У ЗМІ розповіли про інформаційну безпеку для кожного: "цифровий слід" та особиста інформація

Читать на русском

У ЗМІ розповіли про інформаційну безпеку для кожного: "цифровий слід" та особиста інформація

Чи чули ви про таке поняття як "цифрова ідентичність"? Це вся інформація про людину, що існує в інформаційному просторі. Причому йдеться не лише про ті дані, які людина особисто публікує про себе в інтернеті, а й ті, які збирають про неї сайти та програми, а також дані, яких ніхто не збирає, але які існують у мережі, передає Українське Радіо.

"Цифровий слід" — ще одне поняття, яке стосується всього, що ми залишаємо в мережі, користуючись інтернетом: геомітки, фото, відео, повідомлення, пошукові запити, паролі, номери карток, пости у соціальних мережах тощо.

Цифрова ідентичність — поняття дуже широке, воно охоплює конфіденційну та особисту інформацію, персональні дані, а також дані про нашу взаємодію з онлайн-середовищем.

Захист персональних даних — справа серйозна і важлива. Цьому аспекту безпеки велику увагу приділяють у Євросоюзі, де вже давно запроваджений GDPR — загальний регламент про захист персональних даних. Він встановлює правила задля безпеки та конфіденційності персональних даних громадян ЄС, надаючи їм контроль над їхньою особистою інформацією та зміцнюючи їхні права у цифровому просторі. Продовжує викладач факультету інформатики Національного університету "Києво-Могилянська академія" Трохим Бабич:

"Тут дуже цікаво дивитись на цей самий страшний GDPR європейський. Я вже чув, що ЕНІССА, це регулюючий орган Євросоюзу, з нашим НКЦК — Національний координаційний центр кібербезпеки — об'єднують зусилля. І, цебто, з нашою інтеграцією в Євросоюз я сподіваюсь на покращення, хоча серед експертів не всі одностайно вважають еталонними політики Євросоюзу, але це краще, чим їх відсутність. І, відповідно, той же GDPR, наприклад, дуже жорстко зобов'язує людей контролювати які ти дані береш у користувача, дуже явно їх показувати.

Це дуже смішно. Візьміть google зі свого телефону мобільного, і вдягніть VPN там будь-якої європейської країни. Ви пройдете 9 кіл пекла узгоджень із гуглом, доводячи, що ви точно дуже хочете сказати просто як вас звати. Персональна ж інформація, це ж те, що можна достеменно ідентифікувати. Ну, в плані, що це не просто Трохим Бабич, а *Трохим Бабич*. А ще він отакого року народження, і от коли це все зводиться до однієї персони.

Право на захист персональних даних і конфіденційність є фундаментальним правом людини, яке набуло ще більшої актуальності зі стрімким розвитком інформаційних технологій. У Європейському Союзі приділяють справді колосальну увагу захисту персональних даних. А як щодо України? Говорить начальник управління департаменту Кіберполіції Євгеній Панченко:

Ми рухаємося ще до Європи. Тому, звичайно, стандарти захисту інформації , якщо ми говоримо про приватний сектор, про державний сектор, то вони доволі чіткі і суворі. Кожен розуміє і має доступ до тієї інформації, яка передбачена безпосередньо їхніми функцій ними обов'язками, або у рамках розгляду певної справи. В той же час людям потрібно оволодіти базовими такими навичками розмежовувати службову, або приватну інформацію, і власну, яку ви використовуєте, наприклад, з родичами, чи з близькими, з друзями.

Тобто, не змішувати ці канали комунікації — тобто дві різні пошти, два різних фінансових телефони і так далі. Крім цього, вам потрібно розуміти, що будь-яку інформацію, яку ви не хочете щоб потрапила в публічний простір, вам варто тримати при собі. І не сподіватись на те, що там певний месенджер, або певний сайт є більш безпечним, тому йому можна надати всі дані. Зокрема, якщо ми говоримо про російські додатки, або сайти, то, звичайно, будьте певні, що туди не потрібно передавати ті відомості, які ви не бажаєте, щоб отримав ворог, або стали публічними.

Чи може вважатися лише ім'я людини персональними даними? Виявляється, не завжди. Особливо якщо йдеться про дуже поширені імена. Та коли ім'я поєднується з іншою інформацією, наприклад, домашньою або робочою адресою, номером телефону — цього, зазвичай, уже достатньо, щоб чітко ідентифікувати особу. За певних обставин колір волосся, місце роботи чи політичні погляди особи теж можна розглядати як персональні дані. Інформація, яка вважається такою, часто зводиться до контексту, в якому збираються дані".

Яку інформацію та як саме можуть використати кіберзловмисники, використовуючи нашу присутність в інтернеті? Пояснює Анастасія Кондрико, директорка Центру медіааналітики "Cyber Media Track":

"Доволі часто люди для своїх паролів використовують свої прізвища, певні дати, дні народження, дні народження своїх дітей, клички своїх улюблених тварин, дівоче прізвище, скажімо так, своєї дружини, або інших родичів і так далі. Зрештою, для того щоб дібрати пароль часто якраз аналіз починається із соціального акаунта. І, зрештою, від того, наскільки людина є активною там, можна пробувати потім активно шукати доступ до інших облікових записів. Те саме стосується і активного використання єдиного номера телефону, або єдиної електронної пошти. Зрештою, якщо це загальновідома інформація, спроба може відбутися. І тут все буде залежати від того, наскільки ми коректно захистили свої гаджети, захистили свою інформацію, ну, і звичайно, свої облікові записи".

Ми легко ділимося приватною інформацією у соціальних мережах, месенджерах, у спілкуванні та листуванні, у десятках різних застосунків (не завжди перевіряючи їхнє походження). Нам здається, що розмови про заплановану поїздку чи покупку не настільки критичні і що ми навряд чи цікаві кіберзловмисникам. Ми ж не публічні особи, ми ж не маємо якихось захмарних рахунків чи активів. Звісно ж, це не так. Продовжує начальник управління департаменту Кіберполіції Євгеній Панченко:

"Зазвичай, це така багатовекторна атака. І таким чином зловмисники формують певний портрет про особу. А, коли вони мають портрет особи, тобто чим ви займаєтесь, чим ви цікавитесь, легше увійти в довіру до вас і отримати додаткові доступи, які, знову ж таки, відкриють їм вікно в ваш банківський додаток. І останній приклад, який був вже опублікований в Інтернеті, це повідомлення нібито від ДСНС про загрозу вибуху на атомній електростанції.
Типовий файл збору інформації з різних невеликих джерел, які могли стати джерелом цієї інформації (маю на увазі інформацію про поштові скриньки) які отримали ці повідомлення. Десь реєструючись на якомусь невідомому сайті, десь залишаючи свої дані для певної знижки, яку ви можете отримати, можливо потенційно в майбутньому, потім такі дані, на жаль, потрапляють в Інтернет і вже шахраї, або зловмисники знають, що ця скринька дійсно валідна.

Тому на неї можна надіслати ось такий фітинговий лист з попередженням про загрозу вибуху, а ви, користуючись тим, що це ніби це загроза життю, перейдете на цей лист, прочитаєте, а, можливо, навіть виконаєте ту інструкції, які там зазначені. Наприклад, в цьому випадку було зазначено, що щоб отримувати найшвидше оповіщення про загрози, перейдіть сюди та залиште свій номер. Таким чином, знову ж таки, валідують, що цей номер для вас актуальний, а він, отже, може використовуватися і в банкінгу".

Отже, від зловмисних дій у цифровому просторі ніхто не убезпечений. Інше питання — що ви зробили для того, аби захистити свою персональну інформацію. Користувачі часто недооцінюють ризики, вважаючи себе не цікавими для зловмисників, а свою особисту інформацію некритичною і неважливою. До речі, а навіщо така інформація зловмисникам? Що вони можуть з нею зробити? Говорить заступник директорки Центру демократії та верховенства права Ігор Розкладай:

"Перш за все, треба розуміти, що ви живете в соціумі. Тобто ви, як людина, можете дійсно бути абсолютно не цікаві зловмисникам. Але ваші контакти можуть. Тобто, ви можете стати ключем для того щоб атакувати іншу людину, яку ви знаєте. Тобто через вас. Так само, як ця система — дуже часто систему зламують не кіберзасобами, а шукають людину, яка має пароль 123… через неї ламають. Атакою є не сама людина, а система. А людина просто є ключиком. Так само і тут.

Тобто, коли ви взаємодієте з іншими людьми, ви можете не бути напряму власне об'єктом атаки. Але ви можете бути опосередкованим способом, як можна атакувати когось більш значимого. Особливо, якщо це, наприклад, родинні зв'язки. Чи робочі зв'язки. Це перша історія, яка може бути. Друга історія, це, звісно, найзнаменитіша — це Кембрідж-аналітика. Коли, аналізуючи аудиторію, аналізуючи її повадки, звички, погляди, можна таргетувати ту ж політичну рекламу і, власне, вже впливати на вибори.

Але це вже про демократію, про збереженість, в принципі, країни. Те, що ті ж росіяни досить активно зараз Україну атакують не лише на фронті. Маючи власне не дуже великі успіхи на фронті, вони почали дуже сильно вкладатися саме в емоційну обробку населення, підживлення конфліктів, внесення якихось роздраїв. Дуже часто вони використовують правдиві ролики, до речі. І це теж дуже небезпечно.

Але що вони роблять, вони намагаються посилити, екстраполювати на всю країну, то одне якесь порушення подається як системна проблема всієї країни. І це найбільш небезпечно. Знову ж таки, має бути розуміння того, що ви можете бути об'єктом в межах певної групи. І ваші звички, поведінки, якщо вони вивчаються, потім стануть проти вас і ви постраждаєте. Тому що ви обираєте когось не того. І потім почнуться історії, коли врешті-решт доведеться виходити знову на Майдан".

Ілюстративне зображення із сайту Pixabay

Одним із місць, де зберігається багато нашої особистої інформації, є електронна скринька. І хоча періодично можна почути, що електронна пошта "померла", мовляв, ніхто нею особливо не користується, насправді ситуація протилежна — кількість користувачів електронної пошти щороку зростає.

Якщо у 2020 році в інтернеті було майже 4 млрд користувачів електронної пошти, то вже цього року їхню кількість прогнозують на рівні майже 4,5 млрд. Таким чином, електронна поштова скринька стає ще одним об'єктом, якому варто приділяти увагу з точки зору безпеки. Більше – директорка Центру медіааналітики "Cyber Media Track" Анастасія Кондрико:

"Звичайно, що в кожної людини, яка сьогодні використовує Інтернет, має бути декілька електронних скриньок. Кожна з яких має реалізовувати свою потребу. Це, в першу чергу, побутовий рівень. Друга історія — це професійні обов'язки. І третя історія — це онлайн-шопінг. Відповідно, якщо ми використовуємо лише одну електронну пошту, вся інформація швидко стає відомою в загальному доступі. І вся інформація, яка нам може надходити від онлайн платформ, від шахраїв, від третіх осіб, буде потрапляти на цю єдину електронну пошту. І наслідки можуть бути різними. Якщо ми не фільтруємо інформації, і не маємо таких основ кібергігієни. Електронна пошта, так само, як і інші наші електронні записи, обов'язково повинна мати унікальний якісний пароль, і двох факторну аудентифікацію.

Це основна умова для того щоб ви не почували себе в небезпеці, використовуючи електронну пошту. Ну, і, знову ж таки, особливо зважати на посилання. Є такий хороший ресурс, називається *https://urlscan.io/*. На цьому ресурсі можна спочатку перевірити посилання, що там є і наскільки воно є безпечним, а вже потім ухвалювати рішення, чи треба нам сюди переходити. Ну, і звичайно, що коли ми вставляємо це посилання в рядок пошуку, звертайте, будь ласка, увагу на початок назви сайту, куди ви плануєте перейти. Має бути *http**s***. Наприкінці **s** означає *sequryty*. Це означає, що браузер бере на себе відповідальність і перевірив протокол захищеності цього ресурсу. І, звичайно, що поруч має бути закритий зелений замочок. Якщо ваш браузер попереджає вас, що тут є небезпека — відкритий замочок червоного кольору і цієї s немає, краще утримати себе від переходу на такий ресурс.

Перебуваючи в інтернеті, ми залишаємо "цифровий слід". Причому він стосується не тільки того, що ми самі викладаємо, а й тієї інформації, яку про нас (відкрито чи приховано) збирають різні сайти або застосунки.

Так, уся інформація, яку браузер отримує від користувача, збирається за допомогою так званих cookies. Це аж ніяк не новітня технологія — уперше про неї заговорили ще в 1990-х роках. Нині ж cookies використовують усі сайти. Cookies збирають інформацію про наші поведінкові патерни: лайки, IP-адреси, місце перебування, кліки і зосередженість на тому чи іншому елементі сайтів та соціальні перетини. Зазвичай ми даємо згоду на використання cookies одразу ж, як переходимо на сторінку сайту, рідше — читаємо політику використання, в якій можна простежити, для чого саме компанія збирає інформацію про користувача.

Також багато хто, напевне, стикався із таргетованою рекламою продуктів, яких ви точно ще не шукали, а лише обговорювали чи тільки думали про них. Рекламні оголошення, які ідеально влучають у сферу ваших інтересів, можливі завдяки тому, що брокери даних переглянули та відсіяли величезний обсяг інформації про вас і продали ці дані компаніям. Хоча рекламні компанії більше цікавляться даними про ваш вік, стать і чистий дохід, аніж відомостями про вашу адресу чи номер телефону, вони все ж використовують цю інформацію для націлювання на конкретні профілі клієнтів".

А тепер повернімося до того, що викладаємо ми самі. І тут варто згадати такий момент, як пересилання особистих документів, фото, скріншотів із важливою інформацією через месенджери. Наприклад, юристові, лікареві або продавцеві. Наскільки це небезпечно? Пояснює інженер із кібербезпеки компанії OptiData Владислав Радецький:

"Час від часу нашим співгромадянам потрібно передавати документи, які містять або інформацію про здоров'я когось із близьких, або якісь фінансові дані, ще якийсь доволі чутливий документ. У цьому випадку я б закликав слухачів за можливістю не передавати файли — на сленгу це називається плейтекстів — не передавати просто так, як вони є без додаткового захисту, без додаткових маніпуляцій через такі дуже популярні месенджери як Вайбер і Телеграм.

З тієї причини, що коли ви користуєтесь чимось безкоштовно, коли ви не маєте доступу до сервинних цих площадок, технічно у вас немає можливості пересвідчитись що файли були дійсно видалені. Коли ви натискуєте кнопку видалити, цей файл пропадає зі списку на вашому пристрої. Але в хмарі його копія може ще деякий час зберігатися. Є багато різних розумних корпоративних засобів по захисту документів. Це називається шифрування, це криптографічний захист документів. Але у більшості випадків то є платним. І потрібна окрема людина яка все це налаштовує і супроводжує.

Тому для більшості людей елементарною пересторогою для захисту під час передачі документів буде те, якщо людина перед відправленням просто помістить документи в архів. І цей архів закриє паролем. Важливо, щоб пароль був не чотири одинички, або там непослідовність від одного до шести. Щоб це було там хоча б 10-12 символів, можливо, не такий складний, але це не має бути проста послідовність. Важливо пам'ятати, якщо ви комусь чи лікарю, чи адвокату, передаєте важливий документ, і ви дотрималися моєї поради, цей документ захистили архівом з паролем, в жодному разі не треба пароль від цього архіву передавати через той самий месенджер, через який ви пересилаєте, або через ту саму електронну пошту.

Просте правило: документ в архіві з паролем іде по одному каналу, пароль іде по іншому. Допустимі варіанти — документ відправляється електронною поштою, пароль передається адресату через месенджер, може бути Сігнал, може бути Тріма, в крайньому випадку це може бути той же Телеграм і Вайбер. Але, головне, щоб сам файл і пароль від нього не йшов одним реченням, одним повідомленням. Тому що будь-хто, хто це може перехопити на стороні отримувача, він одразу отримує доступ до інформації.

Щоб максимально захистити свою особисту інформацію в інтернеті, передусім треба бути уважними до того, що ви оприлюднюєте у соціальних мережах або інших загальнодоступних ресурсах. Навіть видаливши їх, ви не можете гарантувати, що ці дані не були збережені іншими особами або ресурсами. Важливо ознайомлюватися з угодами користувача або політиками конфіденційності сайтів чи застосунків. Принаймні спробуйте визначити, які саме дані запитує сайт або застосунок. Чи влаштовує вас надання такої інформації? Чи потрібна така інформація для мети, з якою ви користуєтеся сайтом або застосунком?

Не забувайте, що ваш комп'ютер або смартфон, облікові записи та застосунки мають налаштування конфіденційності. Ви можете обмежити категорії та обсяг даних, які дозволено їм збирати. Особливо звертайте увагу на налаштування щодо засобів оплати онлайн, геолокації, зображень, номера телефону.

Видалення застосунку зі смартфона чи комп'ютера не означає видалення ваших персональних даних. Якщо ви бажаєте припинити їхню обробку, переконайтеся, що діяли згідно з правилами власника сайту або застосунку щодо повного видалення вашого облікового запису.

Перед тим, як утилізувати чи продати свій комп'ютер або смартфон, переконайтеся, що всі персональні дані на ньому надійно знищені. Робіть це згідно з рекомендаціями виробника або використовуйте відповідні програми".

Ще кілька практичних порад — від директорки Центру медіааналітики "Cyber Media Track" Анастасії Кондрико:

"Сьогодні ми повинні привчити себе до того, що кожна людина повинна мати як мінімум два номери телефону. Один з них використовувати для доступу до фінансової інформації, зокрема, до онлайн банкінгу, до налаштувань, які пов'язані з фінансами, а інший, звичайно, має бути загальновідомий, який ми використовуємо в звичайному житті. Стосовно електронної пошти так само. Має бути пошта для побутового рівня, для виконання професійних обов'язків, і, звичайно, окрема для реєстрації на різних онлайн платформах. Зокрема, коли ми наповнюємо і створюємо свою сторінку у соціальних мережах, треба, перш за все, почитати політику конфіденційності. На жаль, ми цього часто не робимо через те, що там забагато символів, забагато знаків, і нам здається, що якщо щось трапиться, то точно не з нами.

Зрештою, звичайно, звертати увагу на тих, кого ми додаємо до своїх друзів через соціальні мережі. Відповідно аналізувати сторінки і звертати увагу на їхні наповнення. Тому що сьогодні вкрай активними є боти і ботоферми. До речі, рекомендую подивитися фільм, який зняли журналісти розслідувачі, який називається "Я — бот". Там досить цікаво розповідається про те, як працює ботоферма, з якою метою вони можуть реалізовувати завдання власників, або адміністраторів ботоферм. Звичайно, що треба з обережністю ставитися до всіх репостів, коментарів, до оприлюднення особистої інформації, фотографії, на яких зображені ви поруч з вашими родичами, колегами, друзями і так далі.

Ну, і, звичайно, що пам'ятати, що сьогодні існує ціла низка інструментів, які дозволяють з'ясувати де саме була створена фотографія, чи отримала вона певне редагування, маю на увазі використання фото шопу та інших графічних редакторів растової графіки. Тому, перш ніж щось оприлюднювати, звичайно, слід пам'ятати про наслідки такого оприлюднення. І, звичайно, паролі і двох факторна аудентифікація. Ви повинні пам'ятати, що кожен обліковий запис наш повинен містити не лише якісний та унікальний пароль, але і звичайно, двох факторна аудентифікація, коли ми через інший пристрій, або інший акаунт можемо дозволити доступ до цієї сторінки".

Інтернет знає про нас більше, ніж ми думаємо. Усе, що ми робимо в мережі, не зникає безслідно. Крім того, не забуваймо про зловмисників, які "полюють" не лише на дані багатих і знаменитих. Будь-яка особиста інформація, будь-які персональні дані можуть стати об'єктом їхньої уваги. Тож будьте пильними і відповідальними, ставтеся розумно до поширюваної інформації. А також зберігайте анонімність і конфіденційність там, де це можливо й раціонально.

Теги: кіберполіція | Киберполиция | Персональные данные | Персональні дані | соцмережі | Соцсети | інтернет | Интернет

Олексій Дем'яненко
РЕДАКТОР СТРІЧКИ НОВИН

20 березня 2024 г., 16:04 | Переглядів: 2464 | Коментарі: 0

Роздрукувати | Надіслати товаришу

Коментарі: