Ochrona przed inwigilacją poczty elektronicznej

Masowa inwigilacja łamie podstawowe prawa człowieka i jest poważnym zagrożeniem dla wolności słowa!
Na szczęście, możemy się przed nią bronić.

Problem

Hasło zabezpieczające Twoją pocztę elektroniczną nie jest wystarczające, aby ochronić ją przed technologiami masowej inwigilacji używanymi przez służby wywiadowcze.

Każdy e-mail wysyłany przez Internet przechodzi przez wiele komputerów zanim trafi do odbiorcy. Służby specjalne i agencje wywiadowcze wykorzystują to, przechwytując miliony wiadomości każdego dnia.

Nawet jeśli sądzisz, że sam nie masz nic do ukrycia – pamiętaj: narażasz na niebezpieczeństwo wszystkich ludzi, z którymi komunikujesz się za pomocą niezaszyfrowanych e-maili.

Szyfrowanie

Odzyskaj prywatność za pomocą GnuPG! GnuPG szyfruje Twoje e-maile jeszcze przed wysłaniem, więc tylko wybrani przez Ciebie odbiorcy mają dostęp do ich zawartości.

GnuPG działa na wszystkich platformach. Możesz go używać z dowolnym adresem e-mail, na każdym komputerzy czy smartfonie. GnuPG jest wolne, otwarte i bezpłatne.

Tysiące ludzi korzystają z GnuPG zarówno do celów zawodowych jak i prywatnych. Dołącz do nas! Każda osoba wzmacnia naszą społeczność i pokazuje, że jesteśmy w stanie sprzeciwić się inwigilacji.

Rozwiązanie

Gdy e-mail zaszyfrowany z użyciem GnuPG zostanie przechwycony i wpadnie w niepowołane ręce, będzie wyglądał jak niezrozumiały ciąg znaków. Bez odpowiedniego klucza prywatnego nie da się go odczytać. Dla docelowego odbiorcy jednak, i tylko dla niego, będzie to najzwyklejsza wiadomość.

W ten sposób zarówno nadawca, jak i odbiorca są znacznie bezpieczniejsi. Nawet jeśli Twoje e-maile nie zawierają poufnych informacji, konsekwentne używanie szyfrowania chroni nas wszystkich przed nieuprawnioną inwigilacją.

Prywatna poczta elektroniczna

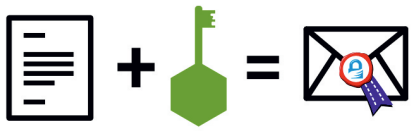
Odzyskaj swoją prywatność!
Używaj GnuPG!

- Wolne Oprogramowanie
- dla wszystkich adresów e-mail
- na GNU/Linuksa, Windowsa, Maca, Androida, ...
- nie wymaga posiadania konta ani rejestracji w żadnym serwisie
- całkowicie bezpłatne

Jak działa GnuPG

Aby zacząć używać szyfrowania GnuPG, należy stworzyć unikalną parę „kluczy" - prywatny i publiczny.
Kluczy używamy w następujący sposób:

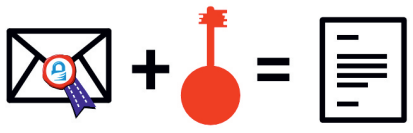
klucz publiczny



do szyfrowania

Kiedy ktoś chce wysłać Ci zaszyfrowanego e-maila, musi skorzystać z Twojego klucza publicznego. Im więcej osób zna twój klucz publiczny, tym lepiej.
Nie martw się: klucz publiczny może jedynie szyfrować wiadomości do Ciebie. Nie da się nim niczego odszyfrować.

klucz prywatny



do odszyfrowywania

Twój klucz prywatny jest jak klucz do frontowych drzwi Twojego domu; należy przechowywać go w bezpiecznym miejscu, jedynie na własnym komputerze. Powinieneś być jedyną osobą, która ma do niego dostęp!
Klucza prywatnego używamy do odszyfrowywania i czytania e-maili, które nadawca zaszyfrował Twoim kluczem publicznym.

Co sprawia, że GnuPG jest bezpieczne?

GnuPG jest **Wolnym Oprogramowaniem** używającym **Otwartych Standardów**, co pozwala mu naprawdę chronić przed inwigilacją. W przypadku zamkniętych formatów i własnościowego oprogramowania proces szyfrowania jest poza kontrolą użytkownika.

Jeżeli nikt nie jest w stanie obejrzeć kodu programu, nie ma żadnej pewności, czy nie zawiera on oprogramowania szpiegowskiego – tzw. „tylnych furtek". Jeżeli oprogramowanie nie działa jawnie, możemy mu co najwyżej ślepo zaufać. Jednym z podstawowych założeń Wolnego Oprogramowania jest właśnie ujawnienie kodu źródłowego: Wolne Oprogramowanie umożliwia i zachęca wszystkich użytkowników do przeprowadzania niezależnych inspekcji i testów kodu. To właśnie ta przejrzystość kodu pozwala na wykrywanie i usuwanie tylnych furtek.

Większość Wolnego Oprogramowania pozostaje pod opieką społeczności dbającej o bezpieczeństwo wszystkich użytkowników. Jeżeli chcesz uchronić się przed inwigilacją, Wolne Oprogramowanie pozostaje jedyną opcją.

Czym jest Wolne Oprogramowanie

Wolne Oprogramowanie może być użyte przez każdego, w dowolnym celu. Każdy może je kopiować, ulepszać, dopasowywać do swoich potrzeb i czytać kod źródłowy.Są to tzw. „cztery wolności".

Nawet, jeżeli chcesz „po prostu używać" programu, wciąż odnosisz korzyści z tych wolności. Dają Ci one gwarancję, że Wolne Oprogramowanie pozostaje pod opieką społeczności i jego dalszy rozwój nie zależy od interesów prywatnych firm czy rządów.

Aby dowiedzieć się więcej na temat Wolnego Oprogramowania i Wolnego Społeczeństwa, odwiedź:

fsfe.org/freesoftware

Porady praktyczne

Technologia wykorzystana w GnuPG stanowi najwyższej klasy zabezpieczenie, jednak niewiedza i nieostrożność użytkownika wciąż mogą spowodować ujawnienie poufnych informacji. Poniższe wskazówki pomogą Ci zachować pełną kontrolę nad szyfrowanymi treściami:

Aby odszyfrować wiadomość potrzebujesz swojego klucza prywatnego oraz **bezpiecznego hasła**. Hasło powinno być złożone z co najmniej 8 znaków i zawierać cyfry, znaki specjalne oraz wielkie i małe litery. Ponadto, nikt nie powinien być w stanie odgadnąć Twojego hasła, nawet znając Ciebie i Twoje zainteresowania.

Stwórz kopię zapasową swojego klucza prywatnego! Dzięki temu w przypadku awarii dysku twardego nie będziesz musiał tworzyć nowego i nie stracisz dostępu do danych zaszyfrowanych utraconym kluczem.

Szyfruj tak dużo wiadomości, jak to możliwe! W ten sposób stworzysz szum uniemożliwiający rozpoznanie, które informacje są naprawdę ważne. Im częściej szyfrujesz, tym mniej podejrzana będzie każda zaszyfrowana wiadomość.

Pamiętaj, że **temat wiadomości nie jest szyfrowany!**

Przewodnik

Pod tym adresem można znaleźć prosty przewodnik o zabezpieczaniu swoich e-maili za pomocą GnuPG:

EmailSelfDefense.FSF.org

Możesz też wziąć udział w jednym z tzw. **„CryptoParty"** w swojej okolicy. Są to spotkania, na których możesz bezpłatnie dowiedzieć się więcej na temat szyfrowania i znaleźć pomoc w odpowiedniej konfiguracji swojego komputera do korzystania z GnuPG i innych narzędzi szyfrujących.

2016-04-04

O FSFE

Ta ulotka została stworzona przez Free Software Foundation Europe (FSFE), organizację non-profit mającą na celu promocję Wolnego Oprogramowania i budowanie wolnego społeczeństwa cyfrowego.

Dostęp do oprogramowania określa jak możesz brać udział w życiu społecznym. Mając to na uwadze, FSFE działa na rzecz równego dostępu do technologii i kultury dla wszystkich, walcząc o cyfrową wolność.

Nikt nie powinien być zmuszany do używania oprogramowania, które nie daje wolności **korzystania z niego, dzielenia się nim, badania i ulepszania go**. Powinniśmy móc kształtować technologię wedle naszych potrzeb.

Działalność FSFE wspierana jest przez społeczność osób, dla których ważne są te wartości. Jeżeli chciałbyś przyłączyć się do nas albo pomóc nam w dążeniu do tych celów, możesz to zrobić na wiele sposobów, niezależnie od swoich umiejętności. Więcej informacji znajdziesz na stronie:

fsfe.org/contribute

Zostań członkiem!

Dotacje pozwalają nam kontynuować pracę i utrzymywać całkowitą niezależność. Możesz wesprzeć naszą pracę, stając się Członkiem Stowarzyszonym FSFE. Opłacając składkę członkowską bezpośrednio pomagasz w promocji i edukacji o Wolnym Oprogramowaniu w Europie.

fsfe.org/join

Możesz zamówić tę i inne ulotki za darmo:

fsfe.org/promo

Free Software Foundation Europe e.V.
Schönhauser Allee 6/7
10119 Berlin
Germany
https://fsfe.org