# Bezpečný e-mail

## Porovnání a zhodnocení bezpečnosti na freemailových serverech

VOJTĚCH BEDNÁŘ

**Freemaily – servery poskytující bezplatné e-mailové služby – používají desítky tisíc uživatelů. Jsou tyto servery bezpečné? Neohrožují jejich data a soukromí? Nemohou z nich dělat oběti virových nákaz a spamu? Umožňují zajištění zpráv proti vykradení? V ČR je situace celkem dobrá, nikoliv však ideální.**

České freemaily začaly vznikat v důsledku masového rozšiřování internetu. Prakticky každý ISP, tedy poskytovatel připojení k internetu, nabízí v rámci doplňkových služeb e-mailovou adresu. Pokud jste zákazníkem libovolné ISP společnosti a využíváte její dial-up služby nebo jiné, získáváte e-mailovou adresu, přičemž doména této adresy je velmi často shodná s doménou poskytovatele. Jiný způsob jak získat přístup k e-mailu je v zaměstnání, na škole nebo členstvím v organizaci mající svou doménu a svůj poštovní server.

Bohužel všechny tyto cesty mají vždy nějakou podmínku. Musíte být zákazníkem, zaměstnancem, studentem, členem. Na přelomu století, ale ještě dříve, začaly tyto e-mailové adresy vykazovat mnoho nedostatků. Hlavním z nich byla nízká flexibilita. E-mail se vyřizoval primárně s využitím standardních protokolů POP3/SMTP. To znamenalo, že k vybrání schránky nebo k odeslání zprávy jste nutně potřebovali e-mailový klient, který musel být pro vaši schránku nakonfigurován. Dalším problémem bylo, že někteří ISP omezovali odesílání či příjem schránky výhradně na svou síť. V důsledku toho jste svou domácí adresu například mohli bez potíží vybrat doma, ale nikde jinde, kde se nepoužíval stejný poskytovatel.

Poslední zásadní vadou konvenčního e-mailu byla jeho účelovost. E-mailovou adresu zaměstnavatele by bylo doopravdy nepraktické používat k soukromým účelům jednak proto, že bychom ho tím mohli poškozovat, jednak proto, že by nám ji mohl monitorovat a případně nás také vyhodit.

S rozrůstajícími se službami internetu a také s přibývajícím počtem uživatelů se stalo praktickým mít více e-mailových adres s poměrně jednoznačným určením. Jedna je pracovní, jedna pro konference, jedna soukromá a tak dále. Freemaily, tedy servery poskytující bezplatné e-mailové služby, vznikly z jednoduché úvahy. Dát uživateli to, oč žádá, tedy univerzální a zároveň všude přístupnou e-mailovou schránku bez prostorového nebo účelového omezení a zároveň na tom vydělat. Zdrojem výdělku se měla stát reklama. Jednak ta, která je automaticky přidávána na konec každé zprávy, jež freemailovým serverem projde, a jednak ta, která je uživateli zobrazována při práci s ním ve webmailovém rozhraní (vysvětlení pojmu je v barevném rámečku v tomto článku).

Čas však ukázal, že samotná reklama zaplatí provoz freemailů jen stěží. Důvody jsou pro to dva. Především, reklama má poměrně malou účinnost. Na konci zprávy si ji málokdo přečte nebo dokonce klikne na odkaz v ní. Použití odkazů v těle e-mailu přitahuje pozornost antispamových filtrů na klientské straně. Propagační materiály v rámci webmailu jsou skvělá věc, ale uživatel pracuje především se svou poštou, a proto se na reklamu nesoustředí. To vše i přes masivní množství zobrazených proužků (impresí) znehodnocuje tento způsob propagace. A tak je třeba peníze získávat někde jinde, nejlépe od uživatelů.

Freemaily v současné době požadují peníze za rozšíření prostoru poštovní schránky, za umožnění práce s klientem a nejen přes webmail, dokonce za bezpečnost. Zejména to poslední je problematické, ale děje se to.

### Svět e-mailu je nebezpečný

Těžko říct proč, ale právě e-mail se stal v poslední době největším zdrojem rizik. Prvním z nich jsou virové, respektive červové nákazy, šířící se jako přílohy e-mailových zpráv. Otevření takové přílohy znamená s největší pravděpodobností nakažení počítače, na kterém si dotyčnou zprávu prohlížíte. Moderní antivirové systémy dokáží nakaženou zprávu poznat a zablokovat, nejsou a ani nemohou být však zcela stoprocentní ve svém výkonu. Problematika SPAMu je otázkou sama pro sebe. Někomu chodí nevyžádané pošty jen málo, někomu stovky zpráv denně. Ten druhý případ, pokud by se s ním nic nedělalo, prakticky znemožňuje normální bezproblémové využívání poštovní schránky. SPAM je třeba filtrovat a likvidovat.

Nezanedbatelná jsou dále rizika spojená s možností vykradení účtu. Získat nezajištěné heslo, které zadáváte do přihlašovacího formuláře nebo které odesílá váš e-mailový klient, opravdu není žádný velký problém. Zfalšovat zprávu tak, aby vypadala jako od určitého odesilatele, je rovněž velice jednoduché (a nelze tomu zabránit).

Před většinou z uvedených, ale i dalších rizik je možné se úspěšně chránit. Úroveň této ochrany závisí jednak na tom, jak se svou schránkou pracujete, a jednak na tom, jak jste technicky vybaveni. Antivirus a antispam jsou v současné době spolu s firewallem základními prostředky bezpečnosti, ale mají nedostatek. Jsou vázány na konkrétní počítač. V případě antiviru pak fungují, až když dojde k pokusu o nakažení, v případě antispamu integrovaného v e-mailovém klientu pak naši linku obvykle neušetří stahování mnoha kilobajtů nevyžádaných zpráv ani skutečnosti, že tyto zprávy zabírají drahocenné místo v naší e-mailové schránce na serveru.

Z výše uvedeného vyplývá, že mnohem praktičtější než řešit problémy až při vybírání e-mailu či stahování pošty, by bylo řešit je již při jejím příchodu do elektronické poštovní schránky. Jinými slovy, integrací antivirového systému a spamového filtru přímo do systému, který poštu na serveru přijímá a ukládá do poštovních schránek. To, co je teoreticky ideální, má však své nedostatky.

Už samotný provoz poštovního serveru vybaveného standardním POP3/SMTP a webmailovým rozhraním, který používá několik desítek tisíc lidí, není levná záležitost. Nákup serverové verze antiviru pak něco stojí, o spamovém filtru platí totéž. Obě tato řešení představují rezidentní procesy, a tedy spotřebovávají serverový prostor i strojový čas a paměť. V případě jednoho počítače se o nic nejedná, ale pokud si svou poštu vybírá několik set až tisíc uživatelů zároveň? Takové systémy se rovněž musí vyrovnat s virovými epidemiemi, kdy do jediné schránky může dorazit ohromné množství nakažených e-mailů najednou, a když je postižených schránek hodně… Jinými slovy, ochrana zpráv na serveru je možná, ale vyžaduje investice, investice, investice.

O něco lepší je situace se zabezpečeným přístupem. Jak práce s POP3 schránkou, tak i s webmailem je zašifrovatelná prostřednictvím standardních řešení obvyklých u jiných aplikací, ne všude se však používá.

### Čechy využívané freemaily

Na světě existuje mnoho freemailových serverů. Dá se však říct, že v Čechách je nejvyužívanějších jen několik z nich, převážně těch, které zde mají svou tradici, jež pocházejí z ČR, anebo je sem naopak úspěšně zaválo celosvětový věhlas. Jak jsou na tom tyto freemaily po stránce bezpečnosti, se podíváme v následující části.

Především je to schopnost vyčistit z pošty virovou/červovou nákazu. Následuje odstranění SPAMu a hned poté schopnost zabezpečit soukromí při samotné práci s poštou – tedy webmailu. Zajímavé také je, zda jsou tyto služby nabízeny již v základním, bezplatném provedení, nebo formou bonusu za příplatek, a také kolik takový příplatek činí.

## Co je dobré vědět

### Technologie e-mailu

**POP3** – Post Office Protocol slouží k vybírání pošty, tedy k jejímu přesunu mezi serverem, kde je uložena a klientským zařízením. Tím nemusí být pouze počítač, ale také například chytrý telefon, PDA, SetTop Box a další zařízení.

**SMTP** – Simple Mail Transfer Protocol slouží k odesílání pošty a jejímu doručení od odesílajícího serveru do poštovní schránky příjemce. Uživatel s ním přijde do kontaktu prakticky pouze tehdy, když nastavuje svůj poštovní program.

**Poštovní klient** – Program, který využíváme pro příjem a odesílání pošty. Samotný e-mailový klient je velmi jednoduchá záležitost, veškerý vývoj těchto programů se proto soustředí na pomocné funkce, které ulehčují jeho používání – adresář, formátování, kódování zpráv, jejich filtrování a podobně. Mezi nejrozšířenější poštovní klienty na platformě Windows patří aplikace Outlook Express, Microsoft Outlook v různých verzích, Mozilla Mail (Thunderbird) a několik dalších.

**WebMail** – Rozhraní, které umožňuje propojit e-mailový systém s uživatelským rozhraním nezávislým na klientovi. Jinými slovy, můžeme si poštu vybírat kdekoliv prostřednictvím webového prohlížeče, a stejně tak ji můžeme také odesílat. Webmail má oproti vybírání klientem několik výhod, ale také nedostatků. Mezi hlavní nedostatky patří problematická archivace zpráv, přidávání příloh, potíže s formátováním a další. Předností je univerzálnost. Funguje na všech kompatibilních prohlížečích, nepotřebujeme žádný program ani konkrétní typ operačního systému.

### Problematika e-mailu

**Začervení obsahu** – Většina současných červů, tedy škodlivých kódů používá pro své šíření e-mailové zprávy, které si automaticky odesílá z napadeného počítače na ukradené nebo i náhodné adresy. I když hlavním rozšiřovatelem červů je sám uživatel – otevře nakaženou přílohu – je nutné tyto červy z e-mailů nějakým způsobem čistit.

**SPAM** – Problém pomalu stejně podstatný jako začervení. SPAM, neboli nevyžádaná pošta, jsou e-mailové zprávy rozesílané hromadně jako propagace, reklama, nebo dokonce jako pokusy o podvod (slavným se stal například nigerijský dopis, lákající z nešťastných obětí peníze).

**Napadení** – POP3 komunikace není standardně žádným způsobem zabezpečena. To znamená, že prakticky kdokoliv může odposlouchat vaše heslo a pak vám zcizit obsah vaší e-mailové schránky, přečíst doručenou a nesmazanou nebo i odeslanou poštu. Pokud používáte webmail, je situace ještě nebezpečnější s ohledem na možnost „vykrást" heslo z prohlížeče pomocí speciálních programů nebo spywaru.

**Vymazání** – Standardní procedurou při práci s POP3 schránkou je její vymazání po dokončení stahování pošty. Když ale používáme webmail, chceme došlé zprávy také nějakou dobu uchovávat. Havárie serveru nebo jeho napadení mohou vyústit ve vymazání naší veškeré pošty, ztrátu dat a tedy i informací, které mohou být cenné.

### Nic není zadarmo

I když se freemaily tváří že nabízejí zcela bezplatné služby, je tomu tak již málokde. Prakticky se ukázalo, že reklama vkládaná do zpráv není tak účinná, jak se mnozí domnívali, a tak nezbývá než chtít po uživatelích peníze. Jen málokdy se tak děje přímým nátlakem, poskytovatelé však nabízejí za drobný poplatek „prémiové" služby. Větší místo, POP3, žádné reklamy, a někdy dokonce i bezpečnost. I v případě, že jejich nabídky nevyužijeme, platíme za provoz také. Reklamy, které jsou rozesílány uživatelům freemailů, jsou v českých podmínkách naštěstí dobře zvládnuté a přijatelné. Také komerční sdělení připojená na konec zpráv se dají přežít. To, co však komplikuje používání, jsou propagační plochy ve webmailovém rozhraní. V některých případech jsou příliš veliké a komplikují ovládání schránky při malém rozlišení, jindy zase využívají příliš rozměrné aktivní objekty (flash) a způsobují tak problémy u pomalejšího nebo datově počítaného připojení.

### Připlatit, či nepřiplatit?

Zamyslete se. Vadilo by vám, kdybyste od zítřka nemohli svou freemailovou adresu používat? Pokud ne, jelikož byste si založili jinou, nebo jich máte beztak dost, připlácet nemusíte. Pokud však ano, byl by to veliký problém, raději si připlatte. Dostanete nejen služby, které poskytovatel freemailu nabízí, ale hlavně mnohem lepší (i právní) záruku délky a kvality jeho služeb. Že nic takového není nutné si budete myslet jen do okamžiku, kdy nastane první podstatný problém.

# Přehled bezpečnosti na českých freemailových serverech

## Seznam E-mail ★★★★☆

*www.seznam.cz*

**Dobrá ochrana zadarmo, více místa za příplatek**

Seznam E-mail je pomocná služba portálu – rozcestníku Seznam.cz, v našich končinách nejrozšířenějšího. V minulosti, ale i v současnosti jsme se na něm mohli setkat s některými problémy s funkčností, především webmailové části, které by se mohly projevit i sníženou bezpečností (za určitých okolností dochází k chybám jeho interních komponent).

Základem zabezpečení Seznamu je implementace antivirového systému Nod32 společnosti ESET. Tento antivirus je ve své desktopové verzi velice kvalitní, a totéž platí i pro serverovou. Nedostatkem, se kterým se potýká, je ovšem včasnost aktualizace a také fakt, že ochranou čas od času nějaký nakažený e-mail projde. Řešením je v tomto případě zvýšená pozornost a samozřejmě lokální antivirový systém.

Ochrana před nevyžádanou poštou je u Seznamu provedena rovněž poměrně kvalitně. Nachází se, stejně jako antivirus, v základní nabídce (zpoplatněno je jen zvětšování velikosti schránky). Poskytuje základní odstraňování nevyžádané pošty, avšak není stoprocentní a poměrně nemalé procento spamu tímto filtrem bez potíží projde.

Zachycené zprávy jsou na serveru přesouvány po odstranění škodlivého kódu do speciální složky, přičemž je možné nastavit jejich automatické mazání. Je to velmi praktické a doporučujeme uživatelům si v nastaveních tuto volbu zapnout. POP3/SMTP přístup chráněn není, do SMTP serveru je třeba se přihlašovat, což má bránit zneužívání Seznamu pro rozesílání nevyžádané pošty. Drobným, avšak dobrým detailem je, že vám Seznam po přihlášení zobrazí umístění počítače, ze kterého jste se přihlásili naposledy, a také čas. Tím můžeme snadno odhalit možné zkompromitování hesla a změnit si je. Omezené je také použití kontrolní otázky pro obnovení hesla.

## MujMail ★★★☆☆

*mail.atlas.cz, www.atlas.cz*

**Dobrá ochrana zadarmo, nejasné řešení nevyžádané pošty**

Stejně jako je Seznam E-mail doplňkem portálu Seznam, je MujMail součástí konkurenčního Atlasu. Po funkční stránce nabízí prakticky totéž co Seznam, tedy webmail a implicitní možnost vybírat si poštu pomocí libovolného klienta. O ochranu pošty před infekcí se stará totožný systém jako v předchozím případě, tedy Nod32, v podání Atlasu však nabízí o něco lepší možnosti konfigurace, a to tři. První z nich je zavirované zprávy doručit po vymazání přílohy standardně do složky Doručené. Druhou možností je stejně jako v případě Seznamu přesouvat začervené zprávy po odčervení do speciální složky, která se zde jmenuje Karanténa, a třetí je tyto zprávy zlikvidovat úplně. Opět můžeme doporučit pouze třetí možnost.

Při přihlašování do webmailu Atlasu je využívána zabezpečená stránka, což je veliké plus tohoto systému. Snižuje se totiž riziko vykradení vašich přihlašovacích údajů, avšak zcela se neeliminuje. Systém přihlašování měl také v minulosti problémy s alternativními prohlížeči, jak se ale zdá, jsou již nyní zažehnány.

Co se ochrany před nevyžádanou poštou týče, Atlas žádný takový systém, na rozdíl od Seznamu, neuvádí. Faktem ovšem je, že adresy na něm nejsou právě pravidelně bombardovány nevyžádanou poštou, což je pozitivní. Celkově musíme říci, že také Atlas je zajištěn poměrně kvalitně.

## Post.cz ★★☆☆☆

*www.post.cz*

**Dobrá ochrana, ale je třeba si připlatit. V základní nabídce pouze před útokem a vykrádáním**

Post, momentálně pod hlavičkou Volného, poskytovatele připojení k internetu, patří nejen k nejstarším, ale také nejznámějším freemailů u nás a dodnes má množství přívrženců. Kromě zabezpečeného přihlašování nabízí možnost kontrolování IP adresy, což zvyšuje zabezpečení a snižuje možnost uživateli „ukrást" sezení, tedy stav, kdy je přihlášen a s e-mailem aktivně pracuje.

Po tomto, velice bezpečném začátku, však bude následovat studená sprcha. Jak antivirus, tak antispam systém obsahuje, bohužel za příplatek. Objednat si je možné obě služby odděleně (tedy zvlášť ochranu před červy i ochranu před nevyžádanou poštou), tak i balíček obsahující obě dvě. Pokud se rozhodnete pro kombinovanou ochranu a zároveň rozšíření e-mailové schránky na 25 MB, zaplatíte 60 Kč měsíčně včetně daně z přidané hodnoty. To je v porovnání s předchozími možnostmi pravda mnoho.

Dalším problémem Postu je konfigurační soubor. Program, který nastavuje stahování pošty, je v spustitelném souboru postcz.exe, a i když autoři prohlašují, že je bezpečný, je toto řešení v situaci, kdy se až příliš mnoho červů šíří podobným způsobem, přinejmenším pochybné.

## E-mail Centra ★★★☆☆

*www.centrum.cz*

**Dobrý nápad s agentem, zobrazení IP adresy, spamový filtr, horší antivirové řešení**

Dalším velkým portálem, často s agresivní propagací, je Centrum.cz. E-mail v rámci tohoto portálu se řadí rovněž k bezpečnějším. Nabízí http autentizaci, tedy možnost přihlašovat se pomocí přenosu jmen a hesel, který je založen na operačním systému a ne na webové stránce. To je určitým kladem.

Zajímavým řešením Centra.cz je takzvaný bezpečnostní agent. Tento chlapík v levém dolním rohu vašeho webmailu je ve výchozím nastavení deaktivován, ale po svém spuštění dohlíží na vaši bezpečnost. Pravidelně upozorňuje na potřebu změnit si heslo a na jeho složitost, přesněji na obtížnost odhadnutelnosti zadaného hesla.



Na dobré úrovni je antispamový filtr, který přesouvá nevyžádanou poštu do spamového koše. Umožňuje však nastavit výjimky – tedy adresy, ze kterých je povoleno přijímat i zprávy, jež by jinak byly vyhodnoceny jako nevyžádaná pošta.

Na dobré úrovni je také zobrazení poslední IP adresy a času přihlášení. To je užitečné v případě, kdy máte podezření, že vaše heslo někdo využívá a na e-mailové schránce parazituje.

Dobrou funkcí je v případě Centra možnost archivovat e-mailovou schránku do počítače. Bohaté nastavení umožňuje povolit nebo zakázat POP3 přijímání pošty a také spouštění nebezpečných příloh. Ty jsou však identifikovány na základě přípon, což zase tak dobré řešení není. Rovněž antispam je dobře konfigurovatelný a bezpečnostní agent je plusem.

## Email.cz ★★★☆☆

*www.email.cz*

**Zajímavé možnosti nastavení, nejasná antivirová ochrana, antispam zřejmě v testovací fázi, placený POP3.**

Freemail, který má svůj účel přímo v názvu. Základní funkcí je zobrazení typu prohlížeče na titulní straně serveru a možnost bezpečného přihlášení s využitím certifikátu, který si můžete nainstalovat. Server testuje IP adresu stejně a umožňuje tak zvýšit bezpečnost při práci s nim (jedná se o ochranu proti útoku).

Dobrým nápadem je využívat kromě přihlašovacího jména ještě uživatelský identifikátor (ID), který potřebujeme při obnovení ztraceného hesla.

Antispamové řešení je u e-mailu zatím v testovacím provozu. Je možné nastavit si příjem zpráv pouze od důvěryhodných e-mailových adres, které máte ve svém adresáři s tím, že lze definovat seznam výjimek. Dále zde funguje systém Spam Assasin, jenž likviduje nevyžádanou poštu na základě počítání jejího skóre. Otázku červů e-mail nijak extenzivně neřeší, avšak za poplatek si můžete aktivovat používání protokolu POP3, který je v jiných službách k dispozici zadarmo.

## Hotmail ★★★☆☆

*www.hotmail.com*

**Hotmail je dobrá služba, ale pokud si za ni zaplatíte. Provázaná s .Net Passportem, což není ideální, avšak zabezpečená kvalitním antivirem.**

Hotmail je tradiční službou Microsoftu postavenou na moderních technologiích. Přihlašování se děje pomocí služby .Net Passport. Je při tom používáno zabezpečené připojení na bázi SSL, tedy s použitím standardní technologie. Bezpečnostní řešení pochází od společnosti McAfee Security. Červy jsou chytány s poměrně dobrou precizností.

Otázka nevyžádané pošty je řešena několika způsoby. Předně, existuje zde možnost hlásit provozovateli serveru podezřelé e-mailové adresy, které jsou následně blokovány. Další možností je nastavení filtru automatického mazání zpráv ze závadných adres, ale komplexní antispamové řešení v podání Microsoftu bohužel neexistuje.

Problémem je také využití .NET Passportu. I když je tato služba bezpečná, je velmi provázaná s počítačem a dalšími službami. To znamená, že prolomení jednoho účtu představuje riziko pro několik dalších služeb. Bezplatná verze také rychle expiruje, podmínky jejího používání jsou podezřelé (provozovatel může promazávat uživatelovu poštovní schránku) a odstranění těchto omezení vás bude stát 32 eur ročně.

### Závěrem

Ze serverů, které jsme zde uvedli, bychom korunu krále dali s největší pravděpodobností Seznamu, následovanému Atlasem. Ze služeb, za které je třeba si připlatit, stojí za zmínku Post a Email, placený Hotmail najde v našem prostředí zřejmě menší využití. 4 0263/FEL ❑