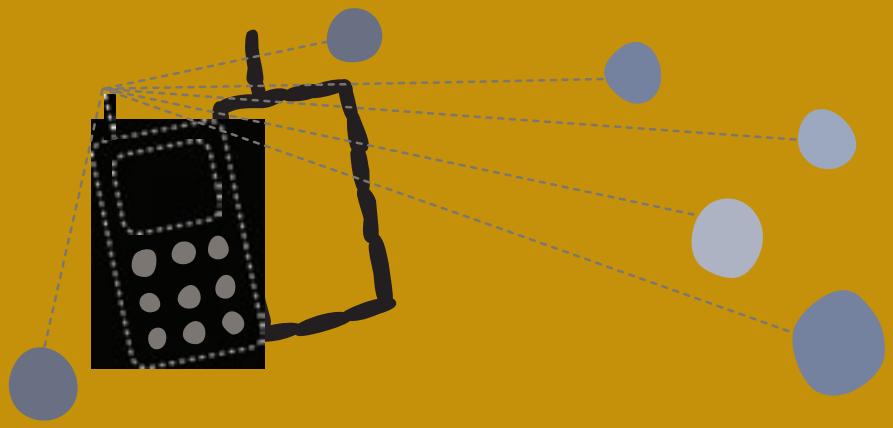
# Інтэрнэт і мабільная сувязь бяспека і канфідэнцыйнасць



НОВЫЯ ТЭХНАЛОГІІ, ТАКІЯ ЯК МАБІЛЬНЫЯ ТЭЛЕФОНЫ І ІНТЭРНЭТ, З'ЯЎЛЯЮЦЦА МАГУТНЫМ ІНСТРУМЕНТАМ У ПРАВААБАРОНЧАЙ ДЗЕЙНАСЦІ , АЛЕ ВЫКАРЫСТАННЕ ІХ ДЛЯ ПЕРАДАЧЫ ДАЛІКАТНЫХ ЗВЕСТАК МОЖА СТВАРЫЦЬ РЫЗЫКУ ДЛЯ ВАС, ВАШЫХ СУВЯЗЯЎ, СЯБРОЎ І КАЛЕГ. ГЭТАЯ КАРТКА ДАПАМОЖА ВАМ ЗРАБІЦЬ ДОСТУП ДА ІНФАРМАЦЫІ БЯСПЕЧНЫМ І ЗАСЦЕРАГЧЫ ВАШЫЯ ДАДЗЕНЫЯ ПАДЧАС КАРЫСТАННЯ МАБІЛЬНЫМІ ТЭЛЕФОНАМІ І ІНТЭРНЭТАМ.

**ШТО АЗНАЧАЕ ЛІЧБАВАЯ БЯСПЕКА І КАНФІДЭНЦЫЙНАСЦЬ?**

Прыкметы парушэння права на інфармацыю і лічбавай бяспекі:

- Паролі таямніча змяняюцца
- Прыватныя паведамленні выглядаюць як быццам былі прачытаныя кімсьці іншым, а не тым, каму яны прызначаліся
- Вэб-сайты робяцца недаступнымі з некаторых краінаў
- Чыноўнікі выяўляюць дасведчанасць у прыватнай карэспандэнцыі, уключна датаў, імёнаў, абмеркаваных тэмаў
- Пад час размовы  па мабільным тэлефоне ствараецца ўражанне, што яго праслухоўваюць

**ЦІ ПАВІННА ГЭТА МЯНЕ ХВАЛЯВАЦЬ?**

Калі падобныя выпадкі могуць скампраміта ваць ваш праект ці выдаць вас і вашыя кантакты следчым ворганам, варта хвалявацца.  Тэхналогіі і праграмнае забеспячэнне, дзякуючы якім можна стварыць пагрозу вашай  канфідэнцыйнасці, часта можна адшукаць у Інтэрнэце. Калі той хто атакуе, мае дастатковы доступ да  Інтэрнэту ці інфраструктуры

мабільнай сувязі у вашай краіне, патрэбныя тэхналогі даволі простыя. Дзяржаўныя агенцтвы, правайдэры Інтэрнэту (ISPs), кампаніі мабільнай сувязі маюць прывілеяваны доступ да інфраструктуры, але падобны доступ могуць мець і іх калегі па офісу, суседзі, аператары Інтэрнэт-кавярняў.

**ЯКІЯ ПЫТАННІ БЯСПЕКІ АСВЯТЛЯЮЦЦА Ў ГЭТАЙ КАРТЦЫ?**

У гэтай картцы разглядаюцца Інтэрнэт-інструменты і мабільныя тэлефоны. Аднак ёсць яшчэ безліч іншых тэхналогій, якія могуць уяўляць для вас небяспеку  цэнзуры, нагляду ці перасляду. Найбольш важныыя,  неапісаныя тут меры бяспекі- гэта рэгулярнае абнаўленне аператыўнай сістэмы кампутара, надзейныя анты-вірусныя праграмы, паслядоўнае захаванне рэзервовых копій. Калі ў вас ёсць падставы меркаваць, што вашы кампутары ці носьбіты інфармацыі, у тым ліку рэзервовыя копіі, знаходзяцца пад рызыкай і могуць быць страчаныя, скрадзеныя ці канфіскаваныя, альбо вы падазраеце, што вашая арганізацыя знаходзіцца пад Інтэрнэт-наглядам (ці калі гэта звычайна для дадзенага рэгіёну), тады вам трэба звярнуцца да комплекса інструментаў “Бяспека пад рукой”, падрыхтаваным Tactical Tech.

## Інтэрнэт-інструменты для праваабаронцаў

Пры выкарыстанні для мабілізацыі і каардынацыі людзей такіх грамадскіх Інтэрнэт-рэсурсаў як Blogger, Facebook, Twitter, памятайце, што інфармацыя, якую вы захоўваеце на падобных платформах, становіцца, у пэўнай меры, уласнасцю аператараў, і што многія з гэтых рэсурсаў могуць утрымліваць больш звестак, чым падаецца.

Калі вы вырашылі даверыць далікатныя праекты аператарам нейкага Інтэрнэт-рэсурса, прачытайце ўмовы палітыкі канфедэнцыйнасці і дамову з карыстальнікам.

Памятайце, што нават самыя пэўныя гарантыі пакідаюць вашу інфармацыю пад непасрэдным кантролем адміністратараў рэсурсаў, якія могуць абнародаваць, прадаць ці перанакіраваць інфармацыю без вашага ведама ці дазволу. Нават калі вы спынілі дзеянне вашага акаўнту, многія з гэтых вэб-сайтаў на сам рэч не выдаляюць змест ці персанальныя дадзеныя, якія вы апублікавалі. У рэшце рэшт, калі зварот да нейкага канкрэтнага камерцыйнага сэрвісу не з’яўляецца прынцыповым, ці то па прычыне даступнасці, ці то дзеля інтэграцыі з іншымі карыстальнікамі, падумайце аб магчымасці выкарыстаць альтэрнатыўныя сэрвісаў, падрыхтаваных праваабарончымі ініцыятывамі: Blip.tv замест YouTube; riseup.net замест Gmail. Калі вы маеце тэхнічныя рэсурсы, можна запусціць уласныя вэб-сэрвісы.

Калі вы карыстаецеся камерцыйнымі платформамі, то прытрымлівайцеся мераў  перасцярогі, каб засцерагчы сябе ад зламыснікаў, якія ведаюць, як знаходзіць прыватную інфармацыю на падобных сэрвісах. Гэта тычыцца ў першую чаргу сайтаў сацыяльных сетак, такіх як Facebook ці MySpace. Вывучыце спосабы захавання канфідэнцыйнасці, якія прапануюць гэтыя платформы, і прадумайце, якія тыпы звестак пра вас ці вашу арганізацыю вы можаце ненаўмысна абнародваць, напрыклад: вашае сапраўднае імя, месца жыхарства, месцы вашых падарожжаў, падрабязнасці надыходзячых падзеяў ці сходаў. Калі падобную інфармацыю збіраць на працягу доўгага часу, яна можа стварыць карціну вашых звычак ці дэталяў працы.

Адным з прыдатных метадаў з’яўляецца стварэнне некалькіх акаўнтаў на любым Інтэрнэт-сэрвісе, якім вы карыстаецеся, што дазволіць вам карыстацца рознымі акаўнтамі ці профілямі для розных праектаў, і захоўвацьтэставыя акаўнты, якія вы можаце выкарыстоўваць, каб “шпіёніць” за сабой. Ваша канфідэнцыйнасць будзе лепш захавана, калі вы будзеце мець розныя магчымасці кантраляваць узровень доступу да інфармацыі  вашага профілю, напрыклад, праз вэб-пошук ці асоб, якія маюць асаблівае права  доступу.

**ПАРОЛІ**

Большасць Інтэрнэт-рэсурсаў выкарыстоўвае адзін пароль для забеспячэння вашага акаўнту. Калі асоба ці арганізацыя-зламыснік даведаюцца гэты пароль, не важна наколькі вы давяраеце сеткавым адміністратарам ці як сур’ёзна ставіцеся да захавання сваёй прыватнасці, – вы адразу згубіце сваю канфідэнцыйнасць і ананімнасць.

Менш вядомыя спосабы ўзлому паролю: нехта можа інсталяваць на вашым кампутары шкодную праграму, якую вы выкарыстоўваеце для ўваходу на бяспечны сайт. Альбо нехта можа назіраць за вашым Інтэрнэт-злучэннем, калі вы ўваходзіце на небяспечны вэб-сайт. Каб абараніць сябе ад атак першага тыпу, карыстайцеся сваім уласным кампутарам ці кампутарам даверанай асобы і правярайце абнаўленні аператыўнай сістэмы і антывірусных праграм. Каб засцерагчыся ад атак другога тыпу, найбольш папулярныя вэб-серверы электроннай пошты, сацыяльных сетак, блогінгу, мапаў, відэа-платформаў выкарыстоўваюць бяспечныя злучэнні HTTPS. Вы можаце праверыць, ці мае ваша старонка бяспечную сувязь, упісаўшы: 'https://' (замест толькі 'http://') у адрасны радок у вашым браўзеры. Шмат якія вэб-інструменты, тым не менш, ужываюць HTTPS выключна дзеля таго, каб засцерагчы паролі, праз якія вы ўваходзіце на іх сайт ці пераходзіце на іншы. У выніку, калі нехта будзе сачыць за вашымі сувязямі дастаткова доўга, ён даведаецца, што вы захоўваеце на гэтым сайце. Найлепшай абаронай будзе выкарыстанне вэб-інструментаў, якія выкарыстоўваюць HTTPS для ўсіх старонак.

**АБМІНУЦЬ ЦЭНЗУРУ**

Вы можаце выкарыстоўваць проксі-серверы, прылады для падману цэнзуры ці праграмы, якія забяспечваюць ананімнасць, напрыклад, Tor, каб схаваць свае асабістыя дадзеныя ад вэб-сайтаў, на якія вы ўваходзіце, ці абмінуць Інтэрнэт-фільтры. Гэтыя прылады карысныя, калі вы хочаце мець доступ да заблакаваных вэб-сайтаў; напрыклад, для даследавання ці атрымання абнаўленняў на вэб-платформах кшталту Facebook.

**ЗАСТАЦЦА АНАНІМНЫМ У СЕТЦЫ**

Праграмы, якія забяспечваюць ананімнасць, напрыклад як Tor, карысныя калі вы не хочаце каб выявілася, якія вэб-сайты вы наведалі. Tor замяняе вашыя злучэнні паміж некалькімі выпадковымі кампутарамі, дзеля таго каб нават ваш Інтэрнэт-правайдар ці назіральнікі на дзяржаўным ўзроўні не ведалі, што вы робіце ў Інтэрнэце. Тым не менш, не карыстайцеся Tor'ам пры перасылцы ці атрыманні далікатнай інфармацыі на небяспечны вэб-сайт ці з яго. Калі вы не звязаныя з сайтам, які падтрымлівае HTTPS, мажліва, што адзін з гэтых кампутараў зможа праглядзець кантэнт, які вы сцягваеце. Tor дастаткова бяспечны, але з цягам часу ён можа запаволіць вашае Інтэрнэт-злучэнне.

## Мабільныя тэлефоны

Праваабаронцы па ўсім свеце выкарыстоўваюць мабільныя тэлефоны , але часта яны ўтрымліваюць значны аб'ём інфармацыі, канфідэнцыйнасць якой мусіць быць захавана. Акрамя адраснай кнігі, у мабільных тэлефонах можа захоўвацца гісторыя тэлефанаванняў, календары, SMS-паведамленні і email'ы.

Падумайце пра інфармацыю, якая захоўваецца на вашым тэлефоне, найперш таму, што тэлефоны дастаткова лёгка канфіскаваць. Напрыклад, вам, напэўна, няма патрэбы трымаць усе вашыя кантакты на мабільным тэлефоне, калі вы займаецеся далікатным праваабарончым пытаннем, таму вам трэба выдаляць інфармацыю з вашага тэлефону і SIM-карты так часта, як гэта магчыма. Для арганізацыі мерапрыемстваў і мабілізацыі сваіх сувязяў варта выкарыстоўваць ананімную, праплачаную SIM-карту і пры магчымасці мяняць тэлефонныя апараты. З прычыны таго, што пошук і фільтрацыю SMS-паведамленняў можна здзейсніць вельмі проста, трэба пазбягаць далікатных ключавых словаў пры адпраўцы тэкставых паведамленняў.

Увесь час пакуль уключаны мабільны тэлефон, яго можна выкарыстоўваць, каб сачыць за вашым месцам знаходжання. Людзі, якія накіроўваюцца на сустрэчу па далікатным пытанні, мусяць выключыць свае тэлефоны і выцягнуць батарэю перад тым як выйсці, уставіць батарэю і ўключыць тэлефон пасля вяртання дадому. Аператары мабільнай сувязі маюць доступ да гісторыі ўсіх званкоў: каму, калі і адкуль яны былі зробленыя. Аператары абавязаныя паводле закону запісваць і даваць дадзеныя па просьбе дзяржаўнага служачага, і могуць захоўваць запісы на працягу некалькіх год.

**ДЗЕЯННЕ: ВЫЯВІЦЬ РЫЗЫКУ НЕБЯСПЕКІ**

Выкарыстоўваючы пытанні, прыведзеныя ніжэй, ацаніце вашую рызыку небяспекі і вырашыце, якія сродкі вы можаце выкарыстоўваць, каб яе зменшыць.

1. **Я працую з далікатнай інфармацыяй.** Важна ведаць, ці вы працуеце з далікатнай інфармацыяй, якая можа быць аб'ектам увагі іншых асоб, здольных сачыць за вашымі дзеяннямі. Ці заангажаваныя вы ў дзейнасці, якую можна лічыць далікатнай ці шкоднай для урада, паліцыі, войска альбо прыватнай кампаніі? Калі так, вы ці іншыя моцна рызыкуеце пры невыкананні мераў бяспекі.
2. **Я працую з людзьмі, асабістыя дадзеныя якіх павінны захоўвацца ў таямніцы.** Быць можа, у вас захоўваецца далікатная асабістая інфармацыя пра людзей , якіх вы падтрымліваеце, напрыклад, звесткі пра сямейны гвалт, прымусовую працу ці выпадкі згвалтавання. Калі людзі даюць вам звесткі, якія могуць ўтрымліваць рызыку для іх, вы павінны гарантаваць захаванне таямніцы.
3. **Часам я размаўляю ў Інтэрнэце з людзьмі, якія займаюцца далікатнымі пытаннямі.** Нават калі вам асабіста не пагражае небяспека, але вы кантактуеце людзей, якія знаходзяцца пад рызыкай, вы можаце стаць аб'ектам пераследу для людзей, якія супрацьстаяць вашым кантактам. Гэта таму што людзі могуць выкарыстаць вас, каб атрымаць доступ да прыватнай інфармацыі іншых.
4. **Я праглядаю ці публікую змест, які можна лічыць далікатным.** Быць можа вы дзеліцеся інфармацыяй з праваабарончымі вэб-сайтамі ці публікуеце артыкулы супраць груп, якія, на вашу думку, не паважаюць правы чалавека. Нават простае наведванне пэўных сайтаў у Інтэрнэце можа выклікаць пагрозу для вас.

## Рэсурсы для захавання бяспекі і канфідэнцыйнасці ў Інтэрнэце

Дзе даведацца больш і спампаваць патрэбныя інструменты:

1. **"Бяспека пад рукой"** (Security in-a-box) быў створаны арганізацыяй Tactical Tech and Front Line, каб задаволіць патрэбы ў бяспецы і канфідэнцыйнасці праваабаронцаў у лічбавым свеце http://security.ngoinabox.org/
2. **"Лічбавая бяспека і канфідэнцыйнасць для праваабаронцаў"** (Digital Security and Privacy for Human Rights Defenders), падрыхтаваны Front Line дае патрэбную інфармацыю для ацэнкі і супрацьстаяння пагрозам лічбавай небяспекі. http://bit.ly/1aCkSs (frontlinedefenders.org)
3. **"Мабільны пад рукой"** (Mobiles in-a-box), падрыхтаваны Tactical Tech, дае ўсе патрэбныя звесткі па канфідэнцыйнасці і бяспеку выкарыстання мабільных тэлефонаў. http://mobiles.tacticaltech.org/security
4. **"Ананімны блогінг з Wordpress & Tor".** Global Voices стварылі гэты праваднік для падтрымкі праваабаронцаў, якія хочуць выкрыць праўду і выказацца онлайн, але адначасова моцна рызыкуюць. http://advocacy.globalvoicesonline.org/projects/guide/
5. **"Будзь ананімным у Інтэрнэце і абміні цэнзуру".** Tor быў распрацаваны для павялічэння вашай ананімнасці у Інтэрнэце, і ён можа таксама выкарыстоўвацца для таго, каб заблытаць Інтэрнэт-фільтры. Вы можаце спампаваць праграму на кампутар і запусціць яе з USB-носьбіта.



TACTICAL TECHNOLOGY COLLECTIVE