Сафонова Т. Р., слухач
магістратури юридичного факультету
Науковий керівник – Косиченко О. О.,
доцент кафедри економічної
та інформаційної безпеки,
кандидат технічних наук, доцент
*(Дніпропетровський державний
університет внутрішніх справ)*

КРАДІЖКА ЦИФРОВОЇ ОСОБИСТОСТІ

Крадіжка цифрової особистості – злочин, за якого незаконно використовуються персональні дані людини для отримання матеріальної вигоди. Англійський термін Identity theft виник у 1964 р., його переклад «крадіжка цифрової особистості» є неточним, оскільки саму особистість вкрасти неможливо. Термінологія в цьому разі тільки заважає. По суті, крадуть персональні дані, які потім використовують для різних злочинних дій. Розглянемо, яку інформацію і навіщо крадуть.

Крадуть фотографії, паспортні дані, копії документів, селфі з документами, копії банківських карток. Ви можете через пошук в Google знайти чимало пропозицій купити копії паспортних даних, можете зустрити серед продаваних і свої.

Насамперед персональну інформацію крадуть для шахрайства. Розглянемо приклад. Якщо ви – красива дівчина, у вашому інстаграмі чоловіки зависають годинами і все у вас добре, поки за інформацією про вашу особу не прийде шахрай. Ваші дані і фотографії можуть прикрасити сторінку на сайті знайомств, з якої потім будуть виманювати передоплату у чоловіків, які бажають з вами познайомитись. Одна з подібних схем працює так: красива дівчина, за акаунтом якої ховається шахрай, знайомиться на сайті знайомств з чоловіком, якому відведена роль жертви. За допомогою шаблонних фраз і повідомлень зловмисник знаходить спільну мову, що закінчується запрошенням у кіно. Але це не звичайний кінотеатр, а квитки на приватні місця, де вони зможуть дивитися кіно лише удвох. Ну як від такого відмовитися? Подібні квитки продаються на спеціальному сайті і надаються як особлива послуга в кінотеатрах. На сайті є можливість оплатити карткою, можливість повернення коштів за квитки за годину до початку, і інші приємні для покупця моменти. Є тільки один маленький нюанс – сайт належить шахраю, і після оплати гроші підуть в кишеню зловмисника, а «красуня» припинить спілкування. Є й інші способи монетизації: фотографії в купальнику відмінно підійдуть для шахрайського сайту інтим-послуг і якщо ваші знайомі потраплять на нього, вам доведеться довго розповідати історію про крадіжку ваших фотографій і даних.

Розглянемо ще приклад щодо отримання бонусів і послуг з післяплатою. Можливо, ви бачили рекламу букмекерських компаній, форекс-сайтів, онлайн покер-румів або інших сайтів, що пропонують новим клієнтам гроші на рахунок, за які ви можете скористатися послугами. Все дуже просто: ваші дані будуть використані зловмисником для створення облікового запису з метою отримання бонусів. Як правило, це досить необразливо для жертви, хіба що ви не зможете скористатися рекламною пропозицією в майбутньому.

Куди менш райдужними можуть бути наслідки придбання на ваші дані послуг з післяплати, коли зловмисник реєструє на ваші дані акаунт, використовує послуги, а в кінці замість їх оплати просто зникає. У цьому разі від вашого імені відбувається повноцінне шахрайство.

Ще приклад. Фотографії красивих дівчат використовуються при створенні акаунтів для спаму в соціальних мережах, це збільшує частоту успішних атак. Найчастіше зловмисники не обтяжують себе міняти дані і беруть реальні дані жертви, включно з ім'ям і прізвищем.

Але не тільки красиві дівчата цікаві шахраям, будь-які крадені дані можуть бути використані для створення вебсторінок. Наприклад, відома російська фабрика тролів, яка була обвинувачена у втручанні у вибори США, використовувала для поширення даних сотні акаунтів. Як ви можете здогадатися, реальні власники даних не знали, що їх фотографії використовуються в політичній кампанії проти одного з кандидатів.

В мережі ви можете знайти пропозиції щодо продажу акаунтів в різних соціальних мережах та інших сайтах. Для реєстрації подібних акаунтів зловмисники також використовують крадені дані, рідше подібні акаунти збираються внаслідок фішингу або витоків даних.

Сьогодні, в умовах великої конкуренції, компанії, що займаються онлайн позиками повсюдно знижують планку вимог до позичальників, спрощуючи процедуру отримання невеликої суми. Подібні ризики цих шахрайських компаній окупають високі відсотки по позиках, які іноді доходять до тисячі відсотків на рік, і великі штрафи за будь-яке прострочення. Мінімізація перевірок і наданих даних перетворила онлайн позики в добре джерело доходів для шахраїв, що беруть позики на чужі персональні дані. У деяких випадках шахраям вистачить електронних копій двох документів жертви, наприклад, паспорта і прав водія. Можна для їх отримання створити оголошення про роботу і просити у потенційних претендентів після «прийняття» на роботу копії документів. Шахраї знають багато способів отримати копії документів і взяти на них позику.

Бувають і більш витончені схеми шахрайства з отриманням позик без відома власника. На одному з російськомовних андеграунд форумів якось з'явилася пропозиція про продаж авіаквитків за 50 % від їх реальної вартості. Власник сервісу, який пропонував послугу, запевняв, що ніякого шахрайства немає, авіаквитки не купуються на крадені кошти. Перший час відвідувачі

форуму ставилися з недовірою до пропозиції, потім позитивні відгуки почали залучати все більше і більше клієнтів. Клієнти відправляли зловмисникові всі персональні дані, включно з копіями документів. У жодного з клієнтів не виникло проблем з польотом. Проблеми виникли пізніше, коли банк, в якому ці квитки оформлялися в кредит без відома клієнтів, почав вимагати повернути суму за авіаквитки, відсотки і значні пені за прострочення. В результаті жертви заплатили по 200–300 відсотків від реальної вартості придбаних квитків.

Становить інтерес приклад шахрайства проти корпорацій. У соціальних мережах створюються профілі співробітників якої-небудь компанії, які там не зареєстровані, й додаються як друзі до реальних. Потім зав'язується спілкування з реальними співробітниками; наступні методи атаки вибирає зловмисник – це може бути компрометація реального співробітника або використання методів соціальної інженерії для одержання необхідних персональних даних для майбутнього шахрайства. Якщо в соціальній мережі до вас додався колега по роботі «як друг», обов'язково верифікуйте його, оскільки за його акаунтом можуть ховатися шахраї.

Висновки. Пам'ятайте: легше запобігти крадіжці цифрової особистості, ніж намагатися видалити персональну інформацію про себе з мережі. Практично це зробити дуже важко. Якщо десь в мережі хочуть отримати від вас персональну інформацію, то спочатку оцініть, що ви отримаєте натомість і чи варто це тих ризиків, які ви отримуєте. Особливо це стосується ваших паспортних даних, номерів телефону, домашньої адреси, акаунтів тощо.

Якщо вам все-таки хочеться десь зареєструватися, наприклад, для скачки книг, то заведіть собі для цих цілей акаунт, у логіну якого немає ваших прізвища й імені. Потім купіть собі нову сім-карту і зареєструйтеся під іншим прізвищем, іменем та по батькові. При цьому природно, дата народження й усе інше повинні бути вигаданими. Ви будете майже в безпеці. Крім того, є багато інших методів для забезпечення своєї особистої інформаційної безпеки.

Бібліографічні посилання

1. Макаров А. Как киберпреступники добывают и используют персональные данные. URL: https://www.anti-malware.ru/analytics/Threats_Analysis/Personal-data-dark-side
2. Косиченко О. О., Рибальченко Л. В. Проблеми безпеки персональних даних в Україні. *Регіональна економіка та управління*. Запоріжжя, 2019. № 4 (26). Ч. 2. С. 68–71.
3. Колисниченко Д. Н. Секреты безопасности и анонимности в Интернете. Санкт-Петербург : БХВ-Петребург, 2021. 256 с.