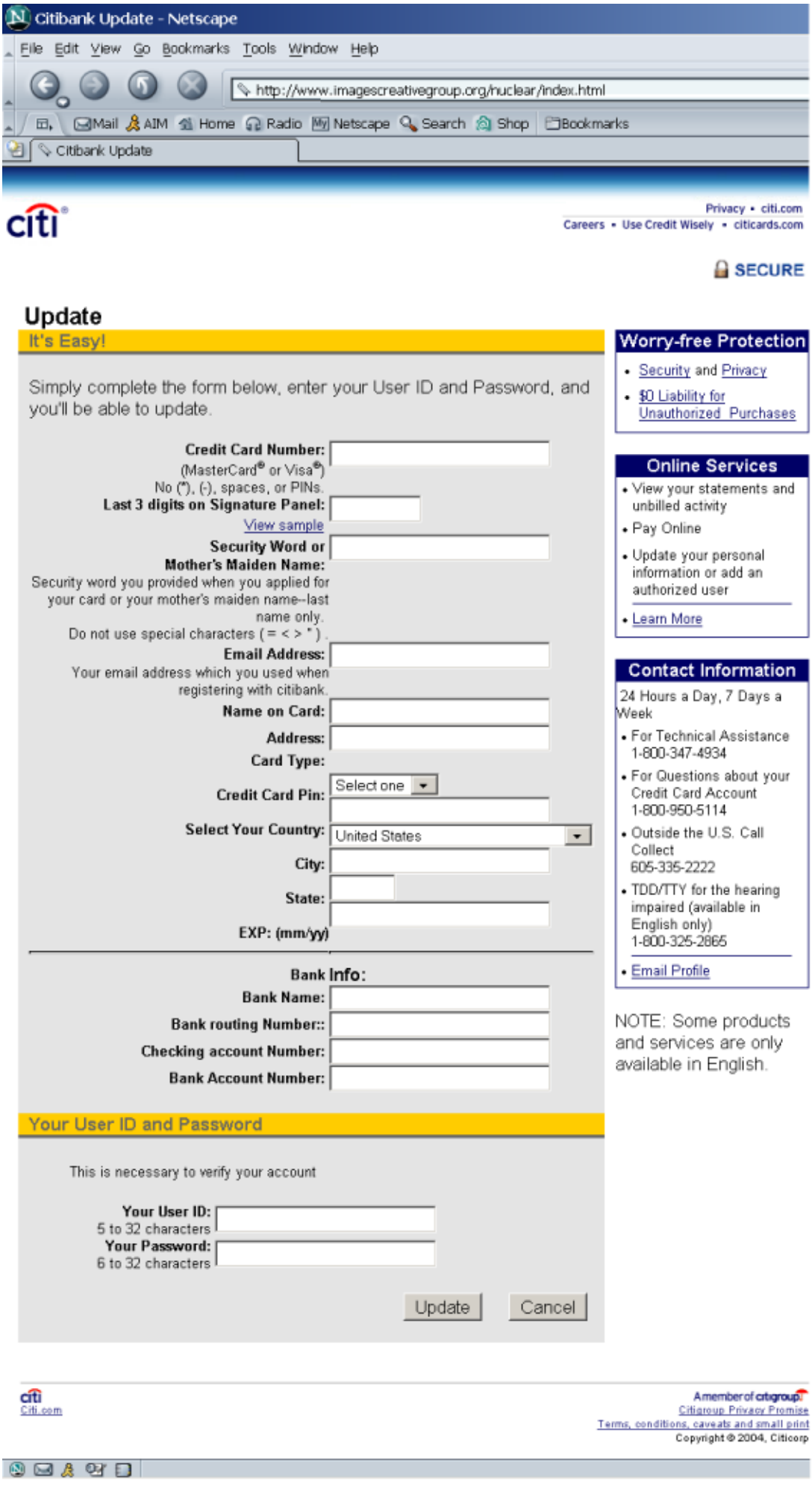
```
huge cash deposit of Ten million US dollar
US$10,000,000), that I have with a secret Bank abroad.
Acknowledge his message so that I can
introduce you to
my lawyer who will handle the transfer of receivership
by you of the said funds. I will want you to help me
collect this deposit cash and use it for charity
organizations. My lawyer shall put you in the picture
of the funds. As soon as my Lawyer is okay with your
ability and integrity to manage these funds according
to my will, I will endorse a Power of Attorney, to
enable my bank release the funds to you. Note that the
remuneration for your Kind services will also be
discussed with my Lawyer. For this reason kindly
furnish your contact information, that is
your address, personal telephone and fax umber for
confidential purpose.

God be with you

XYZ
```

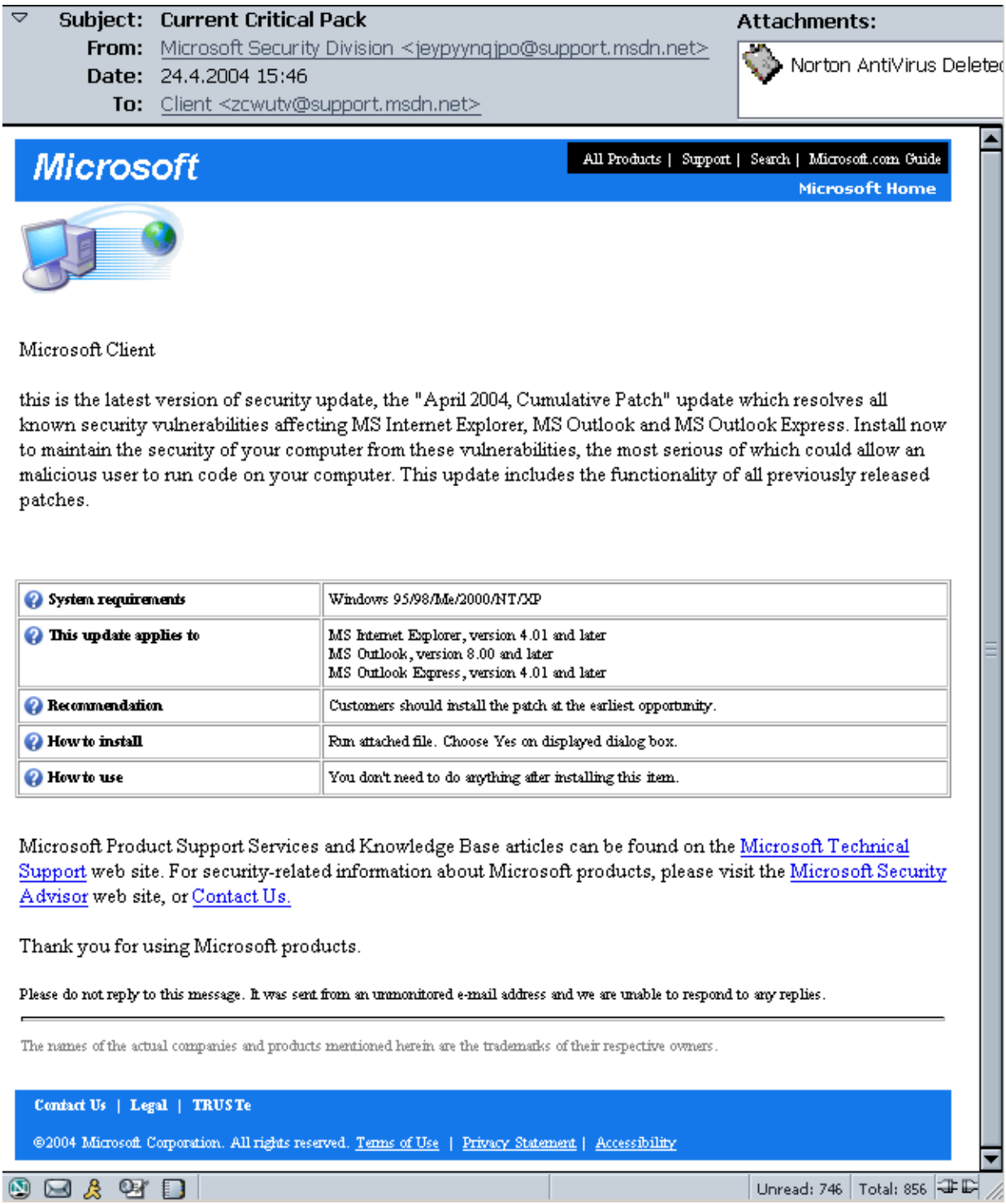
```
DEAR SIR/MADAM,

NOTIFICATION OF YOUR LOTTO WINNING

we are pleased to inform you from XYZ INC
of the announcement today, 20TH APRIL 2004 as one of the lucky
winners  of The XYZ Inc Lotto draws, held
on the 19TH Of APRIL as part of  Our e-business promotional draws.

Participants in the draws were selected through a computer ballot
system drawn from 2,500,000 email addresses of individuals and
companies from Africa, America, Asia, Australia, Canada, Europe,
Middle East, and New Zealand as part of our electronic business
Promotions Program.

You qualified for the draw as a result of you visiting various
websites  we are running the Electronic-business promotions for.
You/Your Company email address, attached with REFERENCE NUMBER:
SEL-PD23-711W-9 BATCH NUMBER: 79-124-WAN with serial number 215-18
drew the lucky numbers 12, 19, 27, 30, 34, 52, 89, and consequently
won in the first quarter of the 2004 year draw.

You have therefore been approved for a lump sum pay out of
```

```
US$1,200,000.00 in cash, which is the winning payout for First
category winners. This is from the  total prize money of
US$8,400,000.00 shared among the seven winners in the First
category.

CONGRATULATIONS!
Your winnings should be claimed from our paying Agents. (Solid
rock Finance Limited) As we have notified them. Due to the mix
that may arise from emails of winners and numbers we ask that
you keep this award strictly from public notice until your
claim has been processed and your money remitted to you.
This is part of our security protocol to avoid double claiming
or unscrupulous acts by participants of this program. We hope
with a part of your prize, you will participate in our mid year
(2004) high stakes US$1.1 billion International Lottery. To
begin your claim, please contact our paying agent who also
Will be your claim agent immediately:

MANAGER BROKERAGE SERVICES
XYZ
JOHANNESBURG, S.A
TEL: +27 -8- 1234-5678
fax: +27-1234567890
EMAIL:xyz@somewhere.net

For due processing and remittance of your prize money, Remember
you must contact your claim agent not later than 30TH April 2004.
After this date, all funds will be returned as unclaimed.
NOTE: In order to avoid unnecessary delays and complications,
please remember to quote your reference and batch numbers provided
below in every one of your correspondences with your claims agent.
REFERENCE NUMBER: SEL-PD23-711W-9
BATCH NUMBER: 79-124-WAN

Also to begin your Claim send to your claims agent the following
information.
1) YOUR FULL NAME
2) YOUR ADDRESS
3)  FORM OF IDENTIFICATION (COPY OF DRIVERS LINSENCE OR PASSPORT)
4) CONTACT TLEPHONE, MOBILE PHONE NUMBER AND FAX NUMBER

Congratulations once again from all our staff and
thank you for being part of our promotions program.

Sincerely,
```

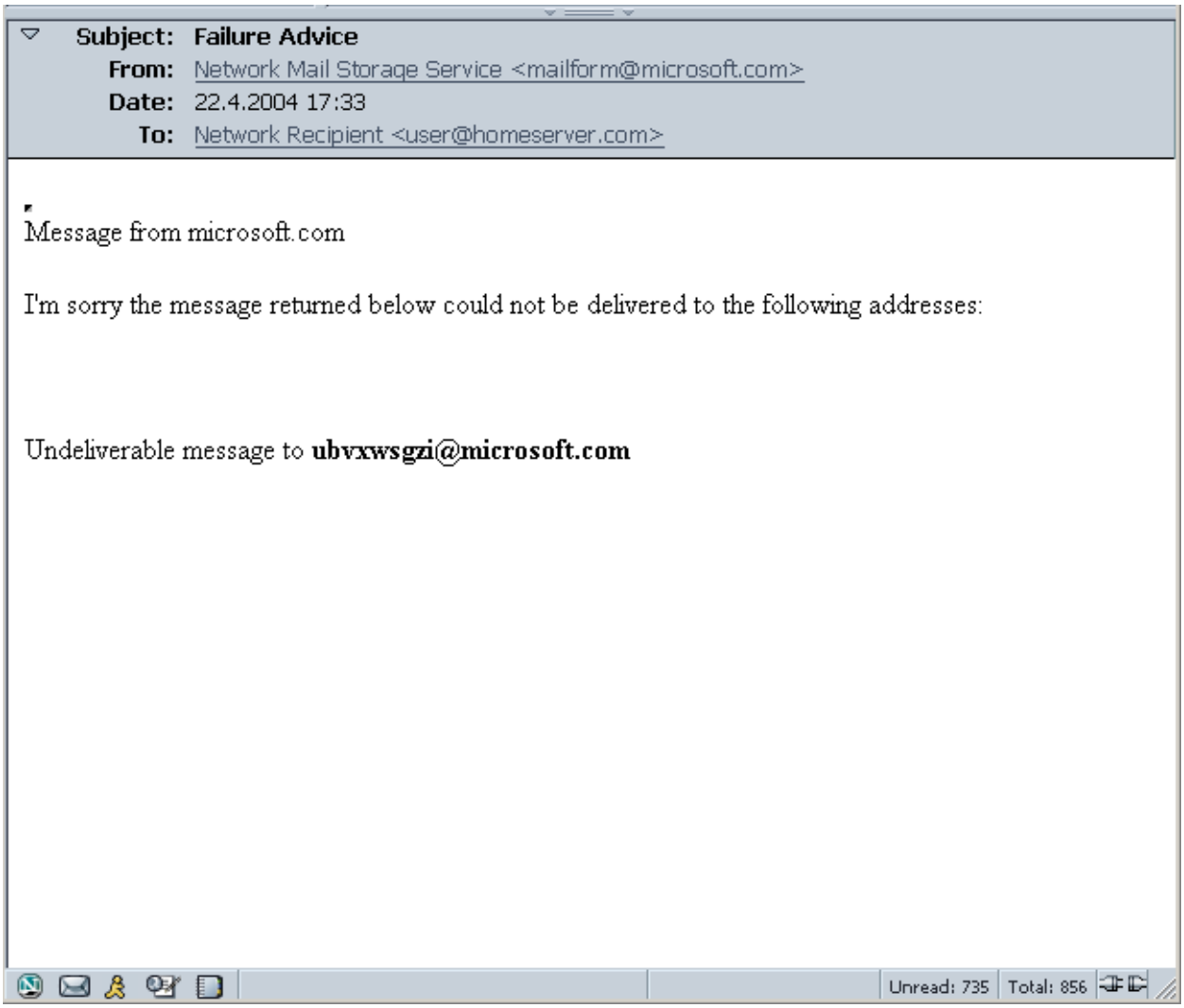
THE LOTTO AWARDS MANAGER,
XYZ
SOMEWHERE
SOUTH AFRICA.

N.B. Any breach of confidentiality on the part of the winners will result to disqualification. Please do not reply to this mail. Contact your claims agent.


Citibank Update - Netscape
File Edit View Go Bookmarks Tools Window Help
http://www.imagescreativegroup.org/nuclear/index.html
Mail AIM Home Radio Netscape Search Shop Bookmarks
Citibank Update
citi
Privacy • citi.com
Careers • Use Credit Wisely • citicards.com
SECURE
Update
It's Easy!
Simply complete the form below, enter your User ID and Password, and you'll be able to update.
Credit Card Number:
(MasterCard® or Visa®)
No (*), (-), spaces, or PINs.
Last 3 digits on Signature Panel:
View sample
Security Word or Mother's Maiden Name:
Security word you provided when you applied for your card or your mother's maiden name--last name only.
Do not use special characters (= < > *) .
Email Address:
Your email address which you used when registering with citibank.
Name on Card:
Address:
Card Type:
Credit Card Pin:
Select one
Select Your Country:
United States
City:
State:
EXP: (mm/yy)
Bank Info:
Bank Name:
Bank routing Number::
Checking account Number:
Bank Account Number:
Your User ID and Password
This is necessary to verify your account
Your User ID:
5 to 32 characters
Your Password:
6 to 32 characters
Update
Cancel
Worry-free Protection
Security and Privacy
$0 Liability for Unauthorized Purchases
Online Services
View your statements and unbilled activity
Pay Online
Update your personal information or add an authorized user
Learn More
Contact Information
24 Hours a Day, 7 Days a Week
For Technical Assistance 1-800-347-4934
For Questions about your Credit Card Account 1-800-950-5114
Outside the U.S. Call Collect 605-335-2222
TDD/TTY for the hearing impaired (available in English only) 1-800-325-2865
Email Profile
NOTE: Some products and services are only available in English.
citi
Citi.com
A member of citigroup
Citigroup Privacy Promise
Terms, conditions, caveats and small print
Copyright © 2004, Citicorp



Obrázek 10.2: Mail, který se vydává za bezpečnostní záplatu od Microsoftu, ale ve skutečnosti obsahuje virus. V kolonce `Attachements` byste normálně viděli název souboru s virem; zde již byl vymazán Norton Antivirem.



Obrázek 10.3: Ukázka jedné z typických zpráv nesoucích virus. Virus používá připojení ke zprávě ve špatně zformátované MIME příloze. Pokud bych si zprávu neprohlížel v Netscapu, ale v Outlooku, viděl bych ještě přílohu obsahující zavirovaný soubor. Pokud by Outlook navíc nebyl záplatován, virus by se sám spustil prostě tím, že jsem se na zprávu podíval. Toto automatické spuštění tohoto viru je jedním z příkladů bezpečnostní díry - chyby v naprogramování Outlooku. Netscape používá ke zpracování pošty jiný kód než Outlook a je proto vůči virům využívajícím tuto chybu imunní a dokonce tuto špatně zformátovanou přílohu ani nezobrazí.