Дайджест

Лукаш Круль (Lukasz Krol)

координатор програм розвитку в Коледжі Європи у Натоліні (Варшава, Польща). Отримав ступінь магістра з політології та міжнародних відносинув Кембриджському університеті. З досвідом у сфері технологій та полотології Лукаш досліджує способи, яким чином об'єднати технологічні та соціальні реалії. Він є дослідником, викладачем і фасилітатором. Лукаш зосереджується на тому, яким чином люди сприймають штучний інтелект, а також на питаннях, пов'язаних з нерівністю та дискримінацією у алгоритмах та технологіях загалом.

Цифрова безпека

Що таке цифрова безпека і для чого вона нам?

Існує багато визначень цифрової безпеки. Та загалом, це захист вашої цифрової особистості, оскільки вона відображає фізичну ідентичність у мережі Інтернет. Цифрова безпека включає інструменти, які використовуються для захисту своєї ідентичності, активів та технологій в цифровому світі.

Одні люди переживають через приватність своїх даних, інші вважають, що «їм нема чого приховувати». Де ж ця межа?

Про це читайте детальніше в інформації від польських експертів Лукаша Круля та Міхала Чижевського.

Ви все ще впевнені, що ваші дані нікому не потрібні?

Нещодавно в мережі можна було побачити багато фото зістарених облич через додаток FaceApp, який є продуктом російської компанії. За допомогою цього додатка, можна збирати величезну кількість даних, як-от фотографії, IP-адреси, конкретні дані з вашого смартфона.

У 2018 році стався скандал стосовно компанії Cambridge Analytica, яка отримала доступ до особистих даних 87 мільйонів користувачів соцмережі Facebook без їхнього відома. Cambridge Analytica - це агентство, яке використовувало персональні дані людей, щоб впливати на виборців під час президентських виборів у США 2016 року.

24 липня 2019 року Федеральна торгова комісія Сполучених Штатів (FTC) оштрафувала компанію Facebook на 5 млрд доларів за порушення конфіденційності.

Ви все ще впевнені, що ваші дані нікому не потрібні?

Читайте про це думки експертів Лукаша Круля та Міхала Чижевського.

Лукаш Круль: Я вважаю, що найбільший ризик, який зараз існує, полягає в тому, що якщо ви розповідаєте людям про такі речі, як Cambridge Analytica, більшість людей не вірять, що ними можна маніпулювати. Чи не так? Більшість людей вважають, що вони раціональні, вони не піддаються політичній рекламі, яка впливає на виборчі кампанії і т. ін. Більшість людей насправді скептично ставиться до того, що ними можна маніпулювати, або що їхню думку можна змінити.

Міхал Чижевський: Приватність (конфіденційність) – це не просто момент у часі, це процес. Ми вже зараз повинні замислюватись, хто і як потенційно може використати опубліковані нами дані через 5 чи 10 років.

CHARLES STEWART MOTT FOUNDATION
Лабораторія Електронної Демократії
Подільська Агенція Регіонального Розвитку

Лукаш Круль: Я думаю, що приватність даних існує на декількох рівнях. І ви не знаєте, яким чином ваші дані можуть бути використані проти вас у майбутньому. Я думаю, що якщо ви перебуваєте в зоні військового конфлікту, то ви не можете передбачити, яка геополітична ситуація буде найближчим часом, ви повинні. дуже перейматись тим, як ваші дані будуть використані для таргетування та профілювання. По-друге, приватність – це інтуїтивна річ. Іноді легше її описати за допомогою емоцій, а не раціонально. Більшість людей звісно ж не хотіла б, щоб трапилась ситуація з Cambridge Analytica. Більшість людей, звісно, не дуже комфортно себе почувають, коли дізнаються яку кількість даних про них збирає Facebook. І я думаю, що одним з найкращих способів переконати людей у важливості питання безпеки даних – є продемонструвати їм, що це не просто про машини, а у Facebook та Google працюють люди.

До прикладу, якщо ви знаходитесь в зоні конфлікту і використовуєте програму для заміни облич, про яку ви нічого не знаєте. Мова не йде про те, що ці дані обробляються машинами. Мова про людей. За кожною машиною стоїть людина. Це незнайомі люди,

яким ви не довіряєте. Ви не знаєте, чому саме ці люди цим займаються. Але в той момент, коли створений алгоритм і дані обробляються технологічно, створюється відчуття абстрагування від людей. Проте за кожним раціональним алгоритмом стоїть людина. Людина, якій ми не можемо довіряти і яку ми не розуміємо.

Є ще одна важлива річ, на які варто наголосити. Йдеться не просто про нечітку інфраструктуру. За кожною маніпуляцією в Facebook стоять люди. Реальні люди, які зможуть вас зрозуміти і таргетувати інформацію. За кожним додатком для зістарення/зміни обличчя стоять люди.

Для більшості людей, дані яких обробляються алгоритмами чи таргетуються ними, алгоритми – це «Ну і що в цьому такого? Що в цьому такого, якщо камера з розпізнаванням обличчя побачить, як я ходжу по аеропорту?» Але це не просто камера, а людина, яка керує цією камерою. І коли йдеться про людину, то тоді ми починаємо ставитися серйозніше.

І було багато мемів стосовно кейсу Cambridge Analytica та зображення Марка Цукурберга. Те ж саме стосовно скандалу з АНБ та обличчям Обами. Варто проводити тренінги, під час яких давати інформацію та вчити людей дбати про цифрову безпеку.

Тому, дбайте про безпеку даних вже сьогодні!

Цифрова гігієна. Що це і для чого потрібна?

Перелік найбільш використовуваних паролів (легко зламати захист)

123456
123456789
qwerty
password
1111111
12345678
abc123
1234567
password1
12345
1234567890
123123
000000
Iloveyou
1234
1q2w3e4r5t

1. Перш за все – це складні паролі (комбінація великих і малих літер, цифр та розділових знаків)
2. Не використовуйте один і той самий пароль для різних акаунтів, навіть, якщо він достатньо безпечний і довгий.
3. Для безпеки входу в системи можна використовувати менеджери паролів (до прикладу KeePass - вільна програма для зберігання паролів, що розповсюджується по ліцензії GPL).
4. Використовуйте паролі для входу в систему ноутбука та телефона.
5. Оновлюйте програмне забезпечення на пристроях (як для комп'ютера, так і для телефону).
6. Перевіряйте походження інформації (у разі отримання підозрілого файлу чи листа, краще уточніть, чи лист був відправлений від тієї особи).
7. Робіть резервне копіювання даних.
8. Використовуючи публічні пристрої (комп'ютери в готелях та інше), по можливості не виконуйте вхід на робочу електронну пошту. Не забувайте виходити з акаунтів.
9. Встановіть двофакторну аутентифікацію (технологія, що забезпечує ідентифікацію користувачів за допомогою комбінації двох різних компонентів) для входу в акаунти (окрім імені та паролю потрібно ввести код підтвердження (SMS-повідомлення, голосовий дзвінок та ін.)
10. Використовуйте, в разі потреби VPN та TOR.
11. Для спілкування використовуйте end-to-end encryption – захищене шифрування, наприклад, Signal (шифрування повідомлень та голосових дзвінків).

І наостанок, не носіть з собою чутливу інформацію та обмежуйте дані, які ви збираєте!

Інформація подана з матеріалів презентації Міхала Чижевського (Michał Czyżewski)

Питання цифрової безпеки є надзвичайно актуальним. Та основне питання, яке ми повинні поставити перед собою: від кого чи від чого ми повинні гарантувати безпеку? Потрібно розуміти, що може трапитись від втрати даних.

Перший приклад: студент/студентка.

Завдання: контролювати власні світлини та публікацію даних; не втратити роботу. А загрозами у цьому випадку можуть стати «doxing» (пошук та публікація приватної інформації про конкретну особу в Інтернеті, зазвичай зі шкідливими намірами) чи «ransomware» (тип шкідливого програмного забезпечення, призначеного для блокування доступу до комп'ютерної системи до сплати суми грошей).

Методи підсилення безпеки:

- Вибір додатків, які встановлюються на пристрій;

- Базова цифрова гігієна (оновлення програмного забезпечення та інші);

- Бекапи (резервне копіювання даних).

Другий приклад: журналіст/журналістка Завдання у цьому випадку можуть бути такими: публікування матеріалів стосовно злочинів; захист джерел інформації. Загрозами можуть бути: рейд на офіс чи житло; прикордонні служби; фішинг державних установ (форма шахрайства, в якій зловмисник під виглядом авторитетного суб'єкта або особи використовує фішингові електронні листи (чи інші засоби комунікації) для розповсюдження шкідливих посилань або вкладень, які можуть виконувати різні функції, включаючи вилучення облікових даних для входу або інформації про обліковий запис (в тому числі паролі та номери банківських карток).

Методи підсилення безпеки:

- Резервне копіювання, збережене в іншому місці;

- Сильний криптозахист (в тому числі використання захищених протоколів, якісних паролів та ін.);

- Резервне копіювання, збережене в іншому місці;

- Операційна безпека (процес, який визначає критичну інформацію, щоб проаналізувати, чи може хтось інтерпретувати інформацію, як корисну для них, а потім виконує заходи, які ліквідують вразливі місця та зменшують ризики), в тому числі це процес захисту окремих частин даних, які можуть бути згруповані для отримання більшої картини (агрегації).

Третій приклад: представник/представниця державної служби

Завдання у цьому випадку можуть полягати у розробці політик; зберігання їх в таємниці. Загрозами можуть стати репутаційна шкода, атака іноземного уряду.

Методи підсилення безпеки:

- Цифрова гігієна

- Операційна безпека

Міхал Чижевські (Michał Czyżewski)

хакер, захисник цифрових прав та IT-євангеліст вільного програмного забезпечення, член-засновник Варшавського хакерського простору (https://hackerspace.pl/about_en) та колективного мистецького простору ODRON (https://odron.org). Технолог із проекту звітності про організовану злочинність та корупцію (https://www.occrp.org/uk), раніше був Tech Lead та викладачем Фонду Panoptykon (https://en.panoptykon.org/) та організатором CryptoParty Warsaw.