**КОГДА ЛИЧНОЕ СТАНОВИТСЯ ПУБЛИЧНЫМ**

***Кто и почему продает мошенникам наши персональные данные?***

Интернет-мошенники, используя наши персональные данные,
с каждым годом совершенствуют технологии своих преступлений.

***Сколько стоят наши данные в сети и к чему может привести их утечка?***

Мне нужно было просто заказать плойку для волос. Обычная процедура онлайн-покупки, которую я проделывала много раз. Зашла на сайт, выбрала модель, ввела свой номер телефона, имя, адрес доставки и нажала на «заказать». Через некоторое время раздался звонок оператора.— Добрый день. Вы заказывали плойку. Верно?— Да.

— Нам нужны ваши паспортные данные.

— Для чего? Я ведь не собираюсь брать товар в кредит.

— Это необходимо для оформления гарантийного письма.

— Как я могу быть уверена, что после нашего разговора мои данные не станут достоянием мошенников?

— Просто поверьте нам.

И будь я менее осведомлена в вопросах безопасности личных данных, без сомнения, продиктовала бы всю запрашиваемую информацию. А между тем, когда плойка была уже у меня, курьеру не понадобилось ничего, кроме моей подписи. Остается только догадываться, кто и с какой целью хотел получить данные, которые не являются обязательными для покупки плойки. И это происходит повсеместно…

Для того чтобы получить скидочную карту, еще совсем недавно магазины просили заполнить анкеты с 20 вопросами. Семейное положение, дата рождения, предпочтения в еде, одежде, косметике, гражданство и многое другое. Вся эта информация аккумулируется в одном месте, превращаясь в огромную базу данных. А представьте, что таких баз — миллионы.

***Кража личности***

В 1964 году в Англии появился термин «кража личности». Он обозначает преступление, при котором незаконно используются персональные данные человека для получения материальной выгоды. Это явление приобрело особое распространение в США во второй половине XX века и было вызвано широким внедрением услуг, предоставляемых удаленно, без личного присутствия. По телефону можно было выпустить карту, получить кредит. Достаточно было продиктовать свой уникальный страховой номер или идентификатор личности (аналог нашего личного номера паспорта). Сначала личные данные похищали с помощью телефона и просеивания мусорных контейнеров в поисках выброшенных счетов, квитанций и других документов, содержащих личные данные. С появлением интернета основным средством мошенничества стала сеть. Сегодня большинство мошенников используют специальные программы-вымогатели. Фишинговые атаки являются предпочтительной формой кражи данных. Они требуют меньше усилий и приносят больше денег. Американская некоммерческая организация «Ресурсный центр по краже личных данных», которая помогает жертвам интернет-мошенников, недавно заявила, что одна атака с использованием программ-вымогателей может принести столько же дохода за считаные минуты, сколько сотни попыток кражи личных данных в течение нескольких лет. Согласно исследованию этой организации, в прошлом году от утечки данных пострадали 300 млн американцев.

В феврале уже этого года мошенники украли из американского бюджета 36 млрд долларов.

Эти деньги предназначались для выплаты пособий по безработице. Государственные служащие думали, что выплачивают эти деньги людям, которые остались без работы. Вместо этого они перечисляли их на счета мошенников, которые представлялись другими гражданами, чьи личности они украли. И теперь этим самым гражданам еще предстоит выплатить налог на пособия по безработице.

***Сколько стоят данные?***

По информации американских экспертов, на черном рынке США набор информации для кражи личности, включающий адрес и SSN, стоит от 16 до 30 долларов. Вероятность стать жертвой такого преступления оценивается в 2 процента для среднего жителя США.

В русскоговорящем сегменте интернета данные о человеке часто предлагают приобрести в формате строк. Это подборка персональных данных о человеке, используя которую, можно «отрисовать» (для этого существуют целые компании) реальный документ. А затем с этим документом сделать, к примеру, ставки в казино или подать заявку на кредит.

— Это из сложного. А вот базу телефонных номеров, пригодную для «работы», собрать несложно. Можно написать простенький скрипт, который будет проходить по объявлениям с бесплатных сайтов и сохранять телефонные номера в подходящем формате, — рассказывает один из тех, кто зарабатывает подобным образом.

В крайнем случае собиратели данных могут копировать номера и вручную.

Понятное дело, что мошенники будут искать потенциально небедных людей. Например, тех, кто продает машины, квартиры, норковые шубы, предпоследние iPhone. Чаще всего вместе с номером телефона жулики получают как минимум имя жертвы.

Чтобы не собирать номера самостоятельно, они часто покупают готовые базы номеров телефонов. Оптом всегда дешевле.

Можно даже в даркнет не ходить. Подобные базы продают и для «холодных звонков». Продавец не уточняет, кто покупает файл: бизнесмен, который хочет поднять продажи, или мошенник. Обычно в таких базах достаточно много информации. В том числе Ф.И.О., пол, возраст, место проживания, уровень доходов, интересы, профессии, семейное положение. Вот пример подобного сайта. Цена контакта — 59 копеек.

***Белорусские реалии***

Не так давно белорусская милиция задержала более 20 человек, которые воровали деньги у граждан с использованием реквизитов их банковских платежных карт. Свыше 100 человек признаны потерпевшими. Ущерб огромный — более миллиона белорусских рублей.

Владимир Зайцев, замначальника главного управления по противодействию киберпреступности МВД:

— «Переодеваясь» в сотрудников различных банков нашей страны, они искусно манипулировали жертвой: сообщали ложную информацию о совершаемом хищении с банковских счетов. После чего звонящие предлагали гражданам для предотвращения несанкционированных операций либо сообщить реквизиты своих карт, либо перевести деньги со своего счета на ложный, либо предоставить доступ к системе дистанционного банковского обслуживания и сообщить коды, приходящие на телефон. Иногда просили установить на смартфон специальное приложение для удаленного администрирования. На протяжении года они осуществляли телефонные звонки через виртуальные номера зарубежных операторов или использовали мессенджеры.

За десять лет в десять раз увеличилось количество хищений с банковских карточек белорусов. А за первые месяцы 2021 года уже зафиксирован рост более чем на 270 процентов по сравнению с этим же периодом прошлого года. Тот факт, что преступлений стало больше, не вызывает удивления у тех, кто знаком со статистикой Национального банка. За десять лет выросло не только количество преступлений, но и примерно на 80 процентов увеличилось число карточек, ежегодно выпускаемых нашими банками. Белорусы сегодня предпочитают хранить сбережения в электронном виде. Мошенники, видя это, используют различные схемы по выманиванию данных о картах. В помощь им — базы данных белорусов, размещенные в интернете, приобрести которые стоит совсем недорого. А дальше начинается преступное мастерство.

Например, в ход идут звонки от имени фальшивых работников банков, надувательство с использованием торговых площадок, взломы социальных сетей и многие другие приемы. Деньги с карточки могут перевести сразу на чужой счет. Либо вся эта информация попадет на специализированные форумы, где покупка и продажа подобных данных, изготовление на их основании фальшивых карт и обналичивание средств поставлены на поток.

В прошлом году оперативники УВД Миноблисполкома тоже вышли на след организованной группы, которая, используя известную интернет-площадку объявлений, обокрала более 350 человек.

— Преступники создали в Telegram закрытую группу, в которой собрали интернет-мошенников и обсуждали свои планы и структуру работы. Они создавали копии страниц реальных объявлений и подбрасывали их потенциальным жертвам. Но в отличие от оригинала фейковая страница предусматривала функцию ввода данных карточки. Жертвы думали, что переводят деньги продавцу, но на самом деле переводили средства мошенникам, — говорит Дмитрий Дудков, начальник управления по раскрытию преступлений в сфере высоких технологий УВД Миноблисполкома.

***В чем причина?***

«Количество сетевых пользователей растет, но сетевая грамотность не повышается», — Дмитрий Бродко, следователь по особо важным делам центрального аппарата Следственного комитета, говорит, что одна из причин стремительного роста подобного типа преступлений кроется в человеческой халатности. С ним согласен и Дмитрий Дудков. Каждый день оперативники его подразделения получают десятки сообщений от граждан о том, что у них выманили деньги с карты. При этом удивительно, но в 95 процентах случаев, говорит Дудков, потерпевшие честно признаются: мы знали о том, что нельзя никому рассказывать данные карточки. Как такое возможно?

Все дело в том, что интернет-мошенники подходят к своей задаче профессионально. Они обучаются методам внушения и при общении с жертвой используют психологические приемы, которые действительно работают.

50-летний житель Минской области шесть раз отвечал на звонки «из банка», каждый раз ответственно сообщая лжебанкирам информацию о своей карте. За полтора часа методом уговоров под различными предлогами мошенники оформили на его карту кредит в размере 8000 рублей. И это произошло за то время, пока мужчина чинил свою машину. Он сам предоставил жуликам всю информацию, будучи уверен, что звонят из его банка.

— Среди потерпевших от подобного вида мошенничества много людей с высшим образованием, есть и представители банков, сотрудники органов внутренних дел, — говорит Дмитрий Дудков.

Неудивительно, ведь граждане соглашаются на уговоры воров, стремясь защитить свои средства. Например, женщина из Минской области, которая сообщила все реквизиты своей карточки звонившему мошеннику, который уверял, что в данный момент кто-то без ее ведома совершает операцию по карте и ее срочно нужно отменить. Но «отменить» у воров не получилось, потому что у держателя карты была установлена защита. Звонивший предложил подойти в банк и разблокировать эту защиту. Ничего не подозревающая жертва пришла в свой банк и все сделала, как ей было велено. Вечером ей перезвонил лжесотрудник и осуществил все нужные переводы. Стремясь защитить свои деньги, жительница Минщины их потеряла...

***Куда уходят деньги?***

— Большинство денежных средств переводятся на счета иностранных учреждений. В некоторых случаях, но гораздо реже, переводы осуществляются на белорусские счета, — рассказывает Дудков. Дальнейшая судьба украденных денежных средств, как правило, туманна. Так, по информации первого заместителя прокурора Минской области Бориса Петровского, в регионе раскрывается лишь 2 процента подобных преступлений. Кроме того, согласно политике банков, владелец карты несет ответственность за ее использование. А это значит, что тот, кто добровольно сообщил данные карты мошеннику, уже не может рассчитывать на какую-либо компенсацию.

***Что делать?***

Парламент уже принял Закон «О персональных данных». После подписания документа Президентом личная информация, которую мы предоставляем банкам, магазинам, медицинским центрам, будет находиться под надежной защитой. Ответственность за ее распространение будут нести операторы — те, кто ее собирает. Следить за добросовестностью операторов будет регулятор (его вскоре определит Совет Министров).

При этом правоохранительные органы со своей стороны также предпринимают меры. Андрей Ковалев, начальник главного управления по противодействию киберпреступности МВД, говорит, что в нашей стране в целом выстроена система, которая позволяет влиять на складывающуюся криминогенную обстановку, связанную с преступностью в сфере высоких технологий. Вместе с тем, по его словам, она требует совершенствования. Поэтому и был разработан проект комплексного плана мероприятий, направленных на принятие эффективных мер по противодействию киберпреступлениям. В план включили в том числе и совершенствование механизма блокировки интернет-ресурсов, которые занимаются противоправной деятельностью.

Кроме этого, оперативники еще больше внимания уделят деятельности координаторов дропов — людей, которые помогают преступникам обналичивать деньги, украденные с помощью интернета. Не так давно в законодательство внесены изменения, которые позволят привлекать к ответственности за подобные деяния.

В план также включили и возможность блокирования банковских счетов, по которым проводятся подозрительные (сомнительные) финансовые операции, а также усиление контроля за порядком распространения SIM-карт, чтобы исключить их анонимное использование. Важный момент, на который обращает внимание Ковалев, — внедрение эффективных систем противодействия мошенничеству (фроду) на сетях электросвязи. Фрод — язва электронной коммерции. Любая компания, которая принимает платежи на своем сайте, рано или поздно сталкивается с проблемой фрода и несет от него убытки. Системы противодействия такому виду мошенничества смогут защитить не только граждан, но и госпредприятия, а также бизнес.