

Fél, hogy lehallgatják a levelezését? Itt egy bombabiztosnak tűnő védelem

Egyelőre még bétás a Ciphertext fejlesztése, de már a tesztverziót is bárki próbálgathatja, aki nem Windowst használ. Utóbbira ugyanis kis késéssel érkezik.



Mindenekelőtt szögezzük le: nincs tökéletes védelem. Ha valaki nagyon belemélyed, szinte bármelyik rendszerben talál gyenge pontokat. Igaz ez a titkosítási megoldásokra is. Ez azonban nem érv a titkosítás használata ellen, hiszen már az is elrettentő lehet, ha egy információhoz csak túlságosan nagy erőfeszítés árán lehet hozzáférni.

Tehát szögezzük le gyorsan azt is: ha valaki fél, hogy lehallgatják a levelezését, használjon valamilyen titkosító eszközt. Például a Ciphertext legújabb fejlesztését. (A cég – és a szolgáltatás –

neve valószínűleg nem csak a titkosított szövegre, hanem a *Dan Brown* híres regényében, A Da Vinci-kódban szereplő, titkos információt rejtő tárgyra, a Cryptexre is utal, ami a Wikipedia szerint Brown leleménye.)

Az a biztos, ha nálunk a kulcs

A New York-i székhelyű Ciphertext abból próbál üzleti csinálni, hogy megbízható titkosítást kínál a felhasználók adataihoz. Maga a cég 2014-ben alakult, és kezdetben a Gmailhez fejlesztett titkosító kiegészítőt. Az akkori koncepciót fejlesztették tovább önálló szolgáltatássá.

A szakértők egyetértenek abban, hogy a legbiztosabb védelmet az adja, ha a titkosító kulcs a felhasználónál van, mert így a szolgáltatónak sincs lehetősége belenézni a rajta átfolyó adatokba. Ezt a módszert használja a Lavabit, a Wickr vagy az olyan népszerű alkalmazások, mint a WhatsApp, és ehhez az eszközhöz nyúlt a Silent Circle is – hogy csak néhány példát említsünk. (Ez a titkosítási mód persze kettős fegyver, mint azt a Telegram tavalyi esete mutatja, hiszen a bűnözőknek is eszközt ad a kezébe.)

Forrás: <https://bitport.hu/fel-hogy-lehallgatjak-a-levelezeset-itt-egy-bombabiztosnak-tuno-vedelem>

Válogatta: Fonyó Istvánné