

Jak na bezpečný e-mail?

PGP pro všechny!

—
Anarchistický Černý Kříž / NoLog.cz



NOLOG
CZ ★

Základ: důvěryhodný poskytovatel

- Váš poskytovatel e-mailu vidí kdy a komu jste co posílali a kdo co posílal vám
 - Pokud není e-mail šifrovaný vidí i jeho obsah
- Proto: vyhněte se komerčním poskytovatelům
 - např. Gmail, Seznam.cz apod.
- Jakého poskytovatele vybrat?
 - Riseup.net
 - Autistici.org
 - Systemli.org



Co je to PGP?

- “Pretty Good Privacy”
- Způsob šifrování dat (nejen e-mailů)
- Jak funguje?
 - Veřejný klíč – tím vaši kamarádi*ky mohou zprávu zašifrovat (veřejný klíč si můžete dát na web a rozdávat ho jak je libo)
 - Soukromý klíč – tím zprávu můžete dešifrovat nebo podepsat (soukromý klíč nikdy nesmí opustit váš počítač!)

Potřebuji PGP, když mám e-mail u Riseupu?

- Riseup.net nikdy data uživatelů*ek nevydal
- Přesto je lepší PGP používat
- PGP umožňuje poslat “bezpečný e-mail” i lidem, kteří u Riseupu nejsou (pokud také používají PGP)

Jak PGP používat?

- Thunderbird + Enigmail
- Thunderbird
 - E-mailový klient
 - Více e-mailových schránek na jednom místě
 - Bezpečnější než webové rozhraní
- Enigmail
 - Doplněk do Thunderbirdu, který umožňuje používat PGP



Další možnosti: ProtonMail.com

- ProtonMail.com
 - E-maily posílané mezi účty na ProtonMailu jsou automaticky šifrované
 - Používání je jednodušší, než nastavování Thunderbirdu + Enigmail
 - Jde o komerční službu (základní účet je zdarma, větší úložiště atp. zpoplatněno)
 - Další zpoplatnění je poměrně drahé



Další možnosti: Tutanota.com

- Tutanota.com
 - Podobná služba jako ProtonMail.com
 - Také zdarma, ale také komerční
 - Zpoplatněné funkce jsou levnější
 - Narozdíl od ProtonMailu některé funkce chybí



Co dál?

- Pokud vám Policie sebere počítač, PGP vám nepomůže
 - Nastavte si šifrování disku na každém zařízení, které používáte
- Dodržujte ostatní zásady bezpečnostní kultury
 - PGP vám nepomůže, když vás usvědčí odposlech atp.

Odkazy

- <https://emailselfdefense.fsf.org/cs/>
- <https://ssd.eff.org/en/module/how-use-pgp-linux>
- <https://ssd.eff.org/en/module/how-use-pgp-mac-os-x>
- <https://ssd.eff.org/en/module/how-use-pgp-windows>