Одним из самых распространённых преступлений сегодня является «угон личности». Эти преступления сегодня наиболее распространены в США, Китае и России.

Что такое «угон личности»?

Иначе **Identity theft** – кража идентификационных «удостоверительных» признаков человека. Какие признаки удостоверяют вас как личность? Прежде всего это

- общие данные;
- биометрия.

Что такое общие данные? Это ФИО, номер паспорта, почта, номер телефона, контакты, семейное положение, место работы, биография и т.д.

Что такое кража личных данных?

Кража личных данных – это получение конфиденциальной личной, финансовой или иной (например, СНИЛС) информации другого лица с единственной целью – использовать имя или личность этого лица для совершения неправомерных действий. Кража личных данных является преступлением и совершается по-разному.

Виды кражи личных данных

Типы кражи личных данных включают в себя преступную, медицинскую, финансовую и детскую кражу личных данных.

В преступной краже личных данных преступник выдаёт себя за другое лицо во время ареста, чтобы попытаться избежать повестки, предотвратить обнаружение ордера, выданного на его настоящее имя или избежать задержания.

В краже медицинской идентичности кто-то идентифицирует себя как другой человек, чтобы получить бесплатную медицинскую помощь.

При краже финансовых личных данных кто-то использует личность или информацию другого лица для получения кредита, товаров, услуг или льгот. Это наиболее распространённая форма кражи личных данных.

Синтетическая кража личных данных является одним из видов мошенничества, в котором преступник сочетает в себе реальную (обычно украденную) и поддельную информацию для создания новой личности, которая используется для открытия мошеннических счетов и мошеннических покупок.

Высокотехнологичная кража личных данных

При осуществлении кражи личных данных всё чаще используют компьютерные технологии для получения личной информации других людей с целью мошенничества. Чтобы найти такую информацию, злоумышленники могут искать жёсткие диски украденных или выброшенных компьютеров, выброшенные гаджеты, проводить взлом смартфонов, компьютеров или компьютерных сетей, получать доступ к компьютерным публичным записям, использовать информацию, полученную с помощью вредоносных программ для заражения компьютеров, просматривать сайты социальных сетей или использовать фишинговые электронные письма или текстовые сообщения.

Кража личных данных происходит так часто, что Федеральное бюро расследований называет её «самой быстрорастущей проблемой преступности в Америке».

Типы мошенничества с использованием личных данных

Кража личных данных – это когда кто-то использует вашу личную информацию без вашего ведома в преступных целях.

Злоумышленники могут использовать украденную информацию для получения доступа к вашим финансовым счетам, взлома ваших учётных записей в Интернете и/или обмана других. Получив доступ к личной информации, похитители личных данных могут следующее:

- тратить деньги со счетов;
- открывать новые банковские счета;
- изменить пароли и контактную информацию для онлайн-аккаунтов;
- подать заявку на получение ссуд, кредитных карт и льгот на своё имя;
- снять квартиру или машину;
- совершать другие преступления.

Другая форма кражи личных данных – это когда кто-то создаёт учётные записи в социальных сетях или на веб-сайтах, используя ваше имя, изображение и/или другую информацию. Хотя это не может нанести вред вашим финансовым счетам, но может повредить репутации. Впрочем, вред финансам тоже может нанести, создав клон вашей учётной записи, а затем попросив друзей перевести денег.

В этом случае ознакомьтесь с условиями сайта или веб-сайта социальной сети, чтобы узнать, как действовать в отношении учётной записи, в которой ложно используется ваше имя или изображение. Если речь идёт о преступной деятельности (например, если кто-то создаёт поддельные учётные записи в Интернете на ваше имя, чтобы беспокоить вас), то сделайте скрины экрана этой онлайн-активности и подайте заявление в местную полицию.

Как воруют личность

Общие методы включают следующее:

- Взлом аккаунта. Это почта, социальная сеть, портальные ресурсы. Атаковать будут, скорее всего, полным перебором паролей, перехват сессии, социальная инженерия, вредоносное ПО типа keyloger.
- Поиск данных через остаточную информацию. Тут «охота» посерьёзнее (хотя народ охотится и за зашифрованными данными с подбором симметричного ключа).
- Поиск личных документов, выброшенных вами в мусорную корзину.
- Взлом банкоматов с целью кражи вашей банковской информации.
- Получение личной информации через общедоступные источники (например, телефонные книги и социальные сети).

Похитители личных данных обычно ищут:

- персональные данные, а дальше используют их по назначению. Например, «утащили» базу с персональными данными, а там только ФИО и телефоны. Далее злоумышленники делают обзвон от имени службы ИБ Сбербанка (наверняка не зная является ли жертва клиентом): «Вы такой-то?»;
- банковские карты и ПИН-коды;
- СНИЛС, страховое (особенно водительское, чтобы потом рекламой заняться или развести на «липовую» страховку);

- паспорт;
- водительское удостоверение;
- SIM-карту.

Ваша личность также может быть украдена из ваших онлайн-транзакций. Если вы не меняете свои пароли и регулярно не усиливаете свои функции веб-безопасности, кто-то может легко получить доступ к таким данным, как

- электронная почта (для кражи личной и финансовой информации, расписаний и т.д.);
- учётные записи онлайн-покупок (для кражи информации о кредитной карте и адресе);
- банковские счета (для перевода средств, открытия новых счетов или подачи заявки на кредит);
- счета кредитных карт (для покупок и подачи заявки на новые карты);
- государственные счета (для изменения вашей контактной информации в государственных удостоверениях личности, льготах и т.д.).

Признаки кражи личных данных

Ваша личная информация может быть украдена без вашего ведома.

Многие люди узнают, что стали жертвами кражи личных данных, когда им неожиданно отказывают в ссуде, работе или аренде из-за проверки кредитоспособности. Вот почему очень важно проверять свой кредитный отчёт хотя бы один раз в год на наличие ошибок или странных действий. Не забывайте проверять уведомления об операциях через почту или SMS.

Могут быть и другие признаки кражи личных данных:

- счета и выписки не приходят в срок – они могли быть украдены из вашего почтового ящика или кто-то мог изменить почтовый адрес ваших счетов;
- вам звонят из коллекторских агентств или от кредиторов по поводу долга, которого у вас нет;
- вы получаете уведомление от банка, или онлайн-бизнеса о новой учётной записи на ваше имя или дополнительных расходах;
- в отчётах о финансовых счетах показаны снятия или переводы, которые вы не совершали;
- кредитор звонит, чтобы сказать, что вам был одобрен или отклонён кредит, который вы не оформляли.

Украсть почту

Давайте подумаем, насколько защищён ваш почтовый ящик? Чаще всего почтовый ящик защищён с помощью обычного пароля. Причём, увы, очень часто пользователи не обременяют себя придумыванием сложного пароля, а обходятся простым «123456» или *Anna2001* для ящика *anna2001@* yandex.ru. Ну и что тут красть? Хотя гораздо проще отправить для Анны письмо от службы ИБ Yandex и заставить сменить её пароль, указав старый и очень защищённый новый на «нашем портале yandex».

Вторая типичная ошибка – использовать один и тот же пароль на различных интернет-сайтах.

Третья довольно распространённая ошибка – хранение паролей на устройстве. Например, в смартфоне. Вы сдаёте ваш смартфон в ремонт? Он защищён сложным PIN-кодом? Длиной хотя бы 6 символов? Да ну?!

На компьютере вы храните пароли в браузере?

И таких ошибок я смогу привести массу. К чему это приводит? Злоумышленник получает ваш пароль к почте. Затем меняет пароль в социальной сети, в учётной записи, привязанной вами к этому же почтовому ящику. Всё! Для атаки от имени вас в социальной сети готово все. Далее от вашего имени вашим друзьям отправляется рассылка с просьбой прислать денег. Причём это самое безобидное.

Как защитить?

Всё больше и больше почтовых сервисов и сервисов социальных сетей используют двухфакторную аутентификацию. При этом для входа в социальную сеть помимо пароля вам нужен ещё и 6-7-значный цифровой код, который меняется каждые 30 секунд в генераторе на вашем гаджете или приходит к вам по SMS (следует учесть, что вариант с SMS менее надёжен).

Биометрия

Образец голоса

Первый биометрический признак – голос. Вспомните, как часто вам звонили с какими-то рекламными предложениями? А перед выборами? «Вас беспокоит соцопрос». А вы уверены, что вам звонят не для того, чтобы получить ваш образец голоса? А ведь подделать голос сегодня совсем не сложно, верно?

А дальше в ход идёт специальное ПО по обработке голоса. Мошенник говорит, а программа переделывает его голос в голос жертвы. Включая интонацию. Дальше идёт звонок родителям, жене, друзьям. «Мама, я попал в полицию». Верно? А почему нет!

Я живой! Или клонирование личности

Другой вариант – использование социальных сетей. Создание фейкового аккаунта-двойника в социальных сетях. Самая частая причина «клонирования» – желание снизить репутацию жертвы.

А теперь вспомните, сколько информации вы сами оставляете в социальных сетях? Сами. Добровольно!

Но что делать если личность уже украдена?

Защитите свою личность

Не забудьте о цифровой гигиене.

- Как можно меньше вашей информации храните в цифровом формате.
- Не храните персональные данные где попало (в облаке, на непонятных устройствах).
- Защищайте устройства с персональными данными с помощью сложных паролей, а лучше с помощью двухфакторной аутентификации с криптографией.

Кроме того:

- Ежедневно очищайте свой почтовый ящик (если вы уезжаете в отпуск, попросите друзей или надёжных соседей забрать вашу почту).
- Храните удостоверения личности и документы, такие как свидетельства о рождении, номера социального страхования и паспорта, в надёжном месте, например в запираемом несгораемом сейфе.
- Уничтожайте любые документы и предметы с личной информацией, если они вам больше не нужны (например, просроченные документы, квитанции и финансовые отчёты).

- Регулярно проверяйте остатки по выпискам из банков, кредитных карт.
- Немедленно сообщайте о любых странных действиях в своих счетах и выписках, даже незначительных (мошенники часто воруют небольшие суммы со многих карт, чтобы избежать обнаружения).
- Проверяйте свой кредитный отчёт один раз в год на наличие ошибок или странных действий.
- Избегайте разглашения какой-либо личной информации по телефону, если вы не звоните сами.
- Избегайте выдачи конфиденциальной личной информации, такой как номер кредитной карты, по телефону, когда вы находитесь в общественном месте (вы никогда не знаете, кто может вас подслушивать).

При совершении покупок

- Носите с собой как можно меньше карт и документов и всегда проверяйте, что кредитная карта, которую вы получаете от кассира, является вашей собственной.
- Никогда не сообщайте никому PIN своей банковской карты, а тем более её номер и CVV.
- Убедитесь, что никто не смотрит, когда вы используете банкомат или POS-терминал.
- Избегайте использования банкоматов в изолированных или тускло освещённых местах. Используйте банкомат в офисах банка (закрытых помещениях) – это защитит вас от кардеров со скиммерами и шиммерами.
- Избегайте раскрытия слишком большого количества личной информации.
- Самое главное – никому не передавайте вашу карту (а то в ресторанах многие передают, а ведь если положить карту внутри чека и провести ручкой, то из-за эмбоссирования номер карты останется на другой стороне чека, а CVV запомнить не сложно.

Если вы в сети или используете мобильное устройство

- Часто меняйте пароли и делайте их надёжными. Совет, безусловно, правильный, но в реальности невыполнимый. Ведь надёжный пароль, увы, быстро забывается! Поэтому гораздо проще использовать менеджер паролей. Какой? Выбирать вам: не хочу, чтобы упрекнули в рекламе. А лучше используйте двухфакторную или двухэтапную аутентификацию (сложность паролей сейчас уже не защита).
- Избегайте размещения в Интернете личной информации, такой как дата рождения и почтовый адрес.
- Убедитесь, что вы просматриваете и понимаете настройки конфиденциальности на всех сайтах социальных сетей, которые вы используете, прежде чем публиковать какие-либо обновления (вам следует регулярно проверять настройки конфиденциальности, поскольку они часто меняются).
- Отключите опцию «географическое отслеживание» на вашем телефоне перед публикацией общедоступных фотографий в социальных сетях (по умолчанию эта опция включена на большинстве телефонов и позволяет кому-то точно определить, где были сделаны ваши фотографии). Но не обольщайтесь, в любом случае вас можно отследить.
- Перед тем, как продать или утилизировать свой компьютер, телефон или планшет, полностью сотрите жёсткий диск или уничтожьте его или всё устройство. К сожалению, уничтожают чаще всего путём простого удаления без маскирования. Это значит, что информация остаётся там же.
- Рассмотрите возможность настройки оповещений по электронной почте или SMS, которые будут уведомлять вас каждый раз, когда осуществляется операция, связанная с безопасностью: вход в сервис, смена пароля, выполнение банковской операции, ваше имя используется где-то в Интернете и т.д.
- Избегайте покупок в Интернете и банковских операций при использовании общедоступного Wi-Fi, поскольку соединение может быть небезопасным. Убедитесь, что ваш домашний Wi-FI использует защищённый протокол, а то соседи его могут за 10 секунд взломать.
- Прежде чем сообщать компании номер своей кредитной карты или другую финансовую информацию, убедитесь, что это безопасный веб-сайт (найдите символ блокировки, расположенный где-нибудь на веб-странице, или убедитесь, что URL-адрес начинается с https...).
- После завершения финансовой операции в Интернете убедитесь, что вы вышли с веб-сайта и очистили файлы cookie и кэш браузера. И снова, совет, в принципе, правильный, да вот только так делают лишь законченные параноики вроде меня. Гораздо проще, если вы задумали провести финансовую операцию, воспользоваться режимом Incognito и автоматически стереть все следы по окончании сеанса или хотя бы выполнить корректный logout с сайта финансового учреждения.
- Отдельно напомню счастливым обладателям токенов с электронными подписями и сертификатами. Вставляйте их только для выполнения аутентификации или финансовой транзакции. Никогда не предоставляйте к ним общий доступ по сети.
- Убедитесь, что на вашем компьютере установлены последние обновления операционной системы, антивирусных баз и другого прикладного ПО, используемого в системе.
- Не загружайте приложения или программное обеспечение на свой телефон или планшет, если они получены не из официальных магазинов приложений или библиотек.
- Минимизируйте набор приложений для выполнения повседневных операций. В случае инсталляции банковских клиентов избегайте установку приложений, «чтобы попробовать». Если ваш телефон поддерживает защищённую папку (разделение телефона на обычную и защищённую область), инсталлируйте банковские клиенты именно в неё.
- Знайте, что правительственные организации, финансовые учреждения и полиция никогда не будут отправлять электронные письма или текстовые сообщения с просьбой сообщить ваши пароли или PIN-коды.
- Никогда не переходите по ссылке из спам-сообщения, особенно если оно обещает награды, призы или любую эксклюзивную информацию.

Владимир Безмалый
Microsoft Security Trusted Advisor
Microsoft MVP
Kaspersky Certified Trainer
Консультант ООН по информационной безопасности