CANADIAN JOURNALISTS FOR FREE EXPRESSION

ÚJSÁGÍRÓK VÉSZHELYZETBEN

MIT TEHETÜNK DIGITÁLIS BIZTONSÁGUNKÉRT?

ÚTMUTATÓ

Független Médiaközpont
2017

ÚJSÁGÍRÓK VÉSZHELYZETBEN

Ezt az útmutatót az Open Technology Fund támogatásával készítette a Kanadai Újságírók a Szólásszabadságért (Canadian Journalists for Free Expression, CJFE) szervezete, amely hozzájárult ahhoz, hogy a Független Médiaközpont magyar nyelvre lefordítsa és publikálja. A CFJE segítségét ezúton is köszönjük.

www.cjfe.org/journalists_in_distress_securing_your_digital_life

© 2017 Független Médiaközpont
Felelős kiadó: MÓRICZ ILONA igazgató, Független Médiaközpont
1064 Budapest, Vörösmarty u. 47/a.
Telefon: (36) 1 609 5392 • E-mail: cij@cij.hu • Web: www.cij.hu
Fordította és szerkesztette: ORBÁN SÁNDOR
Design és tördelés: GALICZ KRISZTIÁN, typiART

A kiadvány megjelenését a Nyílt Társadalom Intézet Alapítvány támogatta.

Az új médiatechnológiák alkalmazása rendkívül fontossá vált az újságírói munkában. Ugyanakkor egyre több digitális eszköz és platform áll rendelkezésre az újságírók ellehetetlenítésére. Ilyen a megfigyelés, a személyazonosítás, illetve a zaklatás, amely a kormány vagy az államgépezettől független szereplők részéről is érheti az újságírókat. A zaklatás elleni védekezés része a fizikai biztonság garantálása mellett ma már a digitális biztonság is. Az online tevékenységbe történő beavatkozás ugyanis az újságírók életét is veszélybe sodorhatja.

A munkájuk miatt üldözött újságírók gyakran kérnek támogatást olyan szervezetektől, amelyek különböző országokban működtetnek segélyprogramokat. Ha újságíróként veszélyes helyzetbe kerülünk, ismernünk kell a digitális biztonsági kockázatokat, amikor ezekkel a szervezetekkel kapcsolatot keresünk! A kapcsolatfelvétellel járó rizikó mérséklése egyben általános digitális biztonságunkat is erősíti.

A továbbiakban olyan információkat és tanácsokat osztunk meg, amelyek hozzájárulhatnak ahhoz, hogy az újságírók biztonsága erősödjön, valamint csökkenjen digitális kitettségük, amelyet az állam képviselői vagy az államgépezettől független szereplők is kihasználhatnak.

Az útmutató külön információkat tartalmaz azok számára is, akik újságírókat segítő szervezetekkel kívánják felvenni a kapcsolatot. Ennek célja, hogy elkerülhetők legyenek a további, még nagyobb biztonsági kockázatok. Ha már kapcsolatba léptünk ilyen szervezettel, és pusztán a digitális biztonság erősítésének egyszerű, általános, de fontos lépéseiről szeretnénk tájékozódni, ez az útmutató segít abban, hogy jobban megértsük azt a kockázatot, amelyet a digitális eszközök és platformok használata jelenthet. Bár ez a dokumentum elsősorban vészhelyzetben lévő újságírók számára készült, azok az internethasználók is meríthetnek a tanácsokból, akik biztonságosabban szeretnék folytatni online tevékenységüket.

MI AZ INTERNET?

Az internet áthatja mindennapjainkat, erre támaszkodunk a munkában és a magánéletben egyaránt. Ugyanakkor számolni kell azzal, hogy a kibertér számos kockázatot, veszélyt, kelepcét tartogat. Ahhoz, hogy kivédhessük ezeket, értenünk kell, miként működik az internet.
Az **internet** több milliárd **elektronikus eszköz** és számos protokoll globális hálózata. A **protokollok** rögzítik azokat a szabályokat, amelyeket a berendezések az utasítások elvégzésekor (például információ küldésekor és fogadásakor) követnek. Ezek a protokollok olyan „nyelvet" alkotnak, amelyet minden elektronikus eszköznek értenie kell. Ha nem ugyanaz lenne a nyelv, az eszközök sem lennének képesek az adatok azonosítására és cseréjére.

Ezt a globális hálózatot fizikai kábelek (réz telefondrótok, televíziós kábelek, száloptikai kábelek stb.), mikrohullámok, rádióhullámok és műholdak kötik össze. Az adatok elektromos jelekként közlekednek ezen a hatalmas infrastruktúrán, gyakran kettes alapú digitális formában. Bármit teszünk az interneten, az adat formájában jelentkezik, kezdve a rendszerbe való belépéstől minden egyes leütésig, amikor például levelet írunk.

A **világháló** (World Wide Web vagy rövidítve web) honlapok együttese, amely az interneten keresztül érhető el. A világháló nem egyezik meg az internettel. Amikor belépünk a netre, a honlapokat alkalmazásokon keresztül érhetjük el: ezek a hálózati böngésző programok. A webes kereső sem azonos az internettel, csak arra szolgál, hogy megjelenítse a honlapot, amelyre ellátogatunk.

Amikor beütjük az oldal URL-jét, vagy ráklikkelünk a kereső által kiadott eredményre, berendezésünk – elektronikus jelzéssel – kérést továbbít a szerverhez. A **szerver** tárolja a honlapokat. Amikor a kérés eljut a szerverhez, az megtalálja az oldalt, és visszajuttatja a megfelelő adatot a berendezésünkhöz. A szerver felismeri eszközünket az egyedi IP (Internet Protocol) cím alapján: ez egy számsor, amilyennel minden eszköz rendelkezik, amely része az internetet alkotó globális hálózatnak.

Magánszemélyek úgy kapcsolódnak az internethez, hogy hozzáférést vesznek egy **internetszolgáltatótól** (ISP). Attól függően, hogy a világ melyik pontján tartózkodunk, a szolgáltató vagy kábellel, hullámsávval és műholddal rendelkezik, vagy hozzáférést vásárol egy ezzel az infrastruktúrával rendelkező multinacionális cégtől. Amikor hozzáférést veszünk egy ISP-től, kapunk egy berendezést, amelynek **router** a neve. (A berendezés lehet router és modem kombinációja is.) Ezt kábelekkel az elektromos hálózathoz és az internethez kell csatlakoztatni. Így a router lehetővé teszi, hogy több berendezéssel csatlakozzunk az internethez wifi vagy ethernet kábel segítségével. Amikor nyilvános wifi hálózatot használunk, olyan routeren keresztül kapcsolódunk az internethez, amely más tulajdonában van.

MIKÉNT KAPCSOLÓDJUNK AZ INTERNETHEZ BIZTONSÁGOSAN?

- A nyilvános internetkapcsolat (internetkávézó, könyvtár, köztéri wifi) kockázatosabb, mint a saját tulajdonban lévő hozzáférés.
- Olyan wifi hálózatokhoz csatlakozzunk, amelyek rendelkeznek WPA vagy WPA2 (WiFi Protected Access) biztonsági protokollal!
- A nyilvános wifi hálózatok megőrizhetik az azokhoz kapcsolódó berendezések adatait. A VPN vagy a Tor használata véd ez ellen.
- Kapcsoljuk ki az eszközeinken a megosztás és a Bluetooth funkciót!

- A telefont vagy a számítógépet úgy állítsuk be, hogy ne kapcsolódjon automatikusan hálózatokhoz, és ne jegyezze meg azokat a hálózatokat, amelyeket korábban használt! Így a berendezés nem áll rá automatikusan a rendszerre.

MOBILHÁLÓZATI KOCKÁZATOK

Alapvető különbségek vannak a mobilhálózati és a számítógépes infrastruktúrák, valamint a vezetékes és a vezeték nélküli internet között. Emiatt a mobilhálózatokon zajló adatátvitel eleve nem biztonságos.

> **„A mobilhálózatokat kereskedelmi vállalkozások működtetik, amelyek a kormány kizárólagos ellenőrzése alatt állhatnak. Ezek a cégek (vagy a kormányok) korlátlanul hozzáférhetnek a fogyasztók adataihoz és kommunikációjához, emellett megismerhetik a hívások, szöveges üzenetek tartalmát, valamint nyomon követhetik az összes, hálózatra kapcsolódott eszközt (így azok használóit) is." –** Security in-a-box (Megjegyzés: a szövegben található linkek angol nyelvű tartalmakhoz vezetnek.)

A telefonunkon tárolt, arra küldött és onnan érkező adatok sérülékenyek, mert mobilhálózatokhoz kapcsolódnak. Továbbá – a számítógépektől eltérően – a telefonok információt szolgáltatnak tartózkodási helyünkről.

- A legtöbb országban a mobilszolgáltatókat törvény kötelezi valamennyi, rajtuk keresztül történő kommunikáció adatainak megőrzésére. Bár nem mindig, de időnként a kormánynak jogában áll, hogy hozzájusson ezekhez az információkhoz.
- Amikor mobilhálózatokon zajlik a kommunikáció, a hang- és a szöveges üzeneteket sokkal könnyebb ellenőrizni különböző megfigyelőeszközökkel.
- Mobiltelefonunk adatai (híváslisták, küldött és fogadott sms-ek, cím- és telefonjegyzék, fotók, videók, szöveges fájlok) sok mindent elárulnak rólunk – ez bennünket is és a velünk kapcsolatban állókat is veszélybe sodorhatja. Néha lehetetlen ezen adatok teljes biztonságát garantálni.
- A mobiltelefonok automatikusan és rendszeresen megadják a tartózkodási helyet a mobilszolgáltatónak. Továbbá sok telefon tartalmaz GPS (Global Positioning System) funkciót. A GPS-adatok beágyazódhatnak a fotókba, sms-ekbe és az internetelérési információkba.
- Tanács: az iPhone-ok általában biztonságosabbak az Android rendszert használó mobiloknál, mert a legtöbb androidos készüléktől eltérően az iPhone biztonsági beállításai rendszeresen frissülnek.

Hasznos források angol nyelven:
– Security in-a-box
– We Fight Censorship

BIZTONSÁGI ÖSSZEFOGLALÓ

Hallgassunk a megérzéseinkre! Ha nem érezzük magunkat biztonságban egy nyilvános helyen, távozunk onnan! Ha okkal hihetjük, hogy illetéktelenek fértek hozzá a mobiltelefonunkhoz vagy számítógépünkhöz, cselekednünk kell: vagy szabaduljunk meg az eszköztől, vagy szerezzünk be biztonsági szoftvert a probléma kiküszöbölésére! Ha úgy gondoljuk, hogy online tevékenységünket megfigyelik, lépjünk; csökkentsük a kockázatot! Ne altassuk el a gyanakvást, ha rossz a biztonságérzetünk!

MILYEN LÉPÉSEKET TEHETÜNK A DIGITÁLIS BIZTONSÁG ERŐSÍTÉSÉRE?

- Olvassunk, tanuljunk, képezzük magunkat! Számoljunk azokkal a kockázatokkal, amelyek a számítógépek, mobiltelefonok és az internet használatakor fennállnak!
- Digitális tevékenységünk más területeihez hasonlóan legyünk óvatosak, amikor újságírókat segítő és emberi jogi szervezetekkel kommunikálunk!
- Ha illetéktelenek férnek hozzá berendezéseinkhez, telepítsünk biztonsági szoftvert, amely véd a behatolástól és törli a rosszindulatú számítógépes programokat!
- Válasszuk ki a számunkra legmegfelelőbb böngészőprogramot a biztonság maximalizálására és a magánszféra védelmének biztosítására! Telepítsük a megfelelő kiegészítőket, hogy növeljük böngészőnk biztonságát!
- Ismerjük meg, miként lehet a legbiztonságosabban kommunikálni a kibertérben! Az e-mailezés, az azonnali üzenetküldés, a VOIP és a közösségi média használata többé-kevésbé biztonságossá tehető.
- A hardver és a szoftver a digitális biztonság alapja, de online viselkedési szokásaink legalább ennyire fontosak. Mindig törekedjünk a biztonságra!
- Használjunk VPN-t (Virtual Private Network)!
- Figyeljünk arra, hogy eszközeink automatikusan telepítsék a biztonsági frissítéseket!
- A rejtjeles titkosítás (encryption) mindenki számára növeli az online biztonságot. Fontos tudni, hogy mit jelent a titkosítás, és miként lehet alkalmazni, amennyiben a körülmények lehetővé teszik azt.
- A bizalom elsőrendű az interneten. Ha úgy érezzük, hogy valaki vagy valami nem megbízható, ne tegyük ki magunkat kockázatnak!

BÖNGÉSZŐK

A böngészők különböző szintű biztonságot garantálnak felhasználóik számára, és ez igaz a magánszféra védelmével kapcsolatos beállításokra is. Használjuk a számunkra legmegfelelőbb böngészőt!

- Használjuk a Google Chrome-ot, ha maximalizálni akarjuk a biztonságot, de nem zavar bennünket, hogy a Google sok személyes információt gyűjt be rólunk!
- Használjuk a Mozilla Firefoxot, ha maximalizálni akarjuk a magánszféra védelmét, de készek vagyunk engedni a biztonságból!
- Csak Apple-terméken (iPhone, Mac stb.) használjunk Safarit!
- Ha lehet, ne használjunk Internet Explorert!
- Próbáljunk ki még biztonságosabb böngészőprogramokat: Brave, Dragon Internet Browser, Epic Privacy Browser, Tor Browser.

A WEBBÖNGÉSZŐK ÖSSZEHASONLÍTÁSA (l. Comparing web browsers):

Böngésző	**Verzió**	**Biztonság**	**Magánszféra**
Chrome	53	Legjobb	Legrosszabb
Firefox	49	Rendben	Legjobb
Safari	10	Jó	Rendben
Internet Explorer	11	Legrosszabb	Rendben

AZONNALI ÜZENETVÁLTÁS (INSTANT MESSAGING)

Az újságírók leginkább a WhatsApp-ot használják azonnali üzenetküldésre, legalábbis ez derült ki a sajtószabadságot támogató kanadai szervezet, a Canadian Journalists for Free Expression (CJFE) felméréséből. A válaszadók 74 százaléka nyilatkozott úgy, hogy a WhatsApp-ot részesíti előnyben. 29 százalék használja közvetlen üzenetváltásra a Skype-ot, míg kilenc-kilenc százalék a Signalt vagy a Vibert. Miként maximalizálhatjuk itt a biztonságunkat?

- Ne használjunk Skype-ot! Az anyacég Microsoft és kívülállók is – például kormányok – viszonylag könnyen hozzáférhetnek a felhasználók adataihoz és üzeneteihez.
- A WhatsApp végpontok között titkosítást biztosít, ami remek dolog. Annak ellenére azonban, hogy WhatsApp nem fér hozzá az üzenetek tartalmához, azt azért látják, hogy kik és mikor állnak kapcsolatban egymással. Ezt a metaadatot tehát rögzíthetik és továbbadhatják másoknak.
- Továbbá a WhatsApp kívánnivalót hagy maga után a magánszféra biztonságának garantálásában. 2016 nyarán ez az azonnali üzenetváltó szolgáltatás elkezdte megosztani a felhasználói információkat anyacégével, a Facebookkal.
- A WhatsApp-hoz hasonlóan a Signal is végpontok közötti titkosítást biztosít, de további előnye, hogy nyílt a forráskódja. Ez azt jelenti, hogy a szoftver alapját képező kódot külső szakértők is megvizsgálhatják, hogy kiküszöböljék a biztonsági hiányosságokat, és kizárják, hogy kerülőutakon (ún. „hátsó ajtókon") keresztül illetéktelenek is hozzáférjenek az üzenetekhez. A WhatsApp-tól eltérően a Signal nem tárol metaadatokat.
- A Facebook Messenger „Titkos beszélgetés" funkciója ugyanazt a titkosítást használja, mint a Signal, de az csak mobiltelefonokon működik.
- A Telegram semmilyen körülmények között sem biztonságos kommunikációs eszköz.

Jó tanács: Ha lehet, használjunk Signalt WhatsApp és Skype helyett!
Hasznos források angol nyelven:
- How to use Signal on iOS (Apple products)
- How to use Signal on Android (Google products)

KÖZÖSSÉGI MÉDIA

Vészhelyzetben lévő újságírók munkavégzéshez és segélykéréshez egyaránt használják a közösségi médiát. A közösségi oldalak közül messze a Facebook a legnépszerűbb, amely nélkülözhetetlen a közönséggel való kapcsolattartásban, de akkor is, ha újságírókat segítő szervezetet próbál elérni a bajba jutott tudósító. Ugyanakkor a Facebook használata – a magánszféra védelmének hiányosságai miatt – kockázatos is lehet. A Facebook folyamatosan változtatja az adatmegosztási gyakorlatát a profitmaximalizálás, illetve annak érdekében, hogy a felhasználók mindent egy helyen találjanak meg. Ez általános romláshoz vezetett a magánszféra védelmét illetően (l. data-sharing practices).

Miként használjuk biztonságosan a Facebookot?
- Ismerjük meg a Facebook magánszférára és adatvédelemre vonatkozó irányelveit (l. privacy és user data)! A Gyakran Ismételt Kérdések között megtalálható, milyen adatokat gyűjt a Facebook a felhasználóiról (l. Frequently Asked Questions).
- Úgy kell megadni a személyes adatokkal kapcsolatos beállításokat, hogy minimális nyomot hagyjunk magunk után a közösségi térben.

  Példák:
  1. Létezik olyan funkció, amely lehetővé teszi, hogy „láthatatlanok" maradjunk a keresőprogramok számára.
  2. Rendelkezni lehet arról, hogy csak barátaink és ismerőseink találjanak meg bennünket e-mail cím és telefonszám alapján.
  3. Egy másik funkció megakadályozza, hogy a Facebook más alkalmazásokat is profilunkhoz kapcsoljon.

Hasznos tanácsok valamennyi közösségi oldal használatához:

- Ismerjük meg a profilunk biztonsági alapbeállításait, és tapasztaljuk ki, hogyan lehet megváltoztatni azokat!
- Használjunk nehezen feltörhető jelszavakat!
- A közösségi térben hozzunk létre különböző profilokat a különböző tevékenységekhez (például újságírás, politikai aktivizmus, speciális kampányok, személyes kapcsolattartás)!
- A legritkább esetben használjuk a közösségi médiát nyilvános helyen elérhető számítógépeken vagy nyilvános wifi hálózaton keresztül! Töröljük a böngészési előzményeket, és ürítsük ki a „cache" mappa tartalmát, ha nyilvános helyen (internetkávézóban vagy könyvtárban) használtunk számítógépet (l. delete your browser history and cache)!
- Mindig nagyon figyeljünk oda, hogy milyen információt osztunk meg közösségi oldalakon! Csak a lehető legszükségesebb személyes információt adjuk meg!
- Belépéskor a „https://" használata biztonságosabb, mint a „http://"-é. Ez még egy biztonsági szintet biztosít az online tevékenységhez azáltal, hogy titkosítja a forgalmat a böngésző (Google Chrome, Mozilla Firefox, Safari stb.) és a közösségi oldal között.
- Számos közösségi oldal mutatja tartózkodási helyünket. Kétszer is ellenőrizzük, hogy a tartózkodási helyet jelző beállítást kikapcsoltuk a mobiltelefonunkon és számítógépünkön!
- Rendszeresen ellenőrizzük, hogy milyen alkalmazások kapcsolódhatnak a közösségi médiaprofilunkhoz! Töröljük a régi és használaton kívüli alkalmazásokat!

Itt (Learn more) többet megtudhatunk a biztonságos közösségi médiahasználatról, így például az egy cég tulajdonában lévő Facebookról és Instagramról, a Twitterről, a YouTube-ról vagy a Flickrről.

INTERNETKÁVÉZÓK

Adódhatnak olyan esetek, amikor csak kávézóban férhetünk hozzá internethez. Ilyenkor fontos észben tartanunk, hogy amint nyilvános helyre lépünk, névtelenségünk, magánszféránk védelme és biztonságunk azonnal veszélybe kerülhet.

Miként csökkenthetjük a rizikót?

- Keressünk olyan internetkávézót, ahol nem kell bejelentkezni vagy azonosító okmányt átadni a számítógépek használatához!
- Ha lehet, legyen nálunk saját számítógépünk, különösen, ha bizalmas információkkal dolgozunk!
- Ellenőrizzük, hogy irányul-e biztonsági kamera a képernyőnkre! Ha lehet, az ilyen helyzetet kerüljük el!
- Üljünk olyan géphez, amelynek képernyőjét tudtunkon kívül más nem láthatja!
- Távozás előtt töröljük a böngészési előzményeket és ürítsük ki a „cache" mappa tartalmát (l. delete your browser history and cache)!
- Hozzunk magunkkal megbízható programokat USB-n (pendrive-on), így elkerülhetjük az előre telepített programok használatát. A Security in-a-box link tartalmazza azokat a hordozható alkalmazásokat, amelyeket internetkávézókba is magunkkal vihetünk, hogy növeljük digitális biztonságunkat.
- **Bízzunk a megérzéseinkben, és hagyjuk el a helyet, ha úgy ítéljük meg, hogy nem vagyunk biztonságban!**

JELSZAVAK

A jelszavak alkotják az első védelmi vonalat, amikor online eszközökön kommunikálunk, vagy ott tárolunk adatokat. A sajtószabadságot támogató kanadai szervezet, a Canadian Journalists for Free Expression (CJFE) felméréséből az derül ki, hogy a vészhelyzetben lévő újságírók mintegy 40 százaléka

könnyen feltörhető vagy valószínűleg könnyen megfejthető jelszavakat használ. Ez azt jelzi, hogy az újságírók gyakran akkor sem tesznek lépéseket a biztonsági kockázatok kivédésére, amikor tisztában vannak a veszéllyel.

A jelszavak biztonsága könnyen növelhető, ha tudjuk, hogy mitől nehéz feltörni azokat. A bajba jutott újságírókat segítő amerikai szervezet, a Committee to Protect Journalists ezen a linken azt taglalja, hogy a behatolók miként törhetik fel viszonylag egyszerűen a jelszavakat.
Hasznos tanácsok nehezen feltörhető jelszavak választásához:

- A személyes adatot tartalmazó jelszavakat könnyű kitalálni.
- A jelmondatok erősebbek a jelszavaknál. A legalább hat szóból álló vagy annál hosszabb mondatok nagyon biztonságosnak tekinthetők.
- Válasszunk sejtelmes kijelentést vagy idézetet, amelyet mások nem tartanak jellemzőnek ránk! Teljes mondatot vagy betűkből és számokból álló rövidítést is lehet alkalmazni. Például:
  „Why is it always so hot outside?" → WiiA50HO?
  „Miért van mindig ennyire meleg odakinn?" → Mvm3MO?
  „That toy tiger I had as a kid was the best!" → TtT1hadAak1Dwa5th3B!
  „Gyerekkoromban ez a játéktigris volt a kedvencem!" → Gyek3zajTri5VolaKe!
- A hosszabb jelmondatok biztonságosabbak, mint a rövidek.
- Kombináljuk a nagy- és kisbetűket számokkal, illetve különleges karakterekkel (!@#$%^)!
- Ne használjuk fel újra ugyanazt a jelmondatot!
- Ne osszuk meg senkivel a jelmondatot!
- Háromhavonta változtassunk jelmondatot!
- Tartsuk szem előtt, hogy a biztonsági kérdésekre adott valós válaszok gyakran nyilvánosan hozzáférhető információvá válnak (például ilyen adat az „anyja leánykori neve", „apja születési ideje", „tanulmányok helye")! (Megjegyzés: a biztonsági kérdést általában akkor teszik fel, ha elfelejtettük a jelszavunk.)
- A rosszhiszemű támadóknak mindig van módszere arra, hogy a jelszavakhoz hozzájussanak, így alkalmazhatnak fizikai fenyegetést is. A Committee to Protect Journalists azt javasolja, hogy legyen egy olyan internetes profilunk/levelezésünk, amely csak ártalmatlan információkat tartalmaz, az ehhez kapcsolódó jelszó fizikai fenyegetettség esetén is kiadható (l. under duress).
- Ezen az oldalon (passfault) ellenőrizhetjük, hogy jelszavunk milyen gyorsan törhető fel.
- Jelmondataink tárolására használjunk jelszókezelő programokat, amelyek segítségével nehezen megfejthető jelszavakat generálhatunk! Ugyankor figyeljünk arra, hogy csak nagyon erős mesterjelszóval lehessen belépni ebbe a programba, különben valamennyi jelszavunkhoz hozzájuthatnak illetéktelenek! Ajánlott szoftverek: KeePass, Password Safe.
- Ha lehet, használjunk kétlépcsős azonosítást: two-factor authentication (2FA)! Ez a honlap megmutatja, mely szolgáltatások esetében lehet használni ezt a funkciót: Two Factor Auth.

„A kétlépcsős azonosítás (Two-factor authentication) egyszerű funkció, amelynek az a lényege, hogy nem csak egy jelszót kell megadnunk, amikor egy profilt vagy szolgáltatást kívánunk elérni. Szükség van egy olyan információ megadására, amelynek birtokában vagyunk (például jelszó), emellett egy eszközzel (például mobiltelefon) is rendelkeznünk kell. A jelszó beütése után telefonunkra érkezik egy második kód, és csak ennek begépelésével férünk hozzá a saját profilunkhoz. Olyan ez, mint amit a kémfilmekben látunk, amikor a PIN kód megadását retinaszkennelés követi. Ez a módszer sokkal biztonságosabb, mint a könnyen meghekkelhető jelszó, és megakadályozza, hogy illetéktelenek hozzáférjenek online profiljainkhoz."

E-MAIL

Az elektronikus levelezés a kapcsolattartás igen gyakori és költségkímélő módja. Ugyanakkor szem előtt kell tartanunk, hogy csak annyira védettek a kimenő és bejövő üzeneteinkben, valamint a levelezőlistáinkban tárolt információk, amennyire általában is biztonságosan használjuk a digitális szolgáltatásokat.

Levelezésünket különböző módszerekkel tehetjük biztonságosabbá. Érdemes azoknak a szolgáltatásoknak az ellenőrzésével kezdeni, amelyeket jelenleg is használunk:

- Váltsunk biztonságosabb szolgáltatóra! Például a Google összegyűjti a Gmail felhasználóinak adatait, ami biztonsági kockázatot jelent. Ha feltétlenül Gmailt akarunk használni, ismerkedjünk meg a szolgáltató magánszféra védelmére vonatkozó szabályzatával (privacy policy), és vegyük számba a rizikófaktorokat!
- A RiseUp szolgáltató például nagyobb biztonságot garantál, és sokkal jobban védi a szerverein tárolt adatokat.
- Emellett a ProtonMail is biztonságos, főként mert végpontok közötti titkosítást (encryption) biztosít, ha a feladó és a címzett is ezt a szolgáltatást használja. Így érdemes lehet barátainknak és családtagjainknak a ProtonMailt ajánlani. Titkosított üzenetet egyébként ProtonMailt nem használónak is lehet küldeni egy jelszó beiktatásával, amelyet a címzett ismer. A program úgy is beállítható, hogy az üzenetek maguktól törlődjenek.
- Érdemes több e-mail címet is létrehozni, és ezekből egyet vagy néhányat csak megtévesztésre használni. Ha több e-mail címmel rendelkezünk, nehezebb megfigyelni bennünket.
- Nehezítsük meg, hogy e-mail címeink alapján azonosítsanak bennünket!

A levelezés biztonsága csak részben múlik azon, hogy milyen szolgáltatókat használunk. Legalább ennyire fontos, hogy okos e-mail használattal minimálisra csökkentsük a kockázatokat:

- Használjunk nehezen megfejthető jelszavakat!
- Ha lehet, alkalmazzunk kétlépcsős azonosítást (two-factor authentication), így növelve a biztonsági fokozatot. (Részletek az útmutató előző – jelszavakkal foglalkozó – részében!)
- A böngészőben HTTPS protokollt használva lépjünk be a levelezőprogramba!
- Ne nyissunk meg olyan üzenetet, amelynek gyanús a címe, mert vírust vagy rosszindulatú szoftvert tartalmazhat!
- Ugyanebből az okból ne nyissunk meg ismeretlentől érkező csatolt dokumentumot sem!
- Rendszeresen töröljük az ideiglenes fájlokat, amelyek a levelezés során keletkeznek! Ennek egyik módja, ha CCleaner-t használunk.
- Ha nyilvános helyen használjuk a levelezőrendszerünket, töröljük a böngészési előzményeket, valamint ürítsük ki a „cache" mappa tartalmát!
- Figyeljünk oda, kivel levelezünk, és milyen információt írunk le!

Megjegyzés: Az e-mail kommunikáció leghatékonyabban nyilvános kulcsú titkosítással (aszimetrikus titkosítás) tehető biztonságossá. A CJFE kanadai szervezet már idézett kutatása azt mutatja, hogy a megkérdezettek negyede használt titkosítást levélváltáskor, és 40 százalékuk nem hallott arról, hogy az e-mailek kódolhatók. Az útmutató következő fejezete a titkosítás alapjairól ad áttekintést. Alapvetően kétféleképpen alkalmazhatunk nyilvános kulcsú titkosítást. A „Security in-a-box" honlap itt ad ehhez eligazítást:

1. Thunderbird + Enigmail + OpenPGP for Windows
2. GPG4USB for Windows – Email and File Encryption

A TITKOSÍTÁS (ENCRYPTION) ALAPJAI

Az adatok leghatékonyabban rejtjeles **titkosítással** védhetők. Ilyenkor az adatokat jelekké alakítják, amelyek első ránézésre nem jelentenek semmit. A rejtjelezett adatok kuszák és önmagukban értelmezhetetlenek. A szöveget csak a megfelelő kulcs (jelszó vagy más azonosító) segítségével lehet helyreállítani.
A titkosításra számos lehetőség van, így egyebek mellett rejtjelezhető merevlemez, egyéb adattárolók (USB, SSD, SD kártya), fájl, mappa, levél, internetes kommunikáció.
Bizonyos eszközök eleve tartalmaznak olyan szoftvert, amely titkosítja a teljes merevlemezt. A Windows Pro 2007 utáni változatainak (a Windows Home-tól eltérően) része a BitLocker program, továbbá valamennyi 2003 után kiadott Mac FileVaultot is tartalmaz. BitLockerrel és FileVaulttal titkosíthatók a hordozható pendrive-ok is. Az újabb Andrioid operációs rendszerrel működő mobiltelefonokban és az iPhone-okban is van beépített titkosítás. **Ellenőrizzük mobileszközeinket, hogy tartalmaznak-e ilyen funkciókat!**

Ingyenes, illetve fizetős szoftverek is rendelkezésre állnak, hogy eszközeinken fájlokat és mappákat titkosítsunk, és ugyanezt megtehetjük hordozható pendrive-okon is. Leggyakrabban az ingyenes és szabad forráskódú VeraCrypt-et ajánlják. Telepítés előtt mindenféleképpen ismerkedjünk meg alaposan ennek a szoftvernek a megfelelő használatával, különben adataink visszaállíthatatlanul sérülhetnek.
Az elektronikus levelezés különösen sérülékeny módja a kommunikációnak, de az e-mailek titkosításával elérhetjük, hogy a levelek tartalma csak ahhoz jusson el, akinek szánjuk. Az e-mailek titkosítása általában a nyilvános kulcsú infrastruktúrára (Public Key Infrastructure, PKI) épül. A PKI egy, csak általunk ismert személyes kulcs, valamint egy közzétehető és másokkal megosztható nyilvános kulcs kombinációja. Ilyenkor a levél címzettjének nyilvános kulcsát használjuk az adott e-mail titkosításához, majd a címzett a saját személyes kulcsát alkalmazza a levél kibontásakor. (Lásd az útmutató e-mailről szóló részét!)

A titkosítás az internethasználat szerves részévé vált több területen is. Ez mindannyiunk biztonságát növeli. Megjegyzendő: egyre inkább a **Secure Socket Layer (SSL)** technológiát használják arra, hogy a kapcsolatot titkosítsák az általunk használt eszköz, illetve a felkeresett honlap vagy az igénybe vett internetes szolgáltatás között. A SSL része szinte valamennyi e-mail szolgáltatásnak. **Amikor SSL-en keresztül kapcsolódunk egy honlaphoz, az oldal URL-je HTTPS-szel és nem HTTP-vel kezdődik majd.** Ha biztosak akarunk lenni abban, hogy böngészéskor SSL-t használunk, telepítsük a HTTPS Everywhere kiegészítő programot!

Az SSL ugyanakkor nem egyezik meg a végpontok közötti titkosítással. Az SSL az eszköz és a honlap vagy internetszolgáltatás közötti adatforgalmat titkosítja. A honlap, illetve az internetszolgáltató ugyanakkor olvashatja az adatokat. A végpontok közötti titkosítás viszont azt is megakadályozza, hogy a megosztott információkat a weboldal vagy az internetes szolgáltató láthassa. Például a Gmail levelezőprogram használ SSL-t, de a Google anyacég ennek ellenére olvashatja az e-mailek tartalmát. A WhatsApp és a Signal viszont biztosít végpontok közötti titkosítást is, ez azt jelenti, hogy anyacégeik, a Facebook és az Open Whisper Systems nem láthat bele üzeneteink tartalmába.

SZOFTVEREK, ALKALMAZÁSOK, KIEGÉSZÍTŐK

Számos szoftver, alkalmazás és kiegészítő növelheti digitális biztonságunkat. Érdemes tanulmányozni az alábbi felsorolást, de ezeken kívül is találhatunk olyan programokat, amelyek leginkább megfelelnek igényeinknek. Ugyanakkor ne feledjük: a megfelelő biztonsági eszközök alkalmazása

mellett legalább annyira fontos az óvatosság az internet használatakor! Leginkább ugyanis ezzel csökkenthetjük a biztonsági kockázatot, amellyel újságíróként vagy egyszerű internetfelhasználóként is számolnunk kell. Az alábbi eszközök közül jó néhányról részletesen is szóltunk az útmutató előző fejezeteiben:

Jelszókezelő programok:
- KeePass
- Password Safe

E-mail szolgáltatók:
- Hushmail
- ProtonMail
- RiseUp
- Tutanota

Biztonsági szoftverek:
- Avast! (vírusvédelem)
- CCleaner (adatok törlése)
- Comodo (hálózati tűzfal)
- Eraser for Windows (adatok törlése)
- Malwarebytes (vírusirtó)
- Spybot (vírusirtó)
- Veracrypt (fájlok titkosítása)

Böngészők:
- Dragon Internet Browser
- Epic Privacy Browser
- FreeBrowser
- Lantern
- Tor Browser

VPN-szolgáltatók:
- NordVPN
- OpenVPN
- Psiphon
- TunnelBear

Nyilvános kulcsú titkosítás levelezéshez:
- Thunderbird + Enigmail + OpenPGP
- GPG4USB for Windows
- Mailvelope

Titkosított azonnali üzenetváltás és VOIP:
- Cryptocat
- Jitsi
- Pidgin
- Signal

Böngészőkiegészítők:
- Adblock Plus
- DoNotTrackPlus
- Ghostery
- HTTPS Everywhere
- NoScript Security Suite
- Privacy Badger
- uBlock Origin

Biztonságos keresőmotorok:
- DuckDuckGo
- F-Secure Safe Search

Android alkalmazások:
- Android Privacy Guard
- Obscuracam (okoskamerák biztonságossá tétele)
- Orbot (Tor böngésző)
- Umbrella (Könnyen megteremthető biztonság)

HOGYAN VISZONYULJUNK A HATÓSÁGOKHOZ?

A kanadai CJFE szervezet felmérése szerint az „Újságírók vészhelyzetben" elnevezésű program (l. Journalists in Distress program) résztvevőinek csaknem 90 százaléka tart attól, hogy internetes kommunikációját időnként vagy állandóan megfigyelik. Esetükben lehetséges veszélyforrást jelenthet annak az országnak a kormánya, ahonnan az újságíró származik, vagy ahol éppen tartózkodik (különösen, ha önkéntes száműzetésben él), de kockázatot jelenthetnek hírszerzők, biztonsági ügynökök és a rendőrség is. Továbbá a megkérdezett újságírók 30 százaléka mondta azt, hogy a hatóságok kobóztak már el tőle elektronikus eszközt, és csaknem ötven százalékuktól el is loptak ilyen berendezést.

Elektronikus berendezéseink betekintést adhatnak egész életünkbe. Amikor országhatáron, ellenőrzőponton lépünk át, vagy nyilvános helyen vagyunk, megelőző lépéseket kell tennünk, hogy a hatóságok fizikailag ne férjenek hozzá telefonunkhoz!

- Telefonunk kijelzője és számítógépünk képernyője automatikusan kapcsoljon ki, amikor nem használjuk az eszközt!
- Ne használjunk olyan jelszavakat, amelyeket a hatóságok gyorsan feltörhetnek, ha rövid időre elveszik tőlünk a berendezést!
- Mindig legyen nálunk a telefonunk! Zárjuk el a számítógépünket, ha nem visszük magunkkal!
- Kerüljük el, hogy mások láthassák eszközeink kijelzőjét, és sohase hagyjuk eszközeinket őrizetlenül!
- Ha meg kell szabadulnunk telefonunktól, ne felejtsük el előbb megsemmisíteni a SIM kártyát és a memóriakártyát!
- Ha lehet, határ-, illetve biztonsági ellenőrzésekkor cseréljük üres kártyára a SIM kártyát!
- Ha lehet, határ- és biztonsági ellenőrzésekkor, illetve hatósági személyek jelenlétében ne legyen nálunk olyan eszköz, amelyen különösen bizalmas információkat tárolunk!

Ezek az elővigyázatossági lépések nem fogják megakadályozni a hatóságokat abban, hogy eszközeinkhez hozzáférjenek. Ugyanakkor megnehezíthető, hogy adatainkat könnyen és gyorsan megismerjék.

SEGÉLYKÉRÉS

Amikor emberi jogi szervezetekhez vagy segélyprogramok képviselőihez fordulunk, személyes információt kell szolgáltatnunk az éppen aktuális helyzetről. Ha ez az interneten keresztül történik – ami manapság a kommunikáció leggyakoribb módja –, fennáll a veszélye annak, hogy bizalmas információ jut illetéktelenekhez.

Hogyan őrizzük meg biztonságunkat, amikor segélyszervezetekkel lépünk kapcsolatba?

- Csak akkor adjunk ki információt, ha teljes biztonságban érezzük magunkat! A CJFE már említett felmérése azt mutatja, hogy a válaszadók 61 százaléka tartott vissza információt ilyen esetben biztonsági megfontolások miatt.
- Töröljük a segélyszervezethez beadott jelentkezési lapot, amint elküldtük azt! Ezt elmulasztva egyetlen dokumentumban rengeteg bizalmas információt tárolunk, amelyhez könnyű hozzáférni.
- Ha digitális biztonságra vonatkozó aggályaink vannak, kérjünk segítséget a támogató szervezet képviselőitől, hiszen ennek biztosítása is feladatuk része!
- Amikor csak lehet, a segélykérésünkkel kapcsolatos információt biztonságosan juttassuk el az újságírókat támogató szervezetekhez! Például a Committee to Protect Journalists elnevezésű amerikai szervezethez fordulhatunk a SecureDrop-on keresztül. A szíriai konfliktus helyszíneiről tudósítók külön formanyomtatványt (l. application form) tölthetnek ki, amely titkosítva 12 segélyszervezethez érkezik meg.
- Ha nincs kialakított módszerünk a titkosított levelezésre (l. az útmutató e-mailekkel kapcsolatos fejezetét), kezdeményezhetjük, hogy Signalon, WhatsAppon vagy más, végpontok közötti titkosítást biztosító szolgáltatáson keresztül váltsunk üzenetet a segélyszervezetek munkatársaival.
- Legyünk óvatosak, amikor közösségi médiafelületen (például Facebookon, Twitteren) nyilvánosan kérünk segítséget!
- Mielőtt segélyszervezetekhez fordulnánk, érdemes alaposan áttanulmányozni ennek az útmutatónak a többi fejezetét, amelyek leírják, hogy milyen eszközökkel és módszerekkel növelhetjük biztonságunkat!

KAPCSOLATFELVÉTEL

Ha valakit újságírói tevékenysége miatt üldöznek, forduljon azonnal a kanadai CJFE szervezet „Újságírók vészhelyzetben" programjához (l. Journalists in Distress program)! Ha a kérés jellege nem felel meg a program kritériumainak, számos más szervezet is nyújthat veszélyhelyzetben támogatást:

- Access Now
- Committee to Protect Journalists
- Digital Defenders Partnership
- Doha Centre for Media Freedom
- Free Press Unlimited
- Freedom House
- Front Line Defenders
- Human Rights Watch
- International Cities of Refuge Network
- International Committee of the Red Cross Hotline
- International Federation of Journalists
- International Media Support
- International Women's Media Foundation
- Institute for War and Peace Reporting
- Journalists Helping Journalists
- The Kality Foundation
- Lifeline Embattled CSO Assistance Fund
- Media Legal Defence Initiative
- PEN American Center
- PEN International
- Prisoners of Conscience
- Reporters Without Borders
- Rory Peck Trust
- Scholar Rescue Fund
- Urgent Action Fund for Women's Human Rights

TOVÁBBI INFORMÁCIÓK

Ez az útmutató hasznos kiindulópont lehet – a digitális biztonsági kockázatok azonban sokfélék, és a védekezésnek is számos módja van. Az alábbiakban további kézikönyveket, útmutatókat ajánlunk, amelyek segíthetik az újságírókat és az emberi jogi aktivistákat abban, hogy környezetük fizikai, valamint digitális értelemben is biztonságosabb legyen.

A digitális biztonságról általában:

- Basic Internet Security (Floss Manuals)
- Defending Accounts against Common Attacks (Source Guides)
- Digital and Mobile Security for Journalists and Bloggers – arabul is (International Center for Journalists)
- Digital Security First Aid Kit (Digital Defenders Partnership)
- Digital Security Guide (Front Line Defenders)
- DIY Guide to Feminist Cybersecurity (Noah Kelley)
- Manual de Seguridad Digital y Móvil (International Center for Journalists)
- Me and My Shadow (Tactical Tech)
- Online Survival Kit (Reporters Without Borders)

- Protect Yourself (Freedom of the Press Foundation)
- Security in-A-Box
- Surveillance Self-Defense (Electronic Frontier Foundation)
- Technology Security (Committee to Protect Journalists)

Az újságírással kapcsolatos digitális biztonság:
- Cybersecurity Quiz (Center for Democracy & Technology)
- Digital Self-Defense for Journalists: An Introduction (Source Guides)
- Journalist on the Move (Electronic Frontier Foundation)
- Journalists Security Guide (Committee to Protect Journalists)
- Ontheline – Report Securely (International Press Institute)
- Secure Journalism at Protests (Martin Shelton)
- Security for Journalists: The Basics (Source Guides)
- Security Tools (Freedom of the Press Foundation)
- UN Plan of Action on the Safety of Journalists and the Issue of Impunity
- 96 Resources for Tip Sheets (Dart Center for Journalism and Trauma)

Közel-Kelet és Észak-Afrika:
- Freelancing in Libya (Rory Peck Trust)
- Syria Media Safety (12 partner organizations)

Újságírók száműzetésében:
- East Africa Journalists in Exile (Rory Peck Trust)
- Guidelines for Exiled Journalists (Reporters Without Borders)
- Iranian Journalists in Exile (Rory Peck Trust)

Tudósítás válságkörzetekből:
- Disaster and Crisis Coverage (International Center for Journalists)
- Reporting for Change: A Handbook for Local Journalists in Crisis Areas (Institute for War and Peace Reporting)
- International Travel and Health – Updates and Reports (World Health Organization)

Jogsegély:
- Manual on European Defamation Law (Media Legal Defence Initiative)
- Manual on Freedom of Expression Law (Media Legal Defence Initiative)
- Manual on Freedom of Expression Litigation in East Africa (Media Legal Defence Initiative)

Ajánlott forrás:
- Digital Security Resources: December 2016 Edition (Martin Shelton)

Ezt az útmutatót az Open Technology Fund támogatásával készítette a Kanadai Újságírók a Szólás-szabadságért (Canadian Journalists for Free Expression, CJFE) szervezete, amely hozzájárult ahhoz, hogy a Független Médiaközpont magyar nyelvre lefordítsa és publikálja. A CFJE segítségét ezúton is köszönjük.

OPEN TECHNOLOGY FUND