office of neighborhood involvement

Мы способствуем распространению культуры вовлечения гражданской общественности, поддерживая общение и сотрудничество всех жителей Портленда и правительства в процессе создания гостеприимных, безопасных и повышающих качество жизни жилых районов и общин.

1221 SW 4th Avenue, Suite 110
Portland, Oregon 97204

Тел. 503-823-4000
Факс 503-823-3050
Телетайп 503-823-6969

Аманда Фриц,
комиссионер

Амалия Аларкон де Моррис,
директор бюро

Город и округа

Информация и направления: телефонная служба

503-823-4000

●

Этот документ можно найти на сайте ONI по адресу

www.portlandonline.com/oni/cp

Хищение личных данных

Когда ущерб наносится от вашего имени...

Программа предотвращения преступлений отдела вовлечения общественности
Весной 2009 г.

Хищением личных данных называют использование вашей персональной информации, такой, как ваши имя и фамилия, номер в системе социального обеспечения или личные финансовые данные, в мошеннических или других преступных целях. Восстановление высокой репутации и рейтинга кредитоспособности жертвы хищения личных данных может быть очень длительным и трудным процессом. Гораздо проще предотвращать такое хищение.

Как осуществляется хищение личных данных?

КАК ПОХИТИТЕЛИ ДАННЫХ ПОЛУЧАЮТ ДОСТУП К ВАШЕЙ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ

- Доступ к конфиденциальной информации можно получить, похищая записи или данные из коммерческих предприятий или учреждений, находясь на работе, подкупая служащего, имеющего доступ к таким записям, посредством «взлома» компьютерных баз данных или обманным путем, вступая во взаимодействие со служащими от вашего имени.
- У вас могут украсть почту, в том числе выписки из банковских счетов, предложения кредитных карт и новые неиспользованные чеки.
- Кроме того, ваш кошелек или ваши личные данные могут быть похищены непосредственно из вашего дома или вашей квартиры.

Скимминг, фишинг, претекстинг и просмотр мусора

Похитители личных данных могут красть номера ваших кредитных или дебитных карт, загружая информацию в электронное устройство для хранения данных, подсоединенное к банкомату или связывающееся со службой передачи данных; такое хищение данных называют «скиммингом» («снятием сливок» в буквальном переводе с английского). Ваши личные данные могут быть похищены по электронной почте («фишинг») или в ходе обмена текстовыми сообщениями по телефону («претекстинг»); при этом похитители притворяются, что представляют действительно существующие компании или учреждения, утверждая, что возникла та или иная проблема, связанная с вашими счетами. Похитители личных данных могут рыться в вашем мусоре в поиске документов, содержащих интересующую их информацию.

Как предотвратить хищение личных данных?

ЗАЩИТА СЧЕТОВ

- Защищайте паролями доступ к вашим кредитным, банковским и телефонным счетам. При этом старайтесь не использовать в качестве паролей легкодоступную информацию, такую, как девичья фамилия вашей матери, дата вашего рождения, последние четыре цифры вашего номера в системе социального обеспечения, ваш телефонный номер или простые закономерные последовательности чисел.
- Защищайте личные данные, хранящиеся у вас дома, особенно если вы совместно арендуете жилье с другими людьми, нанимаете помощников или поручаете кому-либо выполнять работу у вас в доме.
- Узнавайте, какие меры защиты информации принимаются у вас на работе, а также в коммерческих предприятиях, кабинетах врачей и других организациях и учреждениях, получающих информацию, позволяющую удостоверять вашу личность. Узнавайте, осуществляется ли обмен относящейся к вам информацией с другими сторонами, и каким образом.
- Не предоставляйте ваши личные данные по телефону, по почте или с помощью Интернета, если вы не были первой стороной, устанавливавшей связь, и если вы не уверены, что точно знаете, с кем имеете дело. Перед тем. как предоставлять любые личные данные, убеждайтесь в том, что вы имеете дело с действительно существующей организацией.
- Сбрасывайте исходящие почтовые отправления в ящики почтового отделения или отдавайте их работнику почтового отделения, но не сбрасывайте их в не охраняемый почтовый ящик.
- Измельчайте квитанции, подтверждающие произведенные вами выплаты, копии заявок на получение кредита, страховые формы, счета врачей, чеки и банковские отчеты, выбрасываемые кредитные карты, срок действия которых истек, а также предложения кредитных карт, получаемые по почте. Для того, чтобы больше не получать новые предложения кредитных карт по почте, позвоните по тел. 1-888-5-OPTOUT.
- Не носите с собой карточку с вашим номером в системе социального обеспечения; оставляйте ее в защищенном месте.
- Сообщайте свой номер в системе социального обеспечения (SSN) только тогда, когда это совершенно необходимо. Если кто-либо просит вас предоставить ваш номер в системе социального обеспечения, спрашивайте: «Зачем он вам нужен? Как он будет использоваться? Как вы защищаете такую информацию от хищения? Что произойдет, если я не сообщу вам этот номер?»
- Заказывая новые чеки, забирайте их в банке сами, не получайте их по почте.

КОМПЬЮТЕРНЫЕ СРЕДСТВА ЗАЩИТЫ

- Следует регулярно обновлять антивирусное программное обеспечение и устанавливать пакеты обновления вашей операционной системы и других программ с тем, чтобы предотвращать доступ неуполномоченных лиц к вашей компьютерной информации и защищать ваш компьютер от инфекций, способных скомпрометировать ваши компьютерные файлы и пароли.

- Не открывайте файлы, полученные от незнакомых вам людей, не выбирайте щелчками мыши ссылки, назначение которых вам неизвестно, и не загружайте программы, предлагаемые неизвестными вам сторонами.
- Пользуйтесь «эффективными» паролями — сочетаниями заглавных и строчных букв и цифр.
- Для того, чтобы предотвращать нежелательный доступ к вашему компьютеру, установите программу межсетевой защиты, если вы пользуетесь высокоскоростной линией компьютерной связи, круглосуточно подсоединенной к вашему компьютеру.
- Не осуществляйте какие-либо финансовые операции, пользуясь Интернетом, если вы не установили защищенный браузер, шифрующий информацию, не подлежащую распространению. Пользуйтесь электронными адресами, начинающимися с сокращения «https», а не «http», и проверяйте состояние пиктограммы замка, находящейся в нижней части окна браузера.
- Проверяйте правила обеспечения конфиденциальности данных, применяемые на сайтах, для того, чтобы узнать, каким образом обеспечиваются точность, доступность, защита и контроль личных данных на сайте, как будут использоваться эти данные и будут ли они предоставляться третьим сторонам.

Если ваши личные данные были похищены...

ПРИНИМАЙТЕ МЕРЫ БЕЗОТЛАГАТЕЛЬНО

- Предупредите о возможности мошенничества с использованием ваших кредитных карт и внимательно проверяйте отчеты об операциях, осуществленных с помощью ваших кредитных карт. Предупреждения о возможности мошенничества позволяют предотвращать открытие похитителем данных каких-либо новых счетов от вашего имени. Обратитесь в одно из трех кредитных бюро:

  Equifax: 1-800-525-6285; www.equifax.com
  Experian: 1-888-397-3742; www.experian.com
  TransUnion: 1-800-680-7289; www.transunion.com
- Закройте те счета, которые, как вам известно или как вы подозреваете, могут использоваться неуполномоченными лицами или могли быть открыты мошенническим образом.
- Сообщите о хищении в местную полицию или в полицию того района, где имело место хищение.
- Подайте жалобу в Федеральную торговую комиссию США. Для того, чтобы зарегистрировать вашу жалобу, посетите сайт www.ftc.gov/idtheft или позвоните по тел. 1-877-438-4338.
- Получите экземпляр документа «Контролируйте ситуацию: борьба с хищением личных данных» («Take Charge: Fighting Back Against Identity Theft») из Федеральной торговой комиссии США (см. выше ее адресные данные) и следуйте ее рекомендациям, относящимся к решению проблем, связанных с хищением личных данных.

ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ О ХИЩЕНИИ ЛИЧНЫХ ДАННЫХ

Гораздо более подробные сведения о предотвращении хищений личных данных и решении проблем, связанных с такими хищениями. см. на сайте *www.ftc.gov/idtheft*
Наша справочная брошюра содержит лишь краткую сводку чрезвычайно полезных советов по предотвращению хищения данных, предлагаемых на этом сайте.