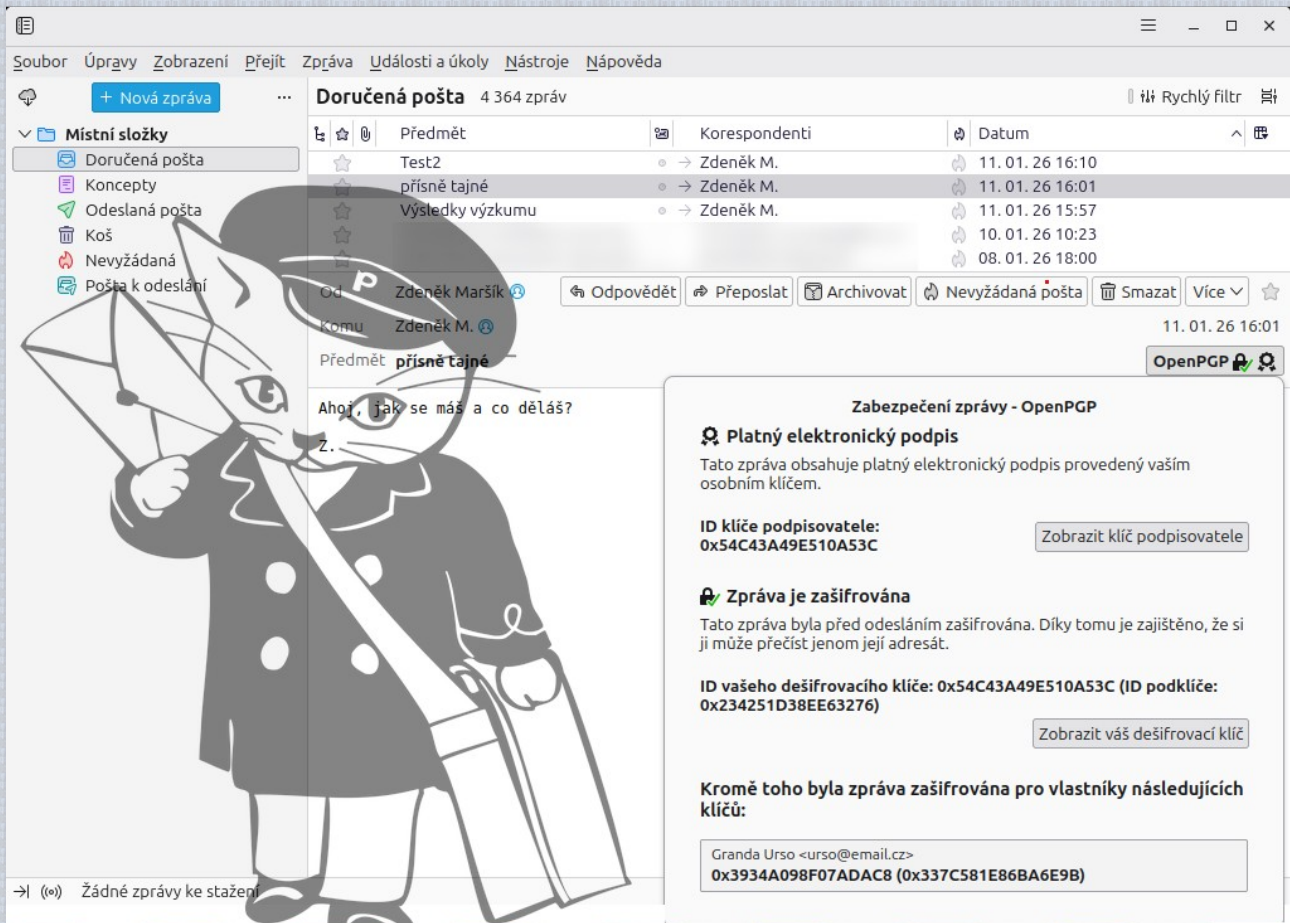


# Elektronická pošta a soukromí

Zdeněk Maršík



Soubor Úpravy Zobrazení Přejít Zpráva Události a úkoly Nástroje Nápověda

+ Nová zpráva ... Doručená pošta 4 364 zpráv Rychlý filtr

Místní složky

- Doručená pošta
- Koncepty
- Odeslaná pošta
- Koš
- Nevyžádaná
- Pošta k odeslání

Předmět	Korespondenti	Datum
Test2	→ Zdeněk M.	11. 01. 26 16:10
přísně tajné	→ Zdeněk M.	11. 01. 26 16:01
Výsledky výzkumu	→ Zdeněk M.	11. 01. 26 15:57
		10. 01. 26 10:23
		08. 01. 26 18:00

Od Zdeněk Maršík  
Komu Zdeněk M.  
Předmět **přísně tajné**

Ahoj, jak se máš a co děláš?  
Z.

Zabezpečení zprávy - OpenPGP

**Platný elektronický podpis**  
Tato zpráva obsahuje platný elektronický podpis provedený vašim osobním klíčem.

ID klíče podpisovatele: 0x54C43A49E510A53C [Zobrazit klíč podpisovatele](#)

**Zpráva je zašifrována**  
Tato zpráva byla před odesláním zašifrována. Díky tomu je zajištěno, že si ji může přečíst jenom její adresát.

ID vašeho dešifrovacího klíče: 0x54C43A49E510A53C (ID podklíče: 0x234251D38EE63276) [Zobrazit váš dešifrovací klíč](#)

Kromě toho byla zpráva zašifrována pro vlastníky následujících klíčů:

Granda Urso <urso@email.cz>  
0x3934A098F07ADAC8 (0x337C581E86BA6E9B)

Ahoj Petře,

posílám Ti citlivé informace o tom, že agent Pávek chce být prezidentem. K tomu mu sekunduje agent Bureš.

S pozdravem

Karel



Takto lehce vidí poskytovatel emailu a další sledovací agentury  
vaši korespondenci na free emailech gmail, seznam ap.  
Takto si představují "listovní tajemství".

Nenechte se sledovat, použijte dopisní obálku!

**ZDARMA**



Pan

Petr Josef

Na Příkopě 2456

PRAHA 5

111 50



(ne)bezpečná emailová komunikace

# Obsah

I. ÚVODEM.....	7
1. Předmluva.....	7
2. Důvod vzniku této publikace.....	7
3. Je tu cenzura?.....	8
II. VZNIK ELEKTRONICKÉ KOMUNIKACE, NAROZENÍ EMAILU.....	9
1. Jak vznikl email.....	9
2. Co je to email zdarma (freemail).....	9
3. Firemní a podnikatelské emaily.....	9
4. Způsob používání, čtení a odesílání emailů.....	10
a) Webmail - používání emailové schránky přes webové rozhraní.....	10
b) Emailový klient.....	10
5. Používání emailů na různých zařízeních.....	11
III. ELEKTRONICKÁ POŠTA (EMAIL) A SOUKROMÍ.....	12
1. Kde všude se používá email.....	12
2. Je obsah emailů chráněn?.....	12
3. Kdo může číst email.....	13
4. Lze u emailu zajistit soukromí?.....	13
5. Jak velkou míru soukromí si zajistíme?.....	15
a) Emailový klient Thunderbird.....	15
b) Emailový klient Claws Mail.....	15
c) K-9 Mail s Openkeychain.....	15
d) Webmail Proton Mail.....	15
IV. ZAJIŠTĚNÍ SOUKROMÍ U EMAILU.....	16
1. Základní přehled šifrování.....	16
2. Symetrická kryptografie.....	16
3. Asymetrická kryptografie.....	17
a) Dvojková soustava, 8 bitový klíč, 7 bitový přenos.....	19
b) Jak velké klíče se v asymetrické kryptografii používají.....	19
c) Hexadecimální čísla - šestnáctková soustava.....	19
V. SOFTWARE GNUPG - ŠIFROVÁNÍ A DIGITÁLNÍ PODPIS.....	21
1. Proč vlastně šifrovat e-maily?.....	21
2. Seznam nejpoužívanějších příkazů gpg (GnuPG).....	23
a) Vytvoření páru OpenPGP klíčů = osobní klíč.....	23
b) Další gpg příkazy.....	24
Ověření souboru s odděleným elektronickým podpisem.....	24
3. Co znamenají zkratky ve výpisu veřejných klíčů.....	29
4. Identifikátory OpenPGP klíče.....	29
5. TOFU (Trust On First Use) – důvěřuj při prvním užití.....	31
6. Kleopatra - grafická správa klíčů.....	31
7. Používání šifrování v OpenPGP standardu.....	31
8. Síť důvěry (web of trust) OpenPGP klíčů.....	31
9. Příklady použití GPG.....	32
VI. BEZPEČNÁ EMAILOVÁ KOMUNIKACE NA NOTEBOOKU A PC.....	35
1. Emailový klient Mozilla Thunderbird.....	35
a) Nastavení emailového klienta Thunderbird.....	35
Nastavení v Thunderbirdu.....	36
b) Nastavení šifrování v Thunderbirdu.....	37
Vytvoření páru klíčů (osobního klíče).....	38
První šifrovaný email.....	39
Správce klíčů v Thunderbirdu.....	41

c) Zálohování OpenPGP soukromého klíče v Thunderbirdu.....	42
d) Co Thunderbird zašifrovat (digitálně podepsat) neumí.....	43
e) Před čím nás Thunderbird s koncovým šifrováním neochrání.....	43
2. Emailový klient Claws Mail.....	44
a) Nastavení emailového klienta Claws Mail.....	44
b) Nastavení šifrování v emailovém klientu Claws Mail.....	45
3. Proton Mail - freemail se zaměřením na bezpečnost.....	47
a) Stažení prohlížeče TOR.....	47
b) Vytvoření účtu na Proton Mail.....	48
c) Proton VPN.....	49
d) Nastavení skriptů pro OpenVPN.....	50
e) Přihlášení do OpenVPN.....	51
f) Zabránění úniku DNS (DNS leak) na firewallu.....	53
g) Zabránění úniku WebRTC (WebRTC Leak).....	54
VII. BEZPEČNÁ EMAILOVÁ KOMUNIKACE NA MOBILECH.....	55
1. Proč na mobilu zabezpečit elektronickou komunikaci.....	55
2. Emailový klient k-9 Mail s OpenKeychain.....	55
a) K-9 Mail - emailový klient pro mobily.....	55
b) OpenKeychain - správce klíčů pro mobily.....	56
Vytvoření páru klíčů pomocí OpenKeychain.....	56
Potvrzení pravosti klíčů.....	57
Základní identifikátory klíčů.....	58
Záloha tajného klíče.....	59
Obnova osobního klíče (páru klíčů), tajného klíče ze zálohy.....	59
c) Zapnutí podpory OpenPGP v K-9 mailu.....	60
3. Zabezpečení emailů s webmailem Proton Mail.....	60
Orbot - TOR pro mobily.....	61
VIII. ZÁVĚR.....	62
IX. ODKAZY A ZDROJE.....	63

# I. ÚVODEM

## 1. Předmluva

Autor této knihy se věnuje již přes 30 let programování, správě počítačových sítí, tvorbě webových aplikací, kyberbezpečnosti, šifrování a bezpečné komunikaci na nezabezpečených kanálech. Zabývá se vývojem aplikací ve VISUAL OBJEKT PASCAL (LAZARUS), PHP s MariaDB (MySQL), instalací operačních systémů Linux pro servery i pracovní stanice s důrazem na bezpečnost. Přes SSH (dálkově) nainstaloval chráněný linuxový webserver (DEBIAN) se šifrovaným podkladovým zařízením (LUKS), vytvořil firewall a pak na tom serveru vytvořil mezinárodní klientský portál v PHP nad MariaDB databází pro obchodníky s akcemi v 8 jazycích.

## 2. Důvod vzniku této publikace

Od nepaměti se nějaká moc snažila buď informace utajovat nebo naopak utajované informace získávat. Popřípadě se vymýšlely způsoby bezpečného přenosu informací. Jako kuriozitu lze uvést, že byla kurýrům na oholenou hlavu napsána informace, kterou pěšky přenášeli například 5 000 kilometrů. Než takovou vzdálenost takový kurýr ušel, hlava mu pěkně obrostla vlasy a tím byla zpráva utajená. Pro přečtení takové zprávy u cílového adresáta stačilo kurýrovy oholit hlavu. V nedávné minulosti bylo šifrování využíváno hlavně špióny nebo armádou.

Těžkou ranou do soukromí, o kterém se veřejnost dozvěděla, byl přísně tajný program Agentury národní bezpečnosti (NSA) [XkeyScore](#)<sup>1</sup>, který analytikům umožňuje, aby bez jakékoliv předchozí autorizace procházeli rozsáhlými databázemi e-mailů, on-line chatů a historií prohlížení internetu milionů lidí, tvrdí dokumenty poskytnuté Edwardem Snowdenem již v roce 2013. NSA se ve výukových materiálech k tomuto programu zvanému XKeyscore chlubí, že je to její systém s „největším dosahem“ k rozvoji rozvědky z internetu.

V současnosti (začátek r. 2026) je v rámci „národní bezpečnosti“ nebo boje proti kriminalitě zvýšené riziko ohrožení soukromí běžných občanů. Dokonce EU v dubnu 2026 má schválit tzv. „[Chat Control](#)“ (CSAM - child sexual abuse material) na chatových aplikacích a online službách, má sice chránit děti, ale otevírá dveře k novým pravidlům pro skenování obsahu uživatelů. Argument, že jsme všichni potencionální zločinci a proto se budou prohlížet a skenovat zprávy všech, nemůže obstát. Přitom **poslat email je jako poslat pohlednici**, kdy všichni, okolo koho email zrovna letí, uvidí co jste psali (Obsah zpráv je snadno snadno přístupný vašemu poskytovateli emailové schránky, poskytovateli internetu ISP nebo systémům pro hromadné sledování XKeyscore, PRISM, UKUSA, ECHELON - pět očí). A přesto lidé posílají emailem důležité soukromé zprávy i dokumenty (zdravotní dokumentaci, kupní smlouvy, notářské zápisy, výsledky výzkumu, faktury...).

Soukromí je osobní oblast člověka, jednotlivce nebo skupiny lidí (například rodiny). Zahrnuje potřebu a právo chránit informace o své osobě, jakož i vlastní tělo a čas, vlastní prožitky a území před zveřejňováním a především před zneužíváním. Jde o jedno ze základních, neporušitelných a nezcizitelných lidských práv a svobod a jako takovému mu náleží patřičná ochrana.

Správci klíčových systémů sice musí zabezpečit své e-mailové schránky podle doporučení „Národního úřadu pro kybernetickou a informační bezpečnost“<sup>38</sup>, ale to se netýká běžných občanů.

Cílem této publikace je ukázat na **nedostatečnou ochranu soukromí** u elektronické komunikace, jak ji zdarma dostat na výbornou úroveň se statusem „**chráněná komunikace**“, jak odstranit další problémy u nechráněné komunikace.

Vážená paní Nováková,


dostavte se 12.8. laskavě ke gynekologickému vyšetření na léčení pohlavní nemoci - chlamidióza.

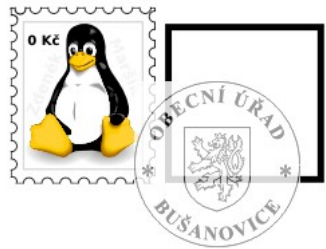
MUDr. Pan Pan

*Takto lehce vidí poskytovatel emailu a další sledovací agentury vaši korespondenci na free emailech gmail, seznam ap. Takto si představují "listovní tajemství".*

**Nenechte se sledovat, použijte dopisní obálku!**

**ZDARMA**





Paní \_\_\_\_\_  
 Jana Nováková \_\_\_\_\_  
 Celetná 2323 \_\_\_\_\_  
 PRAHA \_\_\_\_\_  
 111 50

Obrázek 1: Nešifrovaná elektronická pošta (email) je jako pohlednice

Neobstojí argument, že **nemám co skrývat**, tak se není čeho bát<sup>2</sup>.

### 3. Je tu cenzura?

V únoru 2022 bylo zamknuto osm tuzemských (dezinformačních?) webů. Byla to ve všech ohledech velmi neobvyklá situace. Stát podle zákona může nařídít vypnout jen takové stránky, které porušují zákon. Šířit lži, nesmysly a dezinformace ale v drtivé většině případů trestné není. Ministerstvo obrany proto dopisem sdužení CZ.NIC, které tuzemské domény spravuje, o jejich dočasné vyřazení z provozu požádalo. To vyhovělo, a osm stránek, mezi nimi i známé adresy jako Aeronet či Protiproud, nebylo do května roku 2022 k dosažení.

**Tady je třeba poukázat na tyto skutečnosti dle ústavy ČR:**

1. Svoboda projevu a právo na informace jsou zaručeny.
2. Každý má právo vyjadřovat své názory slovem, písmem, tiskem, obrazem nebo jiným způsobem, jakož i svobodně vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na hranice státu.
3. Cenzura je nepřípustná.



**ÚSTAVA ČESKÉ REPUBLIKY**  
 LISTINA ZÁKLADNÍCH PRÁV A SVOBOD  
 Politická práva



#### Článek 17

(1) Svoboda projevu a právo na informace jsou zaručeny.

(2) Každý má právo vyjadřovat své názory slovem, písmem, tiskem, obrazem nebo jiným způsobem, jakož i svobodně vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na hranice státu.

(3) Cenzura je nepřípustná.

## II. VZNIK ELEKTRONICKÉ KOMUNIKACE, NAROZENÍ EMAILU

### 1. Jak vznikl email

Elektronická pošta, zkráceně e-mail [ímejl] nebo jen email, mail. Email (resp. textová komunikace mezi uživateli) je ve skutečnosti starší než Internet. E-mail v Internetu (tak jak ho známe dnes) má počátek v roce 1971 (zavedení znaku @) a ve standardu RFC 821 pro přenos elektronické pošty protokolem SMTP, který byl vydán v roce 1982. K masívnímu používání elektronické pošty (emailu) došlo až zpřístupnění volných emailových služeb hotmail v r. 1996. Takové emaily měly tvar například: `katexina.novakova@usa.net`.<sup>3</sup>

V českých zemích později začali nabízet emailové služby zdarma „centrum“, „atlas“, „seznam“ a další.

Pamatujte, že emailová komunikace není bezpečná kvůli několika klíčovým rizikům. Hlavní problém spočívá v tom, že **emaily nejsou koncově šifrované**, což znamená, že mohou být snadno zachyceny útočníky třetích stran. Navíc zpráva může být přečtena někým jiným než zamýšleným příjemcem, zejména při odesílání na více adres najednou. Emaily **nejsou ani elektronicky podepsány**, takže **skutečný odesílatel je nejistý**.

### 2. Co je to email zdarma (freemail)

Email zdarma (freemail) je služba, kterou poskytují provozovatelé za účelem možnosti zřízení emailu pro běžné uživatele (domácnosti). Pro firmy, podnikatele, obce, státní správu, příspěvkové organizace a další, kteří si platí doménu a webhosting, obvykle poskytovatel webhostingu umožňuje také zřízení podnikových poštovních (emailových) schránek. Takovou obecní poštovní schránku poznáme podle **domény druhého řádu**, která je většinou stejná, jako internetová adresa. Například Brno má internetové stránky: `https://www.brno.cz/` (www se už zadávat nemusí). Emailová adresa pro informace je: `informace@brno.cz`. Doména II. řádu je: `brno.cz`. **Z toho vyplývá, že kdo má svoje webové stránky, internetovou prezentaci na své doméně II. řádu, má možnost také používat svůj email, např.** `josef.novak@stavebniny.cz`. Přesto tito drobní řemeslníci většinou používají freemail od seznamu přes webové rozhraní `www.seznam.cz` s konzumací množství reklam a souhlasem s poskytováním osobních údajů třetím stranám.

**U emailu zdarma si doménu vybírat nemůžeme**, musí se používat ta z registrace u poskytovatele emailu zdarma (freemailu), např. `frantisek.dobrota@seznam.cz`.

Do roku 2026 jsou největší poskytovatele emailu zdarma Seznam, Centrum, Proton Mail, Tuta Mail, Microsoft Outlook, Google Mail, Yahoo Mail. Tito poskytovatelé nabízejí dvě metody přístupu k emailům přes webové rozhraní i pomocí emailového klienta.

Podle výše uvedeného vyplývá, že **freemaily jsou určeny pouze pro studenty, běžné občany a domácnosti**.

### 3. Firemní a podnikatelské emaily

Jak už bylo výše zmíněno, firmy, podnikatelé, státní a obecní správa mají svoje internetové stránky i svoje emailové schránky. Také téměř výhradně **používají emailového klienta** jako je MS outlook, Thunderbird, Kmail, Clawsml, Evolution a další.