Генеральный прокурор Нью Йорка Литиция Джеймс
Letitia James

Dear New Yorker,

Ваша идентификационная информация находится под угрозой. В Интернете, по телефону и даже при личной встрече мошенникам как никогда легко украсть вашу личную информацию и использовать ее для мошеннических действий.

От кражи личных данных ежегодно страдают миллионы людей. Мошенники оформляют на ваше имя кредитные карты, получают ваши медицинские пособия и даже используют ваш номер социального страхования для налоговых махинаций, нанося ущерб вашему кредитному статусу и вынуждая тратить время и деньги на исправление ситуации.

Вы можете защитить свою личную информацию и предотвратить большинство форм кражи личных данных, приложив немного усилий, и мы готовы помочь вам узнать, как это сделать.

Более подробную информацию о том, как сохранить свои личные данные в безопасности или что делать, если вы считаете, что ваши данные были украдены, можно найти на нашем сайте ag.ny.gov.

С уважением,

Letitia James

Источники

Офис Генерального прокурора штата Нью-Йорк, Бюро по борьбе с мошенничеством в отношении потребителей

Сообщайте о мошеннических действиях или подавайте жалобу.

(800) 771-7755 / ag.ny.gov

Федеральная торговая комиссия США

Сообщайте о мошеннических действиях или кражах персональных данных.

877- 382-4357 / ftc.gov

Годовые кредитные отчеты

Проверить или заморозить кредитные операции.

877-322-8228 / annualcreditreport.com

Основные агентства кредитной отчётности

Experian:
(888) 397-3742 / experian.com

TransUnion:
(800) 888-4213 / transunion.com

Equifax
(800) 685-1111 / equifax.com

Innovis
innovis.com

Защитите свою личную информацию

Рекомендации для обеспечения безопасности вашей личности

Генеральный прокурор Нью Йорка Литиция Джеймс
Letitia James

Защитите свою личную информацию.

Хотя обычно предоставление своего имени или номера телефона безопасно, предоставление кому-либо даты рождения, номера социального страхования или номера любого счета может привести к краже вашей личности. Вам также следует избегать раскрытия любой информации, которую вы используете в качестве “запасного” ответа для веб-сайтов, при восстановлении пароля.

Никогда не сообщайте свою личную информацию человеку, который случайно обратился к вам. Если вы сами не обращались к нему, есть вероятность, что вас пытаются “поймать на удочку”.

Фишинг - это попытка заставить жертву предоставить личную информацию, такую как имя пользователя, пароль или номер кредитной карты. Мошенники могут писать вам СМС, звонить по телефону или отправлять письма по электронной почте. Они часто выдают себя за государственное учреждение, банк или известную компанию. Они потребуют вашу личную информацию, чтобы решить какую-то проблему или чрезвычайную ситуацию, или скажут, что им просто нужно “подтвердить вашу информацию”, прежде чем они смогут вам что-то предоставить.

На самом деле, ни одна из этих организаций не станет связываться с вами таким образом для получения важной информации. Если вы не уверены, позвоните в компанию - по опубликованным номерам, чтобы уточнить, действительно ли это были они. Некоторые фишинговые атаки содержат просьбу перейти на веб-сайт или открыть прикрепленный файл. ***Не скачивайте прикрепленные файлы и не переходите по ссылкам от незнакомых людей.*** Они могут содержать вирусы, которые могут заразить ваш компьютер и украсть вашу личную информацию.

Подозрительные сообщения

Даже если кажется, что сообщение пришло из надежного источника, например, от родственника или известной компании, это все равно может быть попытка фишинга: мошенники могли завладеть аккаунтом или создать новый аккаунт с похожим именем. Если вы получили сообщение нехарактерное отправителю, содержит только ссылку или вложение без каких-либо объяснений или кажется подозрительным, дважды проверьте поле “от”, чтобы убедиться, что это правильный адрес, или позвоните отправителю, чтобы убедиться, что это действительно он. Подобное может произойти как в социальных сетях, так и по электронной почте или текстовым сообщениям, поэтому не доверяйте подозрительному сообщению только потому, что оно пришло от “друга”.

Номер социальной страховки

Компании практически нет необходимости запрашивать ваш номер социальной страховки. Если они его запрашивают, спросите, зачем он им нужен, особенно если это не государственное учреждение, работодатель, банк или финансовая организация. ***И, опять же, никогда не давайте его тому, кто связался с вами без просьбы.***

Используйте брандмауэр, обновляйте свою операционную систему

Использование интернета может сделать ваш компьютер уязвимым для вирусов. Обновляйте свою операционную систему и антивирус, а также держите брандмауэр включенным, чтобы обеспечить безопасность.

Создавайте надежные пароли

Если вы пользуетесь интернетом, вам нужны надежные пароли, и их должно быть несколько. Надежный пароль:

- Длинный Он должен содержать как минимум восемь символов, но чем больше, тем лучше.
- Его не должен угадать тот, кто изучит вас, поэтому никаких дней рождения или имен родственников.
- Вы можете его запомнить. Сочетание длинных, необычных слов (“batterystapler”) может быть полезным.
- Использован только один раз. Если вы повторите пароль и кто-то узнает его один раз, он сможет получить доступ ко всем вашим учетным записям.

Диспетчер паролей

В современных браузерах есть “диспетчер паролей”, который можно установить и он запомнит ваши пароли за вас: просто загрузите менеджер, и все остальное будет сделано автоматически. Храните пароль от вашего диспетчера как можно надежнее: если мошенник получит к нему доступ, он сможет получить доступ ко всем вашим учетным записям.

Защита устройств паролем

Относитесь к учетным записям на мобильных телефонах и компьютерах так же, как к учетным записям на веб-сайтах: создавайте для них уникальные, надежные пароли.

Пароли по умолчанию

Некоторые устройства, например, роутер или модем, поставляются с паролем по умолчанию. Пароли по умолчанию редко бывают надежными, поэтому их следует немедленно изменить.

Регулярно меняйте пароли

Даже если вы следуете этому совету, чем дольше вы используете пароль, тем больше вероятность того, что его получит злоумышленник: веб-сайты могут быть небезопасны. Всегда меняйте пароль, если сайт, который вы посещали взломали, и периодически меняйте пароли в любом случае, чтобы оставаться в безопасности.

Защищённые соединения

Небезопасный веб-сайт или сеть Wi-Fi могут раскрыть вашу личную информацию. Никогда не ведите личные или финансовые дела по общественной сети, и проверяйте “безопасность” веб-сайта, прежде чем передавать конфиденциальную информацию. Безопасные веб-сайты будут начинаться с **“https://”** вместо **“http://”**

Удалите ненужные данные

Уничтожайте все записи с личной информацией, если они вам больше не нужны. Уничтожайте физические документы, такие как квитанции, налоговые декларации, финансовые или медицинские записи; удаляйте или деактивируйте цифровые учетные записи и удаляйте цифровые файлы. Помните, что даже удаленные файлы могут оставаться на жестком диске, поэтому вам понадобится специальное программное обеспечение безопасности, чтобы стереть все личные данные, если вы избавляетесь от старого компьютера.

Проверяйте выписки

Внимательно проверяйте выписки с кредитных карт и банковских счетов на предмет любых действий, не санкционированных вами.

Тщательно проверяйте медицинские счета и медицинскую страховку, чтобы убедиться, что вы действительно получили описанное лечение.

Отчёт о Кредитных Операциях

Каждый человек имеет право на получение одной бесплатной копии своего отчёта о кредитных операциях в год, от каждого из основных бюро кредитных историй. Если вы видите счета или запросы, которые вы не инициировали или не узнали, это может указывать на то, что кто-то другой пытается использовать вашу личность. На сайте annualcreditreport.com или по номеру (877) 322-8228 можно заказать отчеты из разных агентств в разное время года для получения регулярного покрытия.

Кража персональных данных детей.

Чаще всего личные данные детей крадут члены семьи с плохим кредитным рейтингом. Защищайте личную информацию своих детей так же, как и свою собственную. Обязательно задавайте вопросы и принимайте меры, если они получают звонки с требованием оплатить счета или кредитные предложения на их имя, если им отказывают в пособии, потому что кто-то другой использует их номер, или если они получают уведомления от Налогового управления США о причитающихся налогах.