УДК 343.4

ТИПЫ КРАЖИ ЛИЧНОСТИ

Я.А. КУРТО
(Представлено: канд. ист. наук, доц. А.Л. РАДЮК)

В данной статье автор анализирует типологию одного из наиболее распространенных киберпреступлений современности - "кражи личности". Рассматриваются особенности каждого вида "кражи личности", а также оценивается актуальная угроза безопасности персональных данных в киберпространстве.

Возникновение сети Интернет и широкое внедрение услуг, предоставляемых удаленно, поставили под угрозу обеспечение безопасности персональных данных. С течением времени мошенники придумывали все более сложные способы завладеть персональной информацией. С конца XX века и по сегодняшний день сотни миллионов законопослушных граждан пострадали от "кражи личности" – использования идентификационной информации граждан в незаконных целях. Множество методов получения персональной информации повлияло на дифференциацию такого киберпреступления, как "кража личности".

Под "кражей личности" понимают мошенничество, которое заключается в получении персональных или финансовых данных пользователей с целью использовать личное имя или удостоверение личности человека для осуществления финансовых операций или покупок [1]. Англоязычный термин "identity theft" был введен в оборот в конце XX века и дословно переводится как "кража личности". По причине трудности перевода термина, в некоторых источниках также может встречаться иная, более точная формулировка феномена – "кража идентичности".

"Кража личности" является мошенничеством, состоящим из нескольких предварительных этапов. Основой данного киберпреступления является получение идентификационной информации человека. Существует значительное количество способов завладеть персональными данными личности. Некоторые из них носят характер фишинга, SMS-фишинга (смишинга), голосового фишинга (вишинг) и т.п. [2]. Однако персональные данные состоят из гораздо большего, чем личное имя, дата рождения или адрес жертвы. В большинстве случаев киберпреступники нацелены на получение номеров социального страхования (США, Великобритания), паспортных номеров, номеров банковских счетов, кредитных карт и биометрических данных. В Интернет-пространстве комплекс таких данных на подпольных сайтах известна как "фуллз" (fullz), и ее стоимость, как правило, оценивается приблизительно в 50 долларов. Стоит отметить, что даже при поимке торговца "краденными личностями" ничего не изымается, персональные данные обычно так и остаются на чёрном рынке. За исключением указанных выше способов "кража личности" может произойти вследствие утечек данных крупных компаний и взлома личного компьютера с помощью компьютерных вирусов.

Стоит отметить, что, хотя в большинстве случаев кража персональных данных совершается в интернете, субъекты подвергаются опасности хищения данных и в реальной жизни. Мошенники имеют возможность собрать персональную информацию при ненадлежащей утилизации документации, содержащей персональные данные, и устанавливать специальные приспособления в банкоматах с целью считывания банковских карт. Вслед за этим мошенники могут либо использовать персональные данные в преступных целях, либо продать их тем, кто сможет реализовать преступный умысел.

Как правило, слыша понятие "кражи данных", мы представим себе кражу и последующую утрату номеров банковских счетов и денежных средств. Такой феномен получил обозначение "финансовая кража личности" (financial identity theft). В таком случае преступники совершают "кражу личности" в корыстных целях.

Персональные данные также могут служить способом избежать наказания за преступление. Когда при задержании преступник представляется не под своим именем, речь идет о "преступной краже личности". Для подтверждения легенды он предоставляет украденные заранее документы. Помимо этого, мошенник портит юридическую историю потерпевшему.

Похититель личных данных в свою очередь может использовать медицинскую страховку для получения медицинской помощи от чьего-либо имени, тем самым обновляя документацию медицинской информацией мошенника. Это может привести к неверному лечению жертвы преступления в будущем. Иной вариант использования медицинских персональных данных – получение лекарств от имени пострадавшего.

Рассмотрим случай "медицинской кражи личности", который произошел в 2019 году в США. Доктор Пол Биддл, 54-летний анестезиолог из Нью-Йорка в течение 4 лет незаконно заказывал наркотические вещества, используя личную идентификационную информацию 23 пациентов, двое из которых умерли. В течение четырех лет врач выписал 888 поддельных рецептов на опиоиды, включая морфин. Он выписывал рецепты через аптеку в Тампе, штат Флорида, оплачивая их без страховки пациента, чтобы избежать обнаружения. Затем Биддл сам употреблял наркотики. Власти стали с подозрением относиться к количеству выписанных Биддлом рецептов на опиоиды. Следователи из Федерального бюро расследований (ФБР) и Управления по борьбе с наркотиками (DEA) начали обыскивать мусор доктора, где доказательства подтверждали, что он использовал информацию о пациентах, чтобы получить рецепты по почте самому себе [3].

Следует отметить, что дети все чаще становятся жертвами “кражи личности”. Совершить киберпреступление мошенникам способствует оцифровка школьных и медицинских записей. Детские данные стоят гораздо дороже на черном рынке, что делает их особенно привлекательной целью для воров. Причиной этому служит то, что несовершеннолетние имеют чистую кредитную историю. Родители, как правило, не задумываются о последствиях игнорирования защиты персональных данных, с которыми могут столкнуться их дети в будущем. По оценкам американских экспертов, семьи, подвергнувшиеся мошенничеству, заплатили более 540 миллионов долларов из собственных средств [4]. Однако существуют и случаи, когда родители использовали персональную информацию их детей для взятия кредитов на имя последних. Таким образом, при достижении определенного возраста ребенок захочет взять студенческий заем, но их банковская история уже будет испорчена. Впрочем, “детская кража личности” - не единственная причина возникновения финансовых проблем у будущих студентов.

Кроме всего прочего, в странах, где студенческий заем имеет распространенный характер, имеет место “кража личности” с использованием следующего метода. Мошенники, получая персональные данные жертвы, берут кредиты на образование на чужое имя, а далее обналичивают чеки, получая денежные средства. “Студенческая кража личности” имеет некоторую схожесть с “кражей личности” с использованием финансовых данных.

Разумно отметить, что пожилые люди более уязвимы для мошенничества с кражей персональных данных, потому что они более доверчивы, менее склонны следить за своими финансовыми счетами, или не знают, на какие угрозы следует обращать внимание. Они могут столкнуться с налоговым мошенничеством, захватом счетов, кражей медицинских данных и многим другим. Это может привести к большим финансовым потерям, при отсутствии достаточных знаний о методах борьбы с киберпреступлениями [5].

Практически невозможно предотвратить и распознать исключительный тип “кражи личности” – синтетическую “кражу личности”. Она значительно отличается от традиционной “кражи личности”, потому что преступники не крадут личность – они создают ее, используя комбинацию реальной и поддельной информации [6]. В июле 2018 года Счетная палата США (U.S. GAO) опубликовало краткий отчет о форуме, созванным Генеральным контролером США на тему мошенничества с использованием синтетических идентификационных данных. Эксперты пришли к выводу о растущей угрозе кибербезопасности, в том числе национальной, но так и не смогли прийти к единому мнению об ущербе, которое повлекло за собой данное киберпреступление. Специалисты оценивают потери от 50 до 250 миллионов долларов до 1 миллиарда долларов за 2016 год [7].

Благодаря крупнейшим центрам ведения статистики и расследования данных преступлений в Соединенных Штатах – Федеральному Бюро Расследований США и Федеральной торговой комиссии (FTC) – мы можем располагать точной статистикой “краж личности”. Федеральная торговая комиссия – это государственное учреждение США, которое помогает защитить потребителей от мошенничества, включая "кражу личности". Согласно отчету комиссии за февраль 2021 предоставил пугающую статистику об увеличении случаев хищения персональной информации, с 444,344 (2018 г.), 650,523 (2019 г.) до 1,387,615 (2020 г.) на территории Соединенных Штатов [8].

Тем не менее, население стало в меньшей степени бояться киберпреступлений. Если в 2014 году, «хищение персональных данных» и «безопасность в сети Интернет» входили в топ-5 рейтинга опасений жителей США, составленного исследователями Чепменского университета (США) [9], то в 2021 году то же исследование поместило “кибертерроризм” лишь на 8 строчку [10].

Реализация “кражи личности” всецело зависит от степени безопасности данных человека в сети Интернет. Именно поэтому эксперты советуют не открывать подозрительные ссылки или вложения, а также неожиданные письма с просьбой подтвердить данные и, кроме того, не передавать свою персональную информацию посредством соцсетей. Более того, следует по крайней мере раз в год проверять свою кредитную отчетность на факт подозрительных действий и тем самым обезопасить себя от “кражи личности”.

Статистика кибератак позволяет сделать вывод о том, что современная всемирная система безопасности личных данных имеет множество недостатков. “Кража личности” обоснованно подверглась разграничению по способам совершения киберпреступления, однако имеют место быть и общие характеристики мошеннических схем. Таковыми являются месть, нанесение вреда репутации человека и желание легкого заработка. Понимание различных способов мошеннических атак может помочь защитить персональную информацию личности и ее финансы. С нашей точки зрения, институт “кражи личности” должен быть освещен в большей степени как средствами массовой информации, так и органами безопасности на местах.

ЛИТЕРАТУРА

1. Кража личности [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/news/tags/%D0%BA%D1%80%D0%B0%D0%B6%D0%B0+%D0%BB%D0%B8%D1%87%D0%BD%D0%BE%D1%81%D1%82%D0%B8/. – Дата доступа: 24.09.2021.

2. 11 Types of Phishing + Real-Life Examples [Electronic resource]. - Mode of access: https://www.pandasecurity.com/en/mediacenter/tips/types-of-phishing/. – Date of access: 27.09.2021.
3. Daitch, H. Real Identity Theft Stories. Case #9: New York Doctor Opioid Addiction Using Patient Information / H. Daitch // Identity Force [Electronic resource]. – 2019. – Mode of access: https://www.identityforce.com/blog/real-identity-theft-stories-part-9 – Date of access: 26.09.2021.
4. Morris, C. More Than 1 Million Children Were Victims of Identity Theft in 2017 / C. Morris // Fortune [Electronic resource]. – 24.04.2018. – Mode of access: https://fortune.com/2018/04/24/stolen-identity-theft-children-kids/ – Date of access: 26.09.2021.
5. Porter, K. 10 Types of Identity Theft You Should Know About / K. Porter // NortonLifeLock [Electronic resource]. – 17.10.2017. – Mode of access: https://www.lifelock.com/learn-identity-theft-resources-types-identity-theft.html – Date of access: 27.09.2021.
6. FBI, This Week: Synthetic identity Theft [Electronic resource]. – 02.01.2020. – Mode of access: https://www.fbi.gov/audio-repository/ftw-podcast-synthetic-ids-010220.mp3/view – Date of access: 28.09.2021.
7. Highlights of a Forum: Combating Synthetic Identity Fraud [Electronic resource]. – 26.07.2017. – Mode of access: https://www.gao.gov/products/gao-17-708sp – Date of access: 28.09.2021.
8. Consumer Sentimel Network. Federal Trade Commission February 2021 [Electronic resource]. – Mode of access: https://www.ftc.gov – Date of access: 05.04.2021.
9. What Americans Fear the Most [Electronic resource]. - Mode of access: https://blogs.chapman.edu/wilkinson/2014/10/21/what-americans-fear-the-most/. – Date of access: 24.09.2021.
10. 11 Types of Phishing + Real-Life Examples [Electronic resource]. - Mode of access: https://www.pandasecurity.com/en/mediacenter/tips/types-of-phishing/. – Date of access: 27.09.2021.