



ОПЕРАЦІЙНА БЕЗПЕКА ТА ОСОБИСТА СТІЙКІСТЬ: ОГЛЯД СИТУАЦІЇ У КРАЇНАХ СХІДНОГО ПАРТНЕРСТВА



ОПЕРАЦІЙНА БЕЗПЕКА ТА ОСОБИСТА СТІЙКІСТЬ: ОГЛЯД СИТУАЦІЇ У КРАЇНАХ СХІДНОГО ПАРТНЕРСТВА

Довідник з кібер-, інформаційних, операційних та особистих загроз, викликаних іноземними авторитарними режимами та внутрішньодержавними утисками

Автори

Грузія: Media Development Foundation – Маріам Патарідзе, Софі Гелава, Тінатін Гоголадзе

Молдова: IPIS - Інститут стратегічних ініціатив – Вікторія Оларі

Україна: Український кризовий медіа-центр – Любов Цибульська, Олександра Цехановська

Рекомендації з операційної безпеки: European Values Center for Security Policy team

Редактор

Андреа Міхальцова, Центр безпекової політики European Values



Цей звіт було створено за фінансової підтримки Європейської комісії. Європейська комісія не несе відповідальності за факти чи судження, наведені у цій публікації, та за будь-яке подальше використання інформації, що міститься у ній. Вся повнота відповідальності покладається на автора цієї публікації.

Авторські права: Сторінка 8: Juan Antonio Segal / Flickr, Сторінка 12: Veaceslav Bunescu / Flickr

1. ВСТУП

Цей звіт став результатом року співпраці між громадськими організаціями (ГО) й аналітичними центрами Центральної Європи та країн Східного партнерства (СхП). Він є частиною проекту з обміну досвідом та підвищення стійкості й самозахисту, який оцінює спроможність громадянського суспільства у Грузії, Україні та Молдові використовувати наданий Центром безпекової політики «European Values» протокол з операційної безпеки та виявлення незаконних методів впливу. У цьому документі ми адаптуємо цей підхід і застосовуємо його до політичних реалій країн СхП.

Автори здійснили ґрунтовне вторинне дослідження тематичних відкритих джерел інформації, соціологічних опитувань та журналістських розслідувань. Вторинне дослідження проводилося шляхом структурованих інтерв'ю з експертами з відповідної тематики та місцевими представниками влади. Співробітники медіа, а також експерти з міжнародної політики та питань безпеки від громадських організацій надали основну частину інформації. Враховуючи чутливість цієї теми, ми прийняли рішення не публікувати перелік імен респондентів – його можна отримати у команди редакторів Центру безпекової політики «European Values».

Наші дослідники сфокусувались на ситуації у сфері медіа в Грузії, Україні та Молдові.

У Грузії наявні деякі практичні кейси з вивчення деструктивного зовнішнього впливу, але кількість детальних та порівнювальних експертних оцінок, що стосувалися б всього масштабу такого впливу, – незначна. Відповідно, практично відсутні конкретні політичні рекомендації для кампаній із захисту громадських інтересів, які проводить громадянське суспільство. Ряд держав поза межами ЄС та НАТО здійснюють деструктивний вплив у Грузії шляхом дипломатичної діяльності, тиску в енергетичній та економічній політиці, через застосування інформаційної зброї та підтримку місцевих маргінальних чи більш масових груп, які мають потенціал до підривної діяльності. Пострадянські країни на кшталт Грузії особливо вразливі до такого шкідливого впливу, який не тільки добре задокументований у звітах США та ЄС, але й відчутний у суспільстві; так званий процес «бордеризації» (від англ. «border» - кордон, прим. перекладача) спричинив для грузинів цілу хвилю відключень електроенергії. Ворожі дії, вчинені у Грузії за посередництва окремих неурядових громадських організацій (НГО), медіа та агентів впливу й політичних сил, спрямовані на дискредитацію процесу євроатлантичної інтеграції в країні та зростання скептицизму щодо її демократичного розвитку. Останні президентські вибори, що пройшли 28 жовтня 2018-го року, продемонстрували, наскільки тісно деякі виборчі кампанії були пов'язані з корупцією та дезінформацією, що перешкоджають діяльності громадських організацій¹.

В Україні перед тими, хто прагне підзвітності влади, також постає чимало викликів. Незважаючи на те, що НГО вибороли можливість

1 Crosby, Alan. "Sex, Lies, And Audiotape: Just Another Election Campaign In Georgia." *RadioFreeEurope/RadioLiberty*. Accessed on October 24, 2018. <https://www.rferl.org/a/sex-lies-and-audiotape-presidential-election-campaign/29561804.html>

вільно і відкрито займатись питаннями публічної політики під час Революції гідності, останнім часом (особливо наприкінці 2018 року, за рік до президентських та парламентських виборів) вони почали відчувати все більший тиск з боку держави. З метою дискредитації громадського активізму, влада ініціювала новий закон, що вимагає від активістів у сфері боротьби з корупцією публічно декларувати свої статки². Після жорсткої критики та широкого невдоволення з боку самих активістів, від цієї ідеї відмовились. Деякі НГО та громадські активісти зазнали безпосередніх фізичних нападів та словесних образ. Особливо складна ситуація у східних регіонах України, де корумпована та проросійська місцева влада й поліція не переймаються з приводу фізичних нападів на журналістів. Найбільш яскравим прикладом є історія антикорупційної активістки з Херсону Катерини Гандзюк, яку облили сірчаною кислотою. Гандзюк критикувала поліцію та правоохоронні органи й засуджувала корупцію в регіональному управлінні Міністерства внутрішніх справ. Вона привернула широку увагу до декількох випадків залученості поліції в корупційні процеси. Катерина загинула від отриманих опіків через 3 місяці після нападу.

Представники громадянського суспільства втратили позиції й у Молдові³, особливо після 2016-го року, коли відбулась зміна уряду, який перейшов під повний контроль Демократичної партії Молдови. У 2017-му міністерство юстиції спробувало впровадити закон, що заборонив би політичну діяльність та діяльність, пов'язану з підтримкою певних змін до законодавства⁴ тим НГО, які отримують закордонне фінансування. Такі суперечливі статті були включені до законопроекту наприкінці березня 2018-го року, але пізніше від них відмовилися. Після своєї критики сумнівних змін у виборчій системі, молдовські НГО зазнають постійних атак з боку державних посадовців та інших осіб/організацій, пов'язаних з правлячою партією⁵, включно з засобами масової інформації, блогерами та Інтернет-тролями. Деякі з молдовських НГО заявили про здійснення на них атак у період з 2016-го по 2018-й роки. Вони включали наклепницькі звинувачення у зв'язках з особами, яких у 2014-му році було засуджено за банківське шахрайство обсягом 1 мільярд євро, відоме також як «скандал з «Пральнею». Нещодавній яскравий випадок стосується парламентського запиту стосовно поїздки, здійсненої до Європейського парламенту⁶ декількома молдовськими активістами, журналістами та двома відомими опозиціонерами, яку про спонсорувала польська НГО Фонд «Otwarty Dialog». Парламентарі припустили, що Фонд є російською маріонеткою, яка спрямовує свої дії на дестабілізацію політичної ситуації в Молдові, і частина з них висловила думку про те, що поїздка активістів

2 "Ukrainian Civil Society Unites to Counter Mounting Threats." *Freedom House*. Accessed on April 18, 2018. <https://freedomhouse.org/article/ukrainian-civil-society-unites-counter-mounting-threats>

3 Macrinici, Sorina."Shrinking space for Civil Society in Moldova." *The Soros Foundation Moldova*. Accessed on April, 2018. <https://www.soros.md/files/publications/documents/Civil%20Society%20Macrinici.pdf>

4 RFE/RL's Moldovan Service. "Moldovan NGOs Reject Proposed Ban On Foreign Funding" *RadioFreeEurope/RadioLiberty*. Accessed on July 12, 2017. <https://www.rferl.org/a/moldova-ngos-reject-foreign-funding-ban/28612337.html>

5 Macrinici, Sorina."Shrinking space for Civil Society in Moldova." *The Soros Foundation Moldova*. Accessed on April, 2018. <https://www.soros.md/files/publications/documents/Civil%20Society%20Macrinici.pdf>

6 Dulgher, Maria."An outline of the 'Open Dialog' scandal. PAS and DTPP in the gunsight of the Moldovan Parliament." *Moldova.org*. Accessed on November 13, 2018. <https://www.moldova.org/en/outline-open-dialog-scandal-pas-dtpp-gunsight-moldovan-parliament/>

потребує розслідування на предмет державної зради. Такі операції з дискредитації нерідко супроводжуються публікацією особистих електронних листів активістів та їхньої переписки у різноманітних месенджерах, що вказує на вразливість критиків уряду до кібератак.

Загальна ситуація, в якій перебувають НГО всіх трьох країн, є критичною. Мало що робиться для їхньої підтримки. З урахуванням цього, Центр безпекової політики прийняв рішення збільшити рівень поінформованості у цих середовищах та поділитись кращими практиками з операційної та особистої безпеки, напрацьованими у консультаціях з низкою експертів з безпекових питань.

Спираючись на категоризацію загроз, ми виділили основні перешкоди для сталої діяльності НГО та розробили наступні рекомендації.

2. МЕТОДОЛОГІЯ: КАТЕГОРИЗАЦІЯ ЗАГРОЗ ТА ПРОПОЗИЦІЇ ВІДПОВІДЕЙ

КАТЕГОРІЯ	ЗАГРОЗА	ЯК ДІЯТИ	ОПИС ЗАГРОЗИ	ПРИКЛАД УСНОЇ ЧИ ПИСЬМОВОЇ ПОГРОЗИ
1	Неадресні повідомлення, що містять образи або натяк на погрозу	Напишіть листа визначеній контактній особі ⁷ зі своєї організації того ж дня ⁸ .	Неадресне повідомлення, що містить грубу й негативну характеристику організації, без конкретної погрози або з непрямою погрозою.	«Ви брехуни, яким платить казна-хто. Навчіться працювати своїми руками. Євреї та ідіоти погано закінчать. Ми з вами розберемося».
2	Адресні повідомлення, що містять натяк на погрозу	Напишіть листа визначеній контактній особі зі своєї організації того ж дня, особисто відзвітуйтесь перед своїм керівником або менеджером з питань безпеки.	Адресне повідомлення з натяком на погрозу, відправлене особисто людині або з вказівкою на цю людину, без уточнення погрози/з натяком на погрозу; анонімні дзвінки без прямих погроз.	«Як ти смієш так зневажати Президента, примітивне ти створіння? Начувайся. З нетерпінням чекаю, коли всі ваші фінансовані США офіси згорять. Я знаю, де вони знаходяться, придурки».
3	Адресні повідомлення загрозливого характеру або безпосередні погрози	Негайно зателефонуйте своєму керівнику або менеджеру з питань безпеки вашої організації.	Повідомлення, адресоване конкретній особі, що включає конкретну погрозу проти цієї людини або її близьких. Містить особисту інформацію (адресу, ім'я) та безпосередню погрозу.	«Попередження тобі було недостатньо, так? Схоже, доведеться використати інші «аргументи», свиня. Почекай-но – я знаю, де ти живеш, на Новакова 3».
4	Фізичний напад	За необхідності зв'яжіться з поліцією. Негайно зателефонуйте своєму керівнику або менеджеру з питань безпеки вашої організації.	Людина має обґрунтовану підозру, що її переслідують, залякують; спроба нападу або безпосередній фізичний напад.	Відчуття, що за Вами стежать на вулиці. Будь-які, навіть неявні, спроби залякування (незнайома особа, що говорить «Зупинись, бо інакше...» та йде).

⁷ Для подібних випадків варто мати спеціальну електронну скриньку, листи з якої автоматично пересилаються менеджеру з питань безпеки.

⁸ Каталогізація корисна на майбутнє, якщо поведінка особи стає більш агресивною.

3. СТРУКТУРА ДЖЕРЕЛ НАЙБІЛЬШ ПОШИРЕНИХ ЗАГРОЗ У ДОСЛІДЖУВАНИХ КРАЇНАХ

	МОЛДОВА	ГРУЗІЯ	УКРАЇНА
КІБЕРБЕЗПЕКА	<ul style="list-style-type: none"> Атака на відмову в обслуговуванні (DDoS) (сайт недоступний) Фішинг (фальшиві електронні листи та посилання) 	<ul style="list-style-type: none"> DDoS (сайт недоступний) Фішинг (фальшиві електронні листи та посилання) Програма-вимагач (англ. ransomware - ransom — викуп і software — програмне забезпечення – прим. перекладача) (шифрування даних) Втрата даних (документів, переписки) 	<ul style="list-style-type: none"> DDoS (робота організації паралізована у коротко- та середньостроковій перспективі) Фішинг Втрата даних (документи)
ІНФОРМАЦІЙНА БЕЗПЕКА	<ul style="list-style-type: none"> Витік паролів (Yahoo, Facebook) Злам електронних скриньок (розкриття комунікацій, викрадення даних) Дискредитація онлайн (неправдиві чутки, брехня, образи тощо) «Крадіжка особистості» онлайн (вдавання іншими особами представників організації) 	<ul style="list-style-type: none"> Витік персональних даних (адреса, номер телефону тощо) Витік паролів (Yahoo, Facebook) Злам електронних скриньок (розкриття комунікацій, викрадення даних) Дискредитація онлайн (неправдиві чутки, брехня, образи тощо) «Крадіжка особистості» онлайн (вдавання іншими особами представників організації) Викрадення особистих матеріалів з накопичувачів пам'яті для подальшого шантажу (особливо фотографії та відеозаписи дітей і неповнолітніх) 	<ul style="list-style-type: none"> Злам електронних скриньок (розкриття комунікацій, викрадення даних) Дискредитація онлайн (неправдиві чутки, брехня, образи тощо) Створення фейкових акаунтів організації та людей у соціальних медіа Атаки в рамках дезінформаційних кампаній та операцій Утиски з боку місцевої влади (використання організацій для політичних цілей, утиски з боку правлячої партії)
БАЗОВИЙ ЗАХИСТ ВІД ЗАСОБІВ РОЗВІДКИ	<ul style="list-style-type: none"> Підозріла діяльність у ближньому колі осіб (шпигунство, випитування інформації, недоречна зацікавленість тощо); Вербування ворожими спецслужбами (прямі пропозиції, надання преференцій тощо); Запрошення на (фейкові) інтерв'ю; Прослуховування/спостереження за допомогою спеціального обладнання на телевізійній компанії. 		
ОСОБИСТА (ФІЗИЧНА) БЕЗПЕКА	<ul style="list-style-type: none"> Залякування (погрози, утиски) Шантаж Акти вандалізму 	<ul style="list-style-type: none"> Залякування (погрози, напади) Шантаж Легкі травми (синці, порізи, садна) 	<ul style="list-style-type: none"> Переслідування під час поїздок закордон (затримання в Росії, Білорусі, Молдові, Вірменії) Акти вандалізму (пограбування офісу)



УКРАЇНА

4. УКРАЇНА

Контекст

Протягом 4 місяців, ми залучили 10 громадських організацій до проходження опитування щодо сучасних викликів у сфері кібербезпеки та інституційної спроможності подолати такі виклики. Зважаючи на розвиненість «третього сектору» в Україні, згода відносно небагатьох респондентів та загальна неготовність з боку багатьох представників НГО та/або активістів взяти участь в опитуванні показова вже сама собою. Ми припускаємо, що багато з них відмовилась від опитування саме через ті фактори, які дослідження мало на меті виявити, - занепокоєння щодо безпеки персональних даних та збереження їхньої конфіденційності в процесі роботи.

Якщо така гіпотеза відповідає дійсності, це свідчить про необхідність підвищувати рівень обізнаності у сфері та вибудовувати довіру під час інформування респондентів про цілі досліджень, особливо коли справа стосується все ще маловідомої площини кібербезпеки. Більше того, потенційні респонденти мають продемонструвати не тільки розуміння та знання існуючих викликів у сфері безпеки і мати довіру не лише до партнерів, з якими вони діляться інформацією, але і до їхніх безпекових спроможностей, оскільки відомі випадки хакерських атак і «зливів» сенситивної інформації, що завдали шкоди не лише особі, що зазнала атаки, але й тим, з ким вона підтримувала близькі контакти.

Усі 10 залучених організацій мають схожий досвід, працюючи у громадському секторі з акцентом на протидію дезінформації та пропаганді або, меншою мірою, на захист прав людини. Але лише того факту, що ці організації є значною мірою обізнаними щодо кібер- та інформаційних викликів, недостатньо для екстраполяції на увесь «третій сектор» в Україні та припущення, що він загалом є спроможним до ефективного реагування на них: зазначені організації й самі можуть мати недостатньо навичок щодо виявлення подібних загроз. Враховуючи це, можна сказати, що зібрані дані свідчать про наступні тенденції:

Підготовка у сфері операційної безпеки

Більшість респондентів зазначили, що не мають підготовки у сфері операційної безпеки, або рівень такої підготовки є недостатнім. Ті, хто отримав будь-яку освітню допомогу з цього питання, як правило отримували її у формі протоколів та/або інструкцій, які, навіть за умови правильного розуміння та застосування, є менш дієвими, ніж практичне навчання у формі тренінгів. Одна із залучених організацій засвідчила, що, у той самий час як вона проводить тренінги з питань безпеки, вона сама прагнула б підвищити рівень власної стійкості. Це свідчить про наявність дворівневої проблеми: лічені постачальники відповідної інформації і самі можуть не мати у своєму розпорядженні найкращих та найновіших інструментів протидії загрозам, ділячись з іншими обмеженим досвідом і все ще залишаючись вразливими.

Наявність протоколу операційної безпеки

Лише двоє організацій-респондентів відповіли, що мають протокол з операційної безпеки. Одна з них зазначила, що намагається використовувати протокол, запропонований третьою стороною, але навіть за умов коректного застосування вищезгаданий брак практичних навичок з дотримання такого протоколу все ще залишає організацію вразливою. Інші учасники не мають чітких інструкцій та покладаються виключно на власні ресурси.

Кризовий менеджмент у випадках порушення інформаційної безпеки

Лише один респондент відповів, що у такому випадку звернувся би до IT-відділу в його/її організації, що свідчить про брак технічних спеціалістів, здатних впоратись з потенційними кібератаками. Більшість стверджує, що звернулися б за допомогою до власних колег або ж до міжнародних партнерів. Не маючи достатньо обізнаних союзників, такі організації залишаються надзвичайно вразливими до кібератак. Міжнародна допомога не є широкодоступною та часто не адаптована до тих інструментів нападу, що використовуються в українському медійному просторі. Прикметно, що довіра з боку НГО до правозахисних органів настільки низька, що лише двоє з респондентів згадали їх як тих, до якого можливо звернутись за допомогою. Незалежно від того, яких саме партнерів вони мають, всі учасники опитування вказали на необхідність додаткових тренінгів з безпеки, здебільшого стосовно інформації, що має відношення до робочого процесу та цифрової сфери, але також і для підвищення особистої безпеки. Окрім того, їм бракує необхідних людських ресурсів, таких як IT-спеціалісти, до яких вони могли б звернутись з різними безпековими запитаннями.

Виклики у сфері безпеки

Кібербезпека

Більшість респондентів висловила занепокоєння щодо можливого витоку даних, втрати персональних даних, DDoS, фішингу та інших типів кібератак. Надійне збереження даних є ключовою потребою, враховуючи тиск, з яким напряду або опосередковано зіткнулися ціла низка організацій. Враховуючи низьку готовність до інформаційних воєн та обмеженість фінансових ресурсів у їхньому розпорядженні, не дивно, що НГО відзначають саме пов'язані з кібербезпекою виклики як найбільш значущу загрозу.

Інформаційна безпека

Найбільше занепокоєння у цій сфері викликають таргетовані кампанії з дискредитації та (спричинені ними) репутаційні втрати. Проблема безпеки персональних даних та їх можливої втрати у разі зламу каналів комунікації також має велике значення.

Особиста безпека

Декілька організацій висловили занепокоєння через можливість арешту їхніх представників у країнах, що мають тісні зв'язки з Російською Федерацією (наприклад, у Білорусі, як вже траплялося з членами деяких українських НГО). Цілком зрозуміло, що вони пригадували випадки залякування, прямих особистих погроз (включно з анонімними), крадіжок, нападів та пошкодження майна, від яких постраждали їх колеги, безвідносно того, чи були два останні інциденти політично мотивованими.

Майбутні загрози

Більшість респондентів очікують інформаційних загроз, спрямованих на дискредитацію відповідних організацій та завдання їм репутаційних збитків. В країні, що стала жертвою збройної агресії, багатьом знайома підбивна та агресивна діяльність уряду Російської Федерації, але є занепокоєння з приводу того, що і власна влада може вдатися до помсти, якщо висвітлювати її дії негативно. Опитані мають застереження стосовно спроможності новообраної (у 2019 році) влади запровадити нову політику у сфері комунікацій, що може суттєво обмежити активність НГО, а також – що влада може почати залучати спецслужби і створювати кіберзагрози, такі як витоки персональних даних та залякування.

Джерела загроз

Як зазначено вище, деякі з опитаних мають побоювання стосовно того, що уряд України, особливо представники президентської партії «Слуга народу», президентського оточення та проросійські діячі, створюватимуть перешкоди для їхньої роботи. Зовнішні загрози, зокрема, з боку Російської Федерації, складають іншу причину для занепокоєння, що пояснюється переважним фокусом на деструктивному російському впливі у середовищі респондентів. Місцеві кримінальні угруповання, що можуть включати й державних службовців, які зловживають своїм становищем, нерідко здійснюють тиск на місцевих представників громадянського суспільства, які намагаються викрити факти існування подібних кримінальних груп на місцях.



МОЛДОВА

5. МОЛДОВА

Інститут стратегічних ініціатив (ICI) провів опитування щодо викликів, пов'язаних з кіберзалякуванням та кібербезпекою, з якими зустрічаються журналісти, НГО, активісти та представники медіа в Республіці Молдова, які працюють з темами російського впливу, пропаганди, дезінформації, корупції тощо. Для заповнення опитувальника було обрано десять респондентів. Аналіз результатів опитування свідчить про наступне:

Підготовка у сфері операційної безпеки

Майже всі респонденти зазначили, що не отримували жодної підтримки у сфері операційної безпеки від місцевих або міжнародних організацій. Деякі з них відповіли, що займалися самоосвітою, і ще частина зазначили, що не хотіли б розголошувати таку інформацію поза межами своєї організації.

Наявність протоколу операційної безпеки

Можна зробити висновок, що практика використання інструкцій, протоколів чи процедур з операційної безпеки не є поширеною в середовищі НГО, активістів та представників медіа Республіки Молдова. Тим не менш, є і деякі позитивні аспекти. Більшість організацій намагається захистити себе шляхом використання стандартних безпекових рішень, пропонованих Google та Facebook, таких як двофакторна автентифікація, антивірусне програмне забезпечення, файрвол тощо.

Кризовий менеджмент у випадках порушення інформаційної безпеки

Більшість респондентів зазначила, що у разі кризових ситуацій, пов'язаних з порушенням безпеки, не довіриться державним інституціям, таким як поліція або прокуратура, і загалом намагається уникати контактів з ними. Більш того, деякі зазначили, що відчують ворожість з боку державних інституцій та мають досвід цинічної поведінки з боку поліції та прокуратури. Цікаво, що у разі нападу, утисків та шантажу, найкращим способом захистити себе організації вважають інформування широкого загалу про подібні інциденти, намагаючись/сподіваючись у такий спосіб уникнути їхнього повторення.

Виклики у сфері безпеки

Кібербезпека

Більшість респондентів назвали основними викликами у сфері безпеки «тролінг» та онлайн-цькування з боку пов'язаних з державою акторів. Ці організації займаються розслідуванням та висвітленням випадків корупції, конфлікту інтересів та зловживання службовим становищем. Респонденти відмітили, що мали досвід атак на їхні веб-сайти та знаходили підозріле обладнання поблизу своїх офісів.

Інформаційна безпека

Майже всі опитані мали досвід витоку паролів на Facebook та зламу електронних скриньок. Окрім того, у наших респондентів викликає занепокоєння цілеспрямована дискредитація журналістів, активістів НГО тощо шляхом дублювання або створення фейкових акаунтів (онлайн-«крадіжка особистості»). Така практика набрала обертів протягом парламентської виборчої кампанії у лютому 2019-го року, коли значна кількість журналістів та громадських активістів з'ясували, що на різних публічних сторінках від їхнього імені роздають коментарі інші особи. У цьому випадку Facebook прийняв безпрецедентне рішення закрити 168 акаунтів, 28 сторінок та 8 акаунтів в Instagram у Молдові, частина яких належала державним посадовцям, оскільки їх запідозрили у поширенні фейків, політичної пропаганди та некоректної інформації перед виборами. Відділ новин Facebook заявив, що, попри спроби з боку осіб, що вдавалися до такої діяльності, приховати свою особистість, зроблений вручну аналіз засвідчив: частина цієї діяльності виконувалась співробітниками молдовського уряду.

Особиста безпека

Низка респондентів розповіли, що, працюючи у цій сфері, стикалися з погрозами, у тому числі й з фізичним залякуванням, пошкодженням їхніх авто. Частину цих дій вчинили невідомі особи, ще частину – представники правоохоронних органів. Так відбулося, зокрема, під час протесту «Осигуру Guguță» - співробітники поліції примусили активістів залишити місце проведення акції, відібравши у них плакати та інші матеріали. Більш того, пов'язані з владою телевізійні канали намагались розповсюджувати недостовірні новини про протестний рух, приводячи у місця протесту сумнівних осіб та п'яниць. Через це в активістів виникли проблеми з особистою безпекою.

Майбутні загрози (1-3 роки)

Більшість респондентів вже стикалися з шантажем, переслідуванням, судовими позовами, залякуванням та фізичними нападами. Вони також звернули увагу на деякі законодавчі зміни, що можуть вплинути на їхню повсякденну діяльність: закон про НГО, закон про свободу медіа, закон про закордонні гранти, закон про доступ до інформації. Враховуючи тематику, з якою вони переважно працюють (фінансові злочини, корупція, зловживання службовим становищем), це може загрожувати їм шантажем, переслідуванням та навіть незаконним затриманням членів родин. Інші потенційні загрози можуть включати переслідування з боку фіскальних служб чи навіть

законодавчого органу (у період проведення цього опитування, парламент виступив з ініціативою заборонити зовнішнє фінансування для молдовських НГО).

Джерела загроз

Усі респонденти вказали на те, що основним джерелом загроз є внутрішні актори, особливо уряд, який діє через правоохоронні органи або осіб, пов'язаних з молдовською владою, які вели кампанії з фальсифікації на Facebook, використовуючи тактики сумнозвісної російської «фабрики тролів». Такий стан справ також створює потенційну загрозу зовнішнього втручання, оскільки агенти Кремля знають, як використовувати місцеві слабкості у таких ситуаціях.



ГРУЗИЯ

6. ГРУЗІЯ

Media Development Foundation (MDF) провела опитування щодо викликів, пов'язаних з кіберпереслідуванням та кібербезпекою, з якими зустрічаються журналісти, НГО, активісти та представники медіа, які працюють з темами російської пропаганди, корупції та прав людини. Дослідження методом комбінованого анкетування (з «закритими» та «відкритими» запитаннями – прим.пер.), у якому взяли участь 24 респонденти, виявило наступні тенденції:

Підготовка у сфері операційної безпеки

Більшості респондентів не пропонували тренінги чи іншу процедурну допомогу у сфері операційної безпеки. Декілька респондентів брали участь в тренінгах з цифрової безпеки, під час яких не було приділено достатньо уваги механізмам уникнення загроз, які необхідні цим конкретним особам/організаціям.

Наявність протоколу операційної безпеки

Більшість респондентів не використовують протоколи операційної безпеки у своїй діяльності. Лише незначна частка з них розробила власні внутрішні правила.

Кризовий менеджмент у випадках порушення інформаційної безпеки

Більшість респондентів відповіли, у що разі інцидентів, пов'язаних з кібербезпекою, вони звертаються до IT-відділу організації, Бюро з питань кібербезпеки Міністерства оборони та відділу реагування на кіберзагрози Міністерства внутрішніх справ. Після того, як було виявлено ознаки злочину, вони звертаються до поліції. У разі інцидентів, пов'язаних з інформаційною безпекою (порушення правил використання персональних даних), респонденти повідомляють про них Інспектору з питань захисту персональних даних або, рідше, – омбудсмену.

Деякі респонденти не мають інформації стосовно того, до кого звернутись за допомогою, щоб вирішити проблему і вжити належних заходів.

Майже всі респонденти потребують навчання у сфері цифрової (паролі, безпека внутрішніх мереж, виявлення програм-вимагачів) та інформаційної безпеки (захист персональних даних). Більшість респондентів відзначили важливість розвитку навичок, що допоможуть ефективно вирішувати проблеми, що виникають під час різних кризових ситуацій. Декілька респондентів також зазначили, що потребують допомоги у плануванні сталої діяльності своїх організацій.

Виклики у сфері безпеки

Кібербезпека

Більшість респондентів називають основним викликом у сфері безпеки «тролінг» та онлайн-цькування з боку ультраправих груп та державних акторів. На особливу увагу заслуговує так званий «державний тролінг» у відповідь на критичні матеріали про діяльність уряду.

Вагомими проблемами називають також фішинг та хакерські атаки на офіційні веб-сайти організацій з метою отримання інформації. Веб-сайт проекту Myth Detector (www.eurocommunicator.ge) MDF у 2015-му році було двічі зламано Luxas Hacker. Під час першої атаки відслідкувати хакера було неможливо, але під час другої вдалося встановити, що IP-адреса зареєстрована в Туреччині. На завантажених на YouTube відео чітко видно адресу веб-сайту “Dark Mirror” <http://dark-mirror.org>. Цим посиланням послуговувався хакер під час атаки на веб-сайт.

Грузія зазнала масованих кібератак 28 жовтня 2019 року. Хакери обрали своїми цілями веб-сайти грузинського уряду, приватних компаній і медіа (TV Pirveli, Imedi, Maestro, Trialeti та Sakinform), а також неурядових організацій (Media Development Foundation).

Головні сторінки зламаних веб-сайтів замінили зображенням колишнього президента Грузії Міхеїла Саакашвілі з підписом «Я ще повернусь!» (англ. “I’ll Be Back”).

Зламані веб-сайти розташовувались на серверах Pro-Service, місцевого провайдера. Компанія заявила, що кібератака торкнулась близько 15 000 веб-сторінок. Міністерство внутрішніх справ оголосило про початок розслідування за статтями 284 та 286 Кримінального кодексу Грузії щодо неавторизованого доступу до комп’ютерних систем та неавторизованого використання комп’ютерних даних та/або систем.

Міністерство внутрішніх справ заявило, що «кібер-атака могла бути здійснена як зсередини країни, так і ззовні», а також що «слідчі дії виявили, що результатом кібератаки стало так зване «стирання» (англ. «defacement») веб-сайту – зміна візуального оформлення головних сторінок».

«Більшості компаній, що потрапили під атаку, послуги з хостингу надають приватні грузинські компанії. Стиль кібератак на кожен з веб-сайтів – ідентичний», зазначається у заяві.

Усі веб-сайти, розташовані на серверах компанії Pro-Service, відновили роботу 29 жовтня. .

Інформаційна безпека

Загальнопоширеною проблемою респонденти назвали цілеспрямовану дискредитацію з боку радикальних груп та державних «тролів» з метою підриву легітимності поширюваної ними інформації. У тому, що стосується інформаційної безпеки, більшість

опитаних наголошують на проблемі розкриття персональних даних (злам акаунтів, витоки інформації, розкриття комунікацій, онлайн «крадіжка особистості»).

Особиста безпека

Низка організацій зазнали нападів, погроз (фізичного насильства, зґвалтування) та агресії з боку ультраправих груп, позиції яких в останні роки посилюються. Опитані журналісти заявили про випадки фізичних нападів та пошкодження майна (пошкодження обладнання та авто). Декілька журналістів стали жертвами фізичного нападу просто через виконання своєї професійної діяльності.

Наприклад, журналіст Rustavi 2 TV Давід Ерадзе зазнав фізичного нападу з боку членів ультраправого руху «Грузинський марш» (2018-й рік); більш того, в його будинок стріляли, на балконі були знайдені гільзи – лише через те, що він готував телевізійний матеріал під час своєї професійної діяльності (2019-й рік).

На журналістів з Tabula напали в ресторані з вигуківанням образ на адресу їхніх релігійних переконань через роботу у виданні (2016 рік).

Окрім того, 39 представників різних медіа отримали фізичні пошкодження, виконуючи свої професійні обов'язки, під час розгону мітингу проти окупації 21 червня.

Майбутні загрози (у перспективі 1-3 років)

Більшість респондентів вважає, що протягом наступних 1-3 років продовжуватиметься тролінг та онлайн-переслідування з боку ультраправих груп і державних акторів, а також онлайн-дискредитація, розкриття особистих даних та погрози. На їхню думку, деякі організації/їхні представники можуть зазнати навіть фізичних нападів та арештів.

Джерела загроз

Серед основних джерел можливих загроз респонденти називають внутрішні – державні установи, найняті та заохочувані ними вороже налаштовані групи, та маргінальні актори, включно з «тролями». Основним витоким зовнішніх загроз респонденти називають кремлівських акторів та їхніх сателітів (як приватних осіб, так і організації), оскільки частина опитаних працює з проблематикою російських впливів.

Респонденти зазначили, що не отримували допомоги з боку міжнародних донорів/закордонних урядів для протидії цим загрозам.

7. ЩО МОЖНА ЗРОБИТИ? РЕКОМЕНДАЦІЇ ДЛЯ НГО ТА АКТИВІСТІВ

НГО варто використовувати базовий методичний посібник у сферах кібер-, інформаційної, контррозвідувальної та особистої безпеки.

Рівні сенситивності інформації

Загалом, ми розрізняємо три рівні сенситивності (чутливості) інформації. Основним критерієм є ступінь її політичної, особистої та безпекової важливості для організацій/осіб та їхньої безпеки. Таку класифікацію використовують для контролю виконання перевіреного часом «принципу необхідності»: інформація сенситивного характеру має надаватися тільки тим, кому з конкретної причини необхідно нею володіти.

РІВЕНЬ СЕНСИТИВНОСТІ	КРИТЕРІЙ ВАЖЛИВОСТІ	ДЕ МОЖЛИВО ОБГОВОРЮВАТИ ІНФОРМАЦІЮ ОСОБИСТО	ДЕ МОЖЛИВО ОБГОВОРЮВАТИ ІНФОРМАЦІЮ ОНЛАЙН
0	Базова операційна інформація, що не є чутливою з політичної чи безпекової точки зору; де-факто публічна інформація.	Будь-де	Будь-де: електронна пошта, Facebook тощо.
1	Внутрішня інформація (непублічна інформація політичного характеру, що не несе загрози національній безпеці або пов'язаним з такою інформацією людям).	На спеціально призначених зустрічах або один на один з відповідальною особою, <u>без використання електронних пристроїв</u> .	Лише через Signal (повідомлення або дзвінок) чи ProtonMail – не звичайна електронна пошта, SMS чи дзвінки.
2	Дуже сенситивна інформація (стосується питань національної безпеки, ідентифікує джерела сенситивної інформації, має потенціал призвести до політичного «вибуху»).	Лише на спеціально призначених зустрічах, один на один з відповідальною особою, <u>без використання електронних пристроїв</u> .	Ніде, тільки особисто без використання електронних пристроїв.

Кожен член організації повинен запровадити і дотримуватися заходів безпеки у п'яти сферах:

- Базовий кіберзахист пристроїв та профілів
- Безпека у соціальних мережах
- Безпека комунікацій
- Безпека даних
- Особиста безпека

Базовий кіберзахист пристроїв та профілів

а. Базові правила безпеки

Припускаємо, що Ви користуєтесь лише широко поширеними операційними системами. У випадку зі стаціонарними комп'ютерами мова йде про Windows та macOS, у випадку з переносними пристроями (наприклад, планшети та мобільні телефони) – iOS і Android. Продукти Apple (хоча й значно дорожчі) вважаються найбільш безпечними, за ними йде Android. Ми наполегливо рекомендуємо не використовувати продукти Lenovo.

і. Налаштування паролів

Правило №1: Використовуємо різні паролі для різних акаунтів (різні цифри, спеціальні символи тощо). На сторінці браузера Mozilla доступний короткий мануал з цього питання.

Правило №2: Пароль має складатись мінімум з 22 знаків з використанням літер, цифр та спеціальних символів.

Правило №3: Паролі варто змінювати раз на три місяці. Для зручності можна встановити нагадування на своєму календарі.

Правило №4: Паролі варто записувати тільки на папері (зберігаючи його у місці, про яке відомо тільки Вам, не на робочому місці; кожному паролю має бракувати принаймні одного знаку на випадок, якщо запис буде втрачено), ніколи не в текстових документах, що зберігаються на комп'ютерах. Виняток становлять менеджери паролів, такі як LastPass чи KeePas2. Іншим інструментом для зберігання паролів може бути так званий «електронний брелок» (для iOS – iCloud Keychain, для Windows – Smart Lock або 1Password), які ми рекомендуємо використовувати для двофакторної автентифікації чи шифрування дисків (див. нижче).

ii. Двофакторна автентифікація – згенерований код необхідно вводити разом з паролем

Правило №5: Двофакторна аутентифікація має бути ввімкнута на всіх сервісах, які дозволяють її використання. Код можна отримати або через SMS, або через мобільний додаток. Ми рекомендуємо не застосовувати аутентифікацію через SMS і налаштувати Google Authenticator. Це необхідно як мінімум для використання Facebook, Twitter, Google та інтернет-банкінгу. Ми рекомендуємо не використовувати технологію розпізнавання обличчя.

- На веб-сторінці показано QR-код, який можна просканувати через мобільний додаток. Після цього до нього прив'язується відповідний акаунт. Додаток показує новий унікальний код кожні 30 секунд, і його необхідно використати за цей час. Вам немає необхідності бути підключеними до Інтернету чи навіть мати телефонний сигнал на мобільному, аби використати додаток; ваш пристрій та сервер залишаються постійно синхронізованими після першого використання. Універсальні інструменти: Google Authenticator (iOS, Android), Authy.

Правило №6: Завжди виходьте з аканту після завершення роботи, так щоби будь-хто, хто працюватиме після Вас, мусив залогінитись знову. Ми рекомендуємо використовувати інший пароль та відбиток пальця для відкриття важливих додатків (Signal, Wickr Me, ProtonMail).

Правило №7: Ніколи не заходьте у свої основні профілі (Google, Facebook, інтернет-банкінг) з чужих пристроїв, якщо в цьому немає нагальної потреби. Якщо Ви були вимушені це зробити, пізніше змініть пароль. В особистих налаштуваннях Facebook варто ввімкнути повідомлення про логін з нерозпізнаних пристроїв, найкраще – через електронну пошту. Встановіть вбудований пароль на своєму пристрої Mac.

Правило №8: Якщо Ви отримали підозрілого електронного листа або приватне повідомлення, перешліть його своїм колегам з чітким попередженням (як у темі, так і у тілі листа) не відкривати його та надіслати на адресу cert.incident@nukib.cz. Спеціалісти з NUKIB допоможуть Вам у реалізації наступних кроків, якщо в них буде необхідність (наприклад, якщо у вкладенні була програма-вимагач тощо).

б. Антивірус

Правило №9: Операційні системи на кшталт Windows 10 уже мають вбудований антивірус. Загалом, немає необхідності встановлювати сторонній захист. Якщо Ви все ж ним користуєтесь, уникайте продукції Kaspersky Lab (є обґрунтована підозра, що компанія пов'язана з російськими розвідувальними службами), Huawei чи ZTE (є обґрунтована підозра, що вони пов'язані з китайськими розвідувальними службами). Ми рекомендуємо до використання Avast Antivirus чи Eset i, навпаки, радимо не користуватись китайськими антивірусними програмами (такими як Qihoo 360, Tencent PC Manager). Ми рекомендуємо використовувати дві антивірусні програми паралельно. Завантажте програму VirusScanner.

Правило №10: Основна частина кібератак здійснюється через електронні листи – за допомогою «фішингу». Основа функціонального захисту від вірусів полягає у тому, щоб не відкривати вкладення до електронних листів від невідомих адресантів. Будьте особливо уважні, коли приєднаний файл має такі розширення як .exe, .pkg, .dmg, чи .app. Більше того, не забудьте перевірити, чи дійсно відправник той, за кого себе видає, перед тим як відкривати приєднаний файл. Пам'ятайте, що навіть файли у таких форматах як .pdf чи .doc. можуть містити шкідливі елементи. За можливості не дозволяйте «використання маркосів» в Excel. Якщо хтось надсилає Вам посилання, було б непогано спершу скопіювати його на virustotal.com, що дасть хоч приблизне розуміння, чи варто цьому посиланню довіряти. Після цього застосуйте правило №8.

Якщо Ви переконані, що на вашому пристрої вже є шкідливе програмне забезпечення, найбезпечніший і найшвидший порядок дій – стерти диск та перевстановити операційну систему і програми, після чого дані можна скопіювати з резервного джерела (попередньо переконавшись, що воно не заражене).

Якщо Ви підозрюєте, що Ваші пристрої заражені, негайно запустіть сканування антивірусною програмою. Навіть якщо результати сканування будуть негативними, будьте проактивними, виконавши наведені нижче кроки. Якщо у Вас залишились підозри, запустіть інший антивірус.

Необхідні дії включають:

i. WINDOWS

Крок 1: Від'єднайте комп'ютер від мережі. Запустіть антивірусне сканування (бажано з зовнішнього носія з оновленим антивірусом).

Крок 2: увійдіть у безпечний режим. Це можна зробити, виключивши Ваш комп'ютер та запустивши його знову. Потім, як тільки Ви побачите щось на екрані, натисніть кнопку F8 декілька разів. Зазвичай це запускає меню розширених налаштувань запуску. Там Ви зможете вибрати безпечний режим та натиснути Enter.

Крок 3: Видаліть тимчасові файли. Поки Ви знаходитесь у безпечному режимі, тимчасові файли варто видалити через інструмент очищення диска. Для цього:

- Увійдіть у стартове меню;
- Всі програми/програми;
- Стандартні – Службові програми/Засоби адміністрування Windows (залежно від версії);
- Очищення диска;
- Прогортайте список файлів, які пропонується видалити, та оберіть тимчасові файли. Їх видалення може прибрати шкідливе забезпечення, якщо воно було запрограмоване на запуск після початку роботи комп'ютера.

Крок 4: Завантажте та запустіть антивірусний сканер. Якщо Ваш пристрій було заражено, Ваш антивірус не перехопив шкідливу програму. Вам варто завантажити (на інший комп'ютер) і перенести та встановити:

- Сканер, що працює у режимі реального часу, такий як безкоштовні AVG Antivirus або Avast, що відслідковують шкідливі програми, поки Ви використовуєте комп'ютер;
- Сканер операційної системи, що запускається за запитом користувача, на кшталт Microsoft Safety Scanner, але його необхідно кожен раз запускати вручну.

Для виявлення шкідливої програми може виникнути потреба запустити обидва типи сканерів. Залежно від типу антивірусної програми, можливо, доведеться підключитись до Інтернету та завантажити додатковий продукт. Також

можливо, що вірус доведеться видаляти вручну. Це варто робити лише у випадку, якщо Ви є досвідченим користувачем реєстру Windows і знаєте, як переглядати та видаляти системні й програмні файли.

Крок 5: Після видалення шкідливої програми, Вам необхідно буде відновити (з резервного носія) чи перевстановити пошкоджені файли чи програмне забезпечення.

с. Оновлення програмного забезпечення

Правило №11: Оновлювати програмне забезпечення – надважливо. Переконайтесь, що як на Вашому комп'ютері, так і на мобільному телефоні увімкнено автоматичні оновлення.

- Якщо у Вас встановлена старіша версія Windows (наприклад, 7 чи 8), необхідно зберігати налаштування оновлень за замовчуванням (наприклад, тримати автоматичні оновлення увімкненими). Якщо система хоче встановити оновлення, дайте на це дозвіл. У Windows 10 відсутній простий спосіб вимкнути оновлення (їх можна відкласти лише у Pro версії, і ми не рекомендуємо цього робити).
- Mac: система перевіряє наявність оновлень автоматично через додаток Mac App Store. Apple завжди надає найкращу підтримку тільки для останньої версії macOS. Увімкніть автоматичні оновлення в Mac/Про цей Mac/Оновлення/Розширені.
- Мобільні операційні системи: регулярно перевіряйте наявність оновлень у налаштуваннях системи та завжди майте найновішу її версію. Для iPhone ми рекомендуємо додаток iVerify, що допоможе Вам крок за кроком пройти усі необхідні безпекові процедури.
- Браузери за замовчуванням (Safari, Internet Explorer, Edge, чи Chrome на пристроях Android) зазвичай оновлюються автоматично разом з операційною системою. Сторонні браузери, такі як Chrome чи Firefox, оновлюються окремо, зазвичай автоматично. Якщо браузер пропонує Вам оновлення, Ви повинні негайно його встановити! Оновлений веб-браузер – це альфа і омега Інтернет-безпеки. Ми рекомендуємо встановити додаток "HTTPS Everywhere", який контролюватиме за Вас безпеку відвідуваних сайтів.

d. Як правильно блокувати та відслідковувати мобільні пристрої

Правило №12: Важливо мати цифровий або інший код для розблокування пристрою (пароль мінімум з 22-х знаків). Якщо пристрій має сканер для відбитку пальця, активуйте його.

- Важливо також налаштувати блокування Вашого ноутбука в такий спосіб, щоб він вимагав ввести пароль кожен раз, коли Ви його закриваєте та відкриваєте знову. Блокуйте свій ноутбук кожен раз, коли залишаєте його, навіть ненадовго (натисніть кнопку Windows + L).
- Придбайте плівку на екран, яка дозволить дивитись на нього тільки під прямим кутом та унеможливить спроби

незнайомих осіб побачити, що Ви пишете, з інших кутів. Коли Ви працюєте з сенситивною інформацією, звертайте увагу на своє розташування відносно вікон. Найпростіший спосіб отримати чужий пароль чи інші дані – саме зазирнувши через вікно.

Правило №13: Зазвичай пристрої мають функцію видалення усіх даних після визначеної кількості невдалих спроб їх розблокувати. Ми рекомендуємо активувати цю функцію. Більше того, варто захистити свою SIM-карту паролем, щоби було недостатньо просто вставити її в інший телефон.

Правило №14: Вкрай важливо тримати увімкненим відслідковування Вашого телефону. На iOS запустіть функцію «Знайти мій iPhone» (тут же Ви зможете знайти подальші інструкції; Apple також дає інструкцію на випадок, якщо Ваш телефон загубиться або буде вкрадений). Якщо Ви використовуєте Android, Вам необхідно встановити та активувати Android Device Manager.

- Втрата чи крадіжка пристрою: потрібно негайно запустити додаток на іншому пристрої або онлайн (Android Device Manager / iCloud), авторизуватись та спробувати встановити місцезнаходження свого пристрою. Виконуючи ці кроки, Ви можете також безпечно видалити всі дані, що зберігаються на пристрої, навіть якщо його зараз неможливо відслідкувати – дані будуть видалені, як тільки пристрій під'єднається до Інтернету.

Правило №15: Пристрої Apple також мають функцію під назвою «Блокування активації». Якщо функція «Знайти мій iPhone» увімкнена і Ви очистили пристрій за її допомогою, він все ще буде прив'язаний до Вашого акаунту, а отже, злодій не зможе продати його на чорному ринку. Пристрій залишатиметься прив'язаним до акаунту постійно, якщо тільки Ви не введете пароль особисто, або якщо він не стане відомий новому власнику – що за використання двофакторної автентифікації майже неможливо.

- Android: Якщо увімкнено Android Device Manager, Ви матимете доступ до всіх функцій з гарантування безпеки на Вашому телефоні.
- Сервіси на кшталт Find My iPhone чи Android Lost також дають Вам віддалений доступ до пристрою для видалення всіх даних у випадку втрати або крадіжки.

Правило №16: Важливо також бути обережними, використовуючи на мобільних пристроях Wi-Fi чи Bluetooth. Також варто обмежити кількість додатків, що мають доступ до Вашої геолокації, до мінімальної. Як правило, відповідні налаштування можна встановити у папці Параметри/Програми/Доступ. Пройдіться по усіх параметрах доступу та оцініть, чи він дійсно необхідний, відключивши його там, де у ньому немає потреби. Ми застерігаємо від використання hands-free (бездротових) приладів через Bluetooth (принтери, навушники), оскільки вони створюють безпекові ризики. Ми рекомендуємо придбати так званий «USB-запобіжник» *[спеціальний перехідний пристрій, що блокує доступ до «пінів», які дозволяють отримувати та відправляти дані – прим. перекладача]*, який гарантуватиме, що до Вашого пристрою потрапляє тільки електроенергія і нічого більше. Подібний спосіб отримати доступ до пристрою *[завантажити з нього дані або передати шкідливий код під час використання власником гаджету неперевіреного USB-порта – прим. перекладача]* дуже простий, навіть якщо його і не беруть до уваги.

Правило №17: Камеру та мікрофон на Вашому мобільному пристрої можна активувати дистанційно. Ніколи не беріть смартфон у місця, де він може бути використаний супротивником для збирання сенситивної інформації. Під час зустрічей, на яких така інформація обговорюється, відкладіть телефон і, якщо це технічно можливо, вийміть з нього акумулятор. Найкраще рішення – покласти всі електронні прилади у сумку, яку варто залишити на відстані 7-10 метрів від себе. У такий спосіб Ви зможете слідкувати за своїми речами, але пристрої не зможуть «підслухати» Вашу розмову. Окрім встановлення заглушки на камеру, ми також рекомендуємо взагалі відключити камеру на Вашому комп'ютері та завантажити додаток «Oversight», який регулює сторонній доступ до камери та мікрофону.

Правило №18: Найкраще – закривати камеру на ноутбучі та знімати заглушку тільки за необхідності. Те ж саме стосується телефону – закрийте камеру чохлам та знімайте його, якщо виникає така потреба.

е. Резервні копії та порядок дій в екстрених ситуаціях (втрата/крадіжка пристрою)

Правило №19: Ми рекомендуємо робити резервні копії особистих та робочих документів на зашифрованому зовнішньому носії, який безпечно зберігається у Вас вдома та від'єднаний від мережі. Компанія iStorage продає недорогі та якісно зашифровані зовнішні жорсткі диски. Сенситивну інформацію рекомендується зберігати на окремому чистому комп'ютері, який ніколи не підключається до Інтернету. Ми також рекомендуємо робити копію свого особистого календаря (бажано Google), що стане у нагоді, якщо виникне необхідність перевірити інформацію про події, які відбулись давно.

Правило №20: Існує велика кількість як безкоштовних, так і платних додатків для шифрування дисків. Нерідко рекомендують VeraCrypt.

Правило №21: Необхідно робити резервні копії тільки унікальних документів, які не підлягають відтворенню. У більшості випадків вони займатимуть не більше декількох сотень мегабайт. Переконайтесь, що ви робите резервне копіювання принаймні раз на місяць.

ф. У випадку втрати або крадіжки пристрою

Крок 1: Перевірте місцезнаходження свого пристрою через обраний Вами спосіб його відстеження. Якщо з'ясується, що Ви залишили телефон чи планшет у навчальному закладі, на роботі, в ресторані, – зв'яжіться з персоналом та заберіть свій пристрій якомога швидше. Подібний сценарій не створює значних ризиків.

Крок 2: Якщо Ви відслідковуєте Ваш пристрій у місцях, які Ви не відвідували або ж побачите його переміщення, негайно зверніться до поліції та передайте інформацію про місцезнаходження пристрою. Швидке реагування є надважливим, оскільки Ви зможете бачити місцезнаходження пристрою лише поки не розрядиться акумулятор, або поки пристрій не відключать від Інтернету.

Крок 3: Якщо Ви знаєте, що на пристрої знаходиться надзвичайно сенситивна інформація, і Ви з певних причин не виконали

вищезазначені рекомендації, ми радимо одразу ж дистанційно стерти дані з пристрою.

Крок 4: Негайно змініть паролі до всіх своїх акаунтів.

Правило №22: У випадку втрати чи крадіжки пристрою, завжди пам'ятайте, що краще втратити, наприклад, 14 днів виконаної роботи, ніж поставити під загрозу безпеку всіх збережених на пристрої даних. Більше того, ігноруючи цей факт, Ви можете поставити під загрозу і дані, що розташовані на хмарних сервісах роботодавця. Якщо Ви не можете постійно мати телефон при собі (наприклад, якщо його необхідно залишити у камері схову), використовуйте одноразові захисні мішечки, аби переконатись, що з телефоном не проводили ніяких маніпуляцій без Вашого відома. Мішечки також мають назву захисних конвертів і їх можна придбати, наприклад, на EuroSeal.cz.

Безпека у соціальних мережах

Правило №23: Будьте пильними, встановлюючи налаштування приватності на Facebook – переконайтесь, що Ваші дописи можуть бачити тільки друзі. З часом, Ви можете створити окремі групи серед своїх друзів для спеціального контенту. Переконайтесь, що Вас не можуть відмітити у постах без Вашого дозволу. Нижче Ви можете знайти детальну інструкцію. Якщо ж Ви свідомо ведете профіль як публічний, дотримуватися цих правил немає необхідності.



About Facebook Apps

Do not login to or link third-party sites (e.g. Twitter, Bing, LinkedIn) using your Facebook account. "Facebook Connect" shares your information, and your friends' information, with third party sites that may aggregate and misuse personal information.

Also, use as few apps as possible. Apps such as Farmville access and share your personal data.

Edit your profile by changing all the options to Only Me (most secure) or Friends Only.

Editing Your Privacy Settings

1) Control Your Default Privacy – Change to Friends Only

2) How You Connect

- Who can look up using your e-mail or phone number? - **Friends**
- Who can look you up using the email address or phone number you provided? - **Friends**
- Who can send you friend requests? - **Friends of Friends**
- Who can send you Facebook messages? - **Friends**

3) Timeline and Tagging

- Who can post on your Timeline? - **Friends**

- Who can see what others post on your timeline? - **Friends**

- Review posts friends tag you in before they appear on your timeline - **On**

- Who can see posts you've been tagged in on your timeline? - **Friends**

- Review tags friends add to your own posts on Facebook - **On**

- Who sees tag suggestions when photos that look like you are uploaded? - **Friends**

4) Ads, Apps and Websites

- Apps you use – **Limit use of Apps**
- How people bring your info to apps they use – **Uncheck all boxes**
- Instant personalization – **Disable Personalization**
- Public Search – **Disable Public Search**
- Ads > subpages > Ads shown by third parties – **No one**
- Ads > subpages > Ads and friends – **No one**

5) Limit the Audience for Past Posts – **Limit the Old Posts to Friends Only**

6) Blocked People and Apps – Here you can block certain people, events and game invites.

ОПЕРАЦІЙНА БЕЗПЕКА ТА ОСОБИСТА СТІЙКІСТЬ: ОГЛЯД СИТУАЦІЇ У КРАЇНАХ СХІДНОГО ПАРТНЕРСТВА

General

Security and login

Privacy

Timeline and Tagging

Blocking

Language

Notifications

Mobile

Public Posts

Apps

Adverts

Payments

Support Inbox

Videos

Timeline and Tagging Settings

Who can add things to my Timeline?	Who can post on your Timeline?	Only me	Edit
	Review posts that friends tag you in before they appear on your Timeline?	On	Edit
Who can see things on my Timeline?	Review what other people see on your Timeline		View As
	Who can see posts you've been tagged in on your Timeline?	Only me	Edit
	Who can see what others post on your Timeline?	Only me	Edit
How can I manage tags people add and tagging suggestions?	Review tags people add to your own posts before the tags appear on Facebook?	On	Edit
	When you're tagged in a post, who do you want to add to the audience if they aren't already in it?	Only me	Edit
	Who sees tag suggestions when photos that look like you are uploaded? (this is not yet available to you)	Unavailable	

Public Post Filters and Tools

Who Can Follow Me

Followers see your posts in News Feed. Friends follow your posts by default, but you can also allow people who are not your friends to follow your public posts. Use this setting to choose who can follow you.

Each time you post, you choose which audience you want to share with.

[Learn more.](#)

Friends

Public Post Comments	Who can comment on your public posts? Friends	Edit
Public Post Notifications	Get notifications from Nobody	Edit
Public Profile Info	Who can like or comment on your public profile pictures and other profile info? Friends	Edit
Comment Ranking	Comment ranking is Off	Edit
Username	You have not set a username.	Edit
Twitter	Connect a Twitter account	Edit

ОПЕРАЦІЙНА БЕЗПЕКА ТА ОСОБИСТА СТІЙКІСТЬ: ОГЛЯД СИТУАЦІЇ У КРАЇНАХ СХІДНОГО ПАРТНЕРСТВА

Правило №24: Було б розважливо приховати свою домашню адресу, номер телефону, електронну адресу та інші дані (або з самого початку не вказувати їх – Facebook нерідко продає такі дані третім сторонам). Перейдіть до вкладки «Про себе» на Facebook, видаліть свою адресу і встановіть налаштування «Лише я» для електронної адреси та номера телефону, щоб їх не міг побачити ніхто інший. Оцініть, як Ваш профіль виглядає очима друзів або незнайомців, скориставшись функцією «Переглянути як». Задля впевненості, пошукайте у Google свою електронну адресу, домашню адресу та номер телефону, аби побачити, де є доступ до цієї інформації та звідки її можна видалити. Цю процедуру варто здійснити також щодо членів Вашої родини.

Правило №25: Обмежте доступ до перегляду свого профілю тільки друзями. Кожного місяця стирайте усі свої переписки на Facebook. Якщо хтось отримає доступ до Вашого профілю, їм не вдасться отримати сенситивні дані з Вашого особистого спілкування.

The screenshot shows the LinkedIn 'Settings' page. On the left, a sidebar lists 'Profile privacy', 'Blocking and hiding', 'Job seeking' (highlighted), 'Data privacy and advertising', and 'Security'. The main content area is divided into three sections:

- Job seeking**: Includes 'Sharing your profile when you click apply' (set to 'No'), 'Let recruiters know you're open to opportunities' (with a 'Close' button), and a toggle for 'Update career interests' (set to 'No').
- Data privacy and advertising**: Includes 'Manage who can discover your profile from your email address' (set to 'Nobody'), 'Manage who can discover your profile from your phone number' (set to 'Nobody'), 'Representing your organization' (set to 'No'), 'Profile visibility off LinkedIn' (set to 'No'), and 'Advertising preferences' (set to 'No').
- Security**: Includes 'Two-step verification' (set to 'On').

The screenshot shows the LinkedIn 'Profile privacy' settings page. It includes the following sections:

- Edit your public profile**: A 'Change' button.
- Manage active status**: A 'Close' button.
- Display your active status**: A toggle for 'Show my connections when I'm active on LinkedIn or available on mobile' (set to 'No'). A note states: '*Changes may take up to 30 minutes'.
- Hide active status from select people**: A text input field for 'Type connection name'.
- Who can see your connections**: A 'Change' button, currently set to 'Only you'.
- Viewers of this profile also viewed**: A 'Change' button, currently set to 'No'.
- Sharing profile edits**: A 'Change' button, currently set to 'No'.
- Profile viewing options**: A 'Change' button, currently set to 'Private mode'.
- Notifying connections when you're in the news**: A 'Change' button, currently set to 'No'.
- Who can see your last name**: A 'Change' button, currently set to 'Abbreviated'.

Правило №26: Не давайте іншим сервісам доступ до свого профілю.

Правило №27: Відключіть персоналізовану рекламу.

Правило №28: Використовуючи Facebook на телефоні, обмежте або відключіть доступ додатка до своєї геолокації.

Правило №29: Фото, зроблені на смартфоні, містять багато сенситивної інформації про час і місце, в якому вони були зроблені. Якщо це можливо, не діліться ними безпосередньо у своїх соціальних мережах або відключіть геолокацію для фото. Окрім того, зменшуйте розмір фотографій та редагуйте їх (це пошкодить метадані фото). iVerify також може знищити ці метадані за Вас. В іншому випадку Ви ризикуєте розкрити інформацію про своє програмне забезпечення та операційну систему.

Правило №30: Не авторизуйтесь на Facebook через інші веб-сторінки – така авторизація завжди має результатом доступ до Ваших даних.

Правило №31: Не додавайте у друзі людей, яких Ви не знаєте. Якщо в минулому Ви не дотримувались цього правила, прогляньте свій список друзів та видаліть з нього тих, кого не знаєте особисто. Це правило не стосується тих, хто цілеспрямовано веде публічну сторінку.

Правило №32: LinkedIn часто використовують для збору персональних даних. Якщо Вам необхідно використовувати цю мережу, розміщуйте у ній тільки публічно відому інформацію. Перевірте, яку інформацію Ви вже розмістили на LinkedIn. Уважно прогляньте всі зв'язки, що можуть привести до Вас або Вашої родини чи близьких друзів (окрім відомих публічно), оскільки це створює ризик «наближення» (хто намагатиметься встановити з Вами контакт та у який спосіб ця особа намагатиметься завоювати Вашу довіру).

а. Безпека інформації про Вас та близьких до Вас людей

Правило №33: Оберіть, яку саме інформацію Ви хочете захистити. Базові критерії – Ваша домашня адреса, інформація про Ваших рідних та Ваші особисті стосунки, яка може бути використана супротивником проти Вас (наприклад, якщо Ви переживаєте кризу в особистих стосунках). Розподіліть всю інформацію на три групи:

- публічна (її можна віднайти онлайн та Ви постите її у соціальних мережах);
- приватна (наприклад, Ваша домашня адреса, особа Вашого партнера, яка відома тільки Вашим друзям);
- сенситивна (доступна тільки обмеженому колу людей, яким Ви повністю довіряєте).

Правило №34: Майте усвідомлення того, що все запощене Вами у соціальних мережах практично неможливо видалити і може бути використане супротивником через багато років після того, як Ви це запостили. Отож, не варто постити фотографії свого дому, своїх дітей та своїх близьких друзів чи рідних. Ми рекомендуємо пройтись по всіх своїх фотографіях на Facebook, Twitter чи Instagram і видалити ті з них, які розкривають дані про місця чи людей, які Ви прагнете тримати захищеними.

Правило №35: Приділіть декілька годин тому, щоб обрати, яку саме інформацію Ви вважаєте приватною чи сенситивною, та пошукати її в Google, щоб побачити, чи не з'являлась вона деінде. У такий спосіб Ви дізнаєтесь, яка інформація про Вас доступна у публічних джерелах. Прогляньте профілі своїх близьких друзів чи рідних та попросіть їх видалити всі Ваші фотографії та не постити їх у майбутньому. Якщо Ви прагнете захистити своїх рідних, не слід мати їх у списку друзів (однакове прізвище робить їх легкою знахідкою), що вимагає серії додаткових кроків з ретроспективного захисту Вашої особистості – автори цього посібника залюбки поділяться з Вами додатковими, більш сенситивними, заходами.

Правило №36: Ваша адреса реєстрації частково є публічною інформацією, доступною у державних базах даних чи в комерційних контрактах. Якщо Ви не хочете, щоб Ваше місце проживання було легко знайти, змініть адресу реєстрації на адресу своїх батьків чи інших рідних. Можливо також встановити адресу реєстрації через свою організацію.

Правило №37: Налаштуйте Google Alerts так, щоб Вам приходило сповіщення на електронну пошту, коли Ваше ім'я (або комбінація з Вашого імені, посади чи назви Вашого роботодавця) з'являється на будь-якому сайті. Спробуйте різні комбінації імені, посади та назви роботодавця. Результати не включатимуть соціальні мережі.

б. Анонімність в Інтернеті

Вся Ваша активність у мережі дає певний рівень інформації про Вашу особистість. Цю інформацію можливо проаналізувати, порівняти та використати для створення Вашого профілю, який може відкрити багато сенситивної інформації про Вас на основі Вашої поведінки онлайн. Хоча такої речі як повна Інтернет-анонімність не існує, ми рекомендуємо зменшити до мінімуму кількість інформації про себе, якою Ви ділитесь, особливо якщо це стосується сенситивної діяльності. Те, що зараз видається очевидним, через 5 чи 10 років може бути використано для психологічного аналізу Вашого профілю:

Правило №38: Користуйтеся DuckDuckGo (<http://duckduckgo.com>) в якості основної пошукової системи. Ця система використовує зашифроване з'єднання та не зберігає ні Вашу IP-адресу, ні історію пошуку. Вимкніть автоматичну авторизацію у всіх інших браузерах. Куки (cookies): у поширених браузерах (Chrome, Firefox, Internet Explorer, Safari) Вам стануть у нагоді приватні/анонімні вікна, які не зберігають куки. Однак Ваша IP-адреса все ще буде ідентифікуватись провайдером, який зможе відслідковувати Вашу онлайн-активність.

Правило №39: Хороший сервіс для того, аби анонімно та конфіденційно ділитись документами, - Crabgrass (<https://we.riseup.net/crabgrass>), де Ви можете зареєструватись анонімно та використовувати його для пересилки документів всередині своєї команди.

Правило №40: Аби приховати свою ідентичність онлайн, рекомендуємо використовувати платну версію VPN. Ми б радили VPNSecure.me, Proton VPN чи Avast, і не лише для ноутбука, але й для Вашого телефону або планшета. Якщо Ви підключитесь до незахищеного Wi-Fi, відслідковувати Ваші дії стане дуже легко. Ніколи не майте справу з сенситивними даними через незахищене з'єднання. Ніколи не оновлюйте своє програмне забезпечення через незахищений Wi-Fi. Змінійте свій домашній пароль на Wi-

Фі кожні три місяці. Ми рекомендуємо використовувати «рубильник» у VPN, що моментально відключає Вас від Інтернету у разі поганого з'єднання, гарантуючи, що Ви завжди будете захищені через VPN.

Правило №41: Існує тільки один спосіб досягти високого рівня анонімності в Інтернеті, і він полягає у використанні спеціального браузера Tor. Ми рекомендуємо його не для постійного застосування – окрім всього іншого, він досить повільний, - а для тієї онлайн-активності, відслідковування якої Ви хочете унеможливити (не йдеться про нелегальну діяльність; Ви можете прагнути захистити себе через політично чутливі заяви, комунікацію з людьми, зв'язок з якими Ви не хочете робити публічним тощо). Якщо Ви використовуєте Tor, не встановлюйте плагіни та не завантажуйте паралельно торенти. Ми також не рекомендуємо відкривати у Tor документи (навіть .doc та .pdf файли). Якщо Ви маєте попрацювати з документами, відключіться від Інтернету на цей час.

Безпека комунікацій

а. Шифрування комунікацій

Якщо Ви від руки записуєте сенситивну інформацію на папері, ми рекомендуємо знищувати ці записи щодня (порвіть їх на маленькі частини та змийте в унітаз). Це гарантує, що Ви не забудете записник із записами за довгий час, піддавши інформацію ризику.

Найменш безпечні засоби комунікації:

- Телефонні дзвінки, текстові повідомлення: провайдери зберігають записи телефонних дзвінків та повідомлень і нерідко можуть надавати їх третій стороні (за певних умов). Моніторити Ваші дзвінки та текстові повідомлення за допомогою наявних на ринку технологій не складно.
- Електронні повідомлення зберігаються на серверах Вашого провайдера, що робить їх доступними для будь-кого, кому відомий ваш пароль від електронної скриньки, та для провайдера. Те ж саме стосується Facebook та Twitter. Незашифроване електронне повідомлення схоже на відправлену поштою листівку – його може прочитати кожен, у кого виникне таке бажання.

Правило №41: Найбільш зашифрований з доступних цивільним особам додатків-месенджерів - Signal, через який Ви можете також робити дзвінки (але не групові). Якщо Ви використовуєте Signal, важливо, щоби всі налаштування приватності були увімкнені – включно зі встановленням кодової фрази та регулярного видалення повідомлень (ми рекомендуємо інтервал в один день). Ми не радимо користуватись WhatsApp чи Skype, маючи справу з сенситивною інформацією. Для інформації дуже чутливого характеру варто використовувати Wickr Me. Не користуйтеся Viber чи Telegram. Роблячи дзвінок через додаток з шифруванням, звертайте увагу на своє оточення. Ніколи не обговорюйте сенситивну інформацію у транспорті, в машині з незнайомцем чи у приміщенні з іншими особами. Найкраще – вийти назовні.

Правило №42: Найбільш безпечна програма для зашифрованих електронних листів – ProtonMail, якщо він використовується обома сторонами. ProtonMail доступний для iOS, Android та стаціонарних комп'ютерів. Рекомендується завантажити платну версію Proton Bridge, оскільки він дозволяє встановити ProtonMail у клієнт електронної пошти на Вашому комп'ютері. Не забувайте про двофакторну автентифікацію. Очищуйте ProtonMail кожні 3 місяці, стираючи всі отримані та відправлені повідомлення. Оскільки для ProtonMail необхідна резервна електронна пошта, рекомендуємо налаштувати другий (можна безкоштовний) акаунт на ProtonMail з надзвичайно потужним паролем (40 знаків), який можна використовувати як резервний для всіх своїх інших профілів - Facebook, Twitter, LinkedIn, Instagram, банківські акаунти.

Безпека даних

Кожна папка зі спільним доступом (наприклад, на Dropbox) безпечна настільки, наскільки убезпечений її найменш захищений користувач.

Рекомендовані налаштування iPhone:

- Параметри > Сповідання > пройдіться по всіх додатках і переконайтесь, що сповідання не відображаються, коли екран заблоковано
- Параметри > Приватність > Служби локації > вимкнено
 - Перевірте всі додатки та вирішіть, де встановити GPS «під час використання», а де «ніколи». Переконайтесь, що ніде не стоїть параметр «завжди».
 - Упевніться, що «ніколи» обрано для: камери (інакше всі Ваші фотографії міститимуть дані про те, де їх було зроблено) та всіх додатків соціальних мереж (наприклад Twitter, Facebook, Instagram).
 - Для системних служб: вимкнути всюди, окрім сигналу SOS та (за бажанням) «Знайти мій iPhone».
 - «Часті адреси» - очистити та вимкнути.
 - Вдосконалення продукту – вимкнути все
- Параметри > Приватність
 - Аналітика і вдосконалення – «не відправляти».
 - Реклама – «Скинути ідентифікатор» та «Обмежити моніторинг» ввімкнено

а. Шифрування диску

Правило №43: Зашифруйте свій диск:

- macOS: має програму для шифрування диску FileVault – після її запуску буде згенеровано ключ відновлення (який можна безпечно зберігати на серверах Apple) і повністю зашифровано диск. Подальша розшифровка – фоновий процес, непомітний для користувача, який не уповільнює роботу системи.

- Windows: шифрувальна функція BitLocker включена тільки у професійних версіях Windows. Додатки на кшталт VeraCrypt чи CipherShed – хороша альтернатива для власників Windows без BitLocker.
- Телефони та планшети з Android 5.0 та вище, як правило, підтримують шифрування, однак у багатьох випадках воно погіршує роботу пристрою і, у такий спосіб, знижує комфорт користувача. Відповідно, ми рекомендуємо вимикати шифрування в подібних випадках, якщо користувач буде дотримуватись нижченаведених порад.

б. Шифрування та безпечне видалення даних, збережених на змінних дисках

Правило №44: USB флеш-диски: на Mac достатньо натиснути правою кнопкою мишки на іконку диска та вибрати опцію «Шифрування». Якщо після цього Ви вставите диск в інший комп'ютер, достатньо просто ввести пароль. Якщо Ви маєте версію Windows з BitLocker, диски можна шифрувати або у секції BitLocker Панелі управління, або просто натиснувши правою кнопкою на іконку флеш-диска. Якщо Ваша версія Windows не включає BitLocker, Ви можете скористатись вищезгаданою програмою VeraCrypt, що має ту ж саму функцію. Ніколи не підключайте невідомий USB-диск до свого пристрою, навіть якщо Ви отримали його від друзів – Ви не знаєте, наскільки серйозно вони ставляться до безпеки диску. Встановіть програму Safeguard, що відкриває тільки перевірені флеш-диски. Для невідомих файлів використовуйте додаток Sandbox.

Правило №45: Просте видалення даних з Вашого диска не робить їх недоступними – отже, необхідно виконати безпечне видалення, що може зайняти більше часу, але після цього Ви зможете передати диск будь-кому:

- На MacOS: Ви можете скористатись програмою Дискова утиліта (секція «Очистити диск» має кнопку для безпечної очистки. Скористайтесь додатком Eraser.
- Windows: На даний момент Windows не підтримує безпечне видалення у базовій конфігурації. Однак навіть безкоштовна версія, наприклад, CCleaner може безпечно видаляти дані зі змінних дисків.

Особиста безпека

Правило №46: Вашого імені не повинно бути в списку мешканців на вході до будинку. Якщо ж Ви змушені його включити, приборіть його з дверей до Вашої квартири.

Правило №47: Якщо Ви маєте поїхати на тривалий час, не оголошуйте про це публічно і переконайтесь, що Ваше місцезнаходження не висвітлюється у постах в соціальних мережах. В якості альтернативи Ви можете постити фотографії вже після повернення додому. Якщо Ви замовляєте таксі або Uber, рекомендується робити це не безпосередньо біля місця проживання, а як мінімум за 50 метрів від нього – і так само залишати авто. Дані про місце знаходження зберігаються у Вашому профілі, і отримати їх доволі легко.

Правило №48: Домовтесь про пароль з близькими до себе людьми, щоб вони могли подзвонити або написати Вам, якщо почуваються в небезпеці, і Ви могли одразу звернутись до поліції та почати шукати їх – переконайтесь, що вони також повідомили

Вам своє місце знаходження. Зробіть те саме для своєї родини. Якщо немає можливості подзвонити, можна відправити екстрений сигнал про допомогу.

Правило №49: Ніколи не заходьте у закриті приміщення з незнайомою людиною. Натомість уповільніть ходу, зробіть вигляд, що маєте телефонний дзвінок чи розверніться і підіть іншою дорогою. Якщо Ви відчуваєте себе некомфортно у будь-якому місці, негайно дістаньте телефон і зробіть вигляд, що телефонуєте близькій людині, голосно сказавши, де саме Ви знаходитесь і, наприклад, що поруч з Вами знаходиться підозріла особа, описавши її зовнішність. Це майже завжди спрацює як запобіжник. В якості альтернативи можете голосно закричати. «Учбова тривога» нічого Вам не коштуватиме, чого не можна сказати про її альтернативу.

Правило №50: Аби приблизно оцінити, наскільки серйозною є конкретна загроза, запам'ятайте нижченаведену схему. Базовий алгоритм дій у випадках фізичної небезпеки: бігти, ховатись, вступати у сутичку.

8. ОСНОВНІ ВИСНОВКИ

- Брак протоколів з кібербезпеки у НГО;
- Брак алгоритму дій для гарантування операційної безпеки/брак бажання йому слідувати;
- Брак відповідних людських ресурсів (спеціалістів) в НГО;
- Недостатньо серйозне ставлення до операційної безпеки;
- Основні помилки у сфері операційної безпеки, яких припускаються державні службовці, журналісти та НГО, що робить їх легкими мішенями:
 - «Я не настільки важливий»
 - «Я не роблю нічого незаконного»
 - «Ці дані не є засекреченими»
- Робота у сфері протидії російському та китайському впливу робить Вас мішенню
- Росія та Китай з легкістю отримують інформацію про тисячі осіб, що працюють у цій сфері.

9. КОРОТКИЙ ЗМІСТ

10 звичок стосовно безпеки, які варто розвинути усім

Правила, дотримуватись яких ми рекомендуємо, перераховані вище. Дуже часто це заходи, до яких необхідно вдатись лише один раз. Окрім цих базових змін у свій поведінці стосовно безпеки, ми також радимо розвинути такі щоденні звички та дотримуватися їх так само, як Ви регулярно чистите зуби та замикаєте двері:

Звичка №1: Для безпечного спілкування використовуйте тільки додаток Signal (як для переписки, так і для дзвінків) та ProtonMail для зашифрованих електронних листів. Не довіряйте таким додаткам як WhatsApp, Facebook Messenger чи Telegram для розмов на більш чутливі теми (правила №41-42).

Звичка №2: Регулярно видаляйте дані зі свого комп'ютера, використовуючи програми Permanent Eraser чи Cleaner (правило №45).

Звичка №3: Більшість кібератак відбуваються через фішинг. Тому відкривайте всі вкладення через Sandbox, а всі посилання перевіряйте через virustotal.com (правило №10).

Звичка №4: Не довіряйте змінним дискам, якщо немає можливості перевірити їхню безпечність. Якщо можливо, дані краще пересилати на ProtonMail. Як альтернативний варіант, можна тримати окремий комп'ютер без підключення до мережі, на якому Ви зможете відкрити USB- диск (правило №44).

Звичка №5: Зберігайте мобільні телефони у безпеці під час сенситивних зустрічей. В ідеалі, електронні прилади краще помістити у сумку на відстані 7-10 метрів від Вас, так щоб вона перебувала у полі зору, але прилади не могли «почути» Вашу розмову (правило №17).

Звичка №6: Рекомендується не використовувати прилади з бездротовим підключенням (навушники, принтери). Придбайте «USB-запобіжник» на свої зарядні пристрої для телефону та комп'ютера (правило №16).

Звичка №7: Додаючи інформацію та фотографії до своїх акаунтів у соціальних мережах, виставляйте тільки те, що можете дозволити побачити супротивникам. Якщо Ви постите будь-яку інформацію про свою родину та рідних чи своє особисте життя, опоненти зможуть створити Ваш психологічний профіль та соціальну карту і використати ці дані (правило №33).

Звичка №8: Завжди використовуйте VPN: VPN Secure Me, Proton VPN чи Avast. Користуйтеся «правилом рубильника» (правило №40).

Звичка №9: Якщо Ви записуєте сенситивну інформацію від руки, її варто розбирати кожен день і пропускати через шредер (або рвати на дрібні частини та позбавлятися їх поза межами Вашого дому чи офісу).

Звичка №10: ВСТАНОВІТЬ НАГАДУВАННЯ У КАЛЕНДАРІ: змінювати паролі кожні три місяці (правила №1-4). Ми радимо щомісяця робити резервні копії особистих документів, змісту електронного календаря та власних робочих файлів на зашифрованому зовнішньому диску (правило №19).



Незашифрований електронний лист – еквівалент публічного постигну своїх повідомлень в режимі реального часу

Ускладніть життя Вашим супротивникам:

1. Використовуйте хороший VPN (Avast Secureline, ProtonVPN, NordVPN,...);
2. Послугуйтеся хорошим антивірусним забезпеченням (Avast, Eset, McAfee,...);
3. Зашифруйте свої дані (VeraCrypt).

Не ставте все на одну карту:

1. Захистіть всі свої акаунти і профілі через двофакторну автентифікацію;
2. Майте декілька добре захищених електронних скриньок для своїх акаунтів; у випадку, якщо одна з них буде зламана, Ви не втратите всі дані;
3. Використовуйте складні паролі, не послугуйтеся одним паролем для всіх акаунтів.

Завжди перевіряйте нових людей, з якими зустрічаєтесь:

1. Завжди проглядайте (через Google) їхню біографію та попросіть людей, котрі їх знають, про коротку характеристику;
2. Не пускайте незнайомих осіб у свій офіс.

Знайте, яку інформацію про свою особу Ви захищаєте:

1. Чи багато на Вашому Facebook інформації про Вашого партнера та дітей?
2. Усвідомлюйте, що публічна інформація є легкодоступною і може бути використана супротивниками проти Вас.