IDENTITYTHEFTVICTIMS
ASSISTANCE NETWORK PROJECT

Massachusetts Elder Identity Theft Coalition

Facilitators:

Janice Fahey, Legal Analyst
Mila Mignosa, Program Coordinator
Дженис Фэхи, Юрист-Консультант,
Мила Мигноса, Координатор Программы
Ten Mechanic Street, Suite 301
Worcester, MA 01608
Phone: 774-214-4420 Fax: 774-214-4453

This presentation was produced by Massachusetts Elder Identity Theft Coalition under award #2016-XV-GX-K004, awarded by the Office for Victims of Crime, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this presentation are those of the contributors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

КОАЛИЦИЯ ПО БОРЬБЕ И ПРЕДОТВРАЩЕНИЮ КРАЖИ ЛИЧНЫХ ДАННЫХ И МОШЕННИЧЕСТВУ В ШТАТЕ МАССАЧУСЕТС

Генеральный прокурор Мора Хили создала Коалицию по борьбе с мошенничеством и предотвращению кражи личных данных в штате Массачусетс с помощью гранта от Национальной Сети Помощи Жертвам Мошенничества и Предотвращению Кражи Личных Данных.

Коалиция создана для поддержки и оказания помощи пожилым людям, тат как они более всего подвержены нападениям мошенников и часто становятся жертвами похитителей личных данных. Они очень уязвимы в силу своего возраста, доверчивости и незнанию как безопасно пользоваться интернетом и компютером.

Задача Коалиции - обеспечить меры по улучшению информационно-пропагандистской деятельности и предоставлению программ помощи жертвам мошенничества и кражи личных данных.

КОАЛИЦИЯ ПО БОРЬБЕ И ПРЕДОТВРАЩЕНИЮ КРАЖИ ЛИЧНЫХ ДАННЫХ И МОШЕННИЧЕСТВУ В ШТАТЕ МАССАЧУСЕТС

ЦЕЛИ:

1. Обучить пожилых людей как защитить себя от мошенничества и правильно хранить и использовать личную информацию.

2. Предоставить тренинг организациям, служащим пожилым людям, по оказанию помощи жертвам мошенничества, включая пошаговый план восстановления после кражи личных данных.

3. Повысить осведомленность среди организаций и бизнесов, которые иногда используются мошенниками в совершении кражи личных данных, с целью предотвращения.

СОДЕРЖАНИЕ ПРЕЗЕНТАЦИИ

- Что такое кража личных данных?
- Как преступники похищают и используют ваши личные данные?
- Советы как снизить риск оказаться жертвой кражи личных данных и мошенничества
- Последствия и что делать, если ваши личные данные были украдены
- Методы и примеры мошенничества

Какие данные являются личными?

Имя и фамилия, или инициал имя и фамилии в сочетании с одним или несколькими из следующих:

- Номер социального страхования
- Номер водительской лицензии или номер удостоверения личности
- Номер финансового счета, кредитной или дебетовой карты

Какие данные являются публичными?

- Ваше имя
- Дата вашего рождения
- Домашний адрес
- Адрес электронной почты
- Номер мобильного или городского телефона

DATA BREACH - ПРОНИКНОВЕНИЕ ХАКЕРОВ В СИСТЕМУ БИЗНЕСОВ С ЦЕЛЬЮ ПОХИЩЕНИЯ ЛИЧНОЙ ИНФОРМАЦИИ ПОТРЕБИТЕЛЕЙ

Случается, когда личная информация потребителей доступна через систему держателя информации или была извлечена и использована неавторизованным лицом для несанкционированного использования.

ПРИМЕРЫ

- **Таргет (январь 2014 г.)** Торговая компания

  Хакеры проникли в сеть Таргет и заразили все кассовые аппараты
- **Anthem Inc. (май 2015 г.)** Организация в сфере здравоохранения Атака привела к краже личных данных более 80 миллионов пациэнтов.
- **Equifax (сентябрь 2017 года)** Компания, хранящая кредитную историю и предоставляющая отчеты о кредитоспособности частных и юридических лиц. 143 миллиона потребителей подверглись утечке личной информации, что составляет примерно половину страны.

ЧТО ДЕЛАТЬ, ЕСЛИ ЕСЛИ ПРОИЗОШЛО ХИЩЕНИЕ ЛИЧНОЙ ИНФОРМАЦИИ

- Запросите и проверьте кредитный отчет
- Подумайте о том, чтобы заморзить кредитование
- Постарайтесь заполнить налоговую декларацию в начале налогового сезона

IDENTITY THEFT - КРАЖА ЛИЧНЫХ ДАННЫХ

- Похищение вашей личной информации может произойти через проникновение воров в компьютерную систему или же воры могут обманно вынудить вас поделиться с ними вашей личной информацией с целью получения финансовых выгод. Например, действовать от вашего имени проводя финансовые операции с банками, открывая новые кредитные линии на ваше имя.

КАК ПОХИТИТЕЛИ МОГУТ ИСПОЛЬЗОВАТЬ ВАШУ ЛИЧНУЮ ИНФОРМАЦИЮ?

- Получать медицинские и другие льготы
- Заполнить налоговую декларацию от вашего вашего имени, с целью получения денежного возврата
- Открыть кредитную линию на ваше имя
- Совершить преступление

ЧТО ДЕЛАТЬ, ЕСЛИ КТО-ТО ВОСПОЛЬЗОВАЛСЯ ВАШЕЙ ЛИЧНОЙ ИНФОРМАЦИЕЙ? ШАГ 1

- Обратитесь в кредитную компанию, где произошло мошенничество
- Попросите закрыть или заморозить эту кредитную карту
- Измените логины, пароли и персональные идентификационные номера (PINS) своих кредитных и дебетовых карт

ЧТО ДЕЛАТЬ, ЕСЛИ КТО-ТО ВОСПОЛЬЗОВАЛСЯ ВАШЕЙ ЛИЧНОЙ ИНФОРМАЦИЕЙ? ШАГ 2

- На веб-сайте Федеральной Комиссии по Торговле (FTC), подайте заявление с жалобой, используя эту ссылку www.ftc.gov
- Зарегестрируйтесь на веб-сайте и ответьте на вопросы
- На основе вашей информации, IdentityTheft.gov создаст ваш отчет о краже личных данных и план восстановления
- Учетная запись позволяет отслеживать прогресс

ЧТО ДЕЛАТЬ, ЕСЛИ КТО-ТО ВОСПОЛЬЗОВАЛСЯ ВАШЕЙ ЛИЧНОЙ ИНФОРМАЦИЕЙ? ШАГ 3

- Напишите заявление в полицию
- Попросите копию заявления
- Это позволит вам получить бесплатный отчет о вашей кредитной истории
- Заявление поможет защитить вас в будущем, если кто-то использует ваши личные данние, чтобы совершить преступление или открыть кредитную карту на ваше имя
- Заявление может потребоваться для выполнения других шагов

ПЕРВОНАЧАЛЬНОЕ УВЕДОМЛЕНИЕ О МОШЕННИЧЕСТВЕ ШАГ 4

- Свяжитесь с одним из трех кредитных бюро и сообщите о мошенничестве
- Это кредитное бюро должно уведомить двух других
- Уведомление действительно в течение 90 дней
- Уведомление бесплатно
- Вы сможете открывать новые кредитные линии. Рекомендуется, если вы планируете совершить большую покупку
- Предотвратит возможность открытия новых кредитных карт на ваше имя мошенниками

ДОЛГОСРОЧНОЕ УВЕДОМЛЕНИЕ О МОШЕННИЧЕСТВЕ
ШАГ 4

- Необходимо связаться с каждым из 3 кредитных бюро
- Уведомление действительно 7 лет
- Бесплатно разместить и удалить, если кто-то воспользовался вашими личными данными с целью мошенничества
- Позволяет вам иметь доступ к вашим кредитным отчетам, но требует дополнительной проверки вашей личности

КОНТАКТНАЯ ИНФОРМАЦИЯ КРЕДИТНЫХ БЮРО ДЛЯ УВЕДОМЛЕНИЯ О МОШЕННИЧЕСТВЕ

- **TransUnion.com/fraud**

1-800-680-7289

- **Experian.com/fraudalert**

1-888-397-3742

- **Equifax.com/CreditReportAssistance**

1-888-766-0008

ЗАМОРАЖИВАНИЕ КРЕДИТА
ШАГ 4

- Необходимо связаться со всеми 3-мя кредитными бюро
- Уведомление действительно, пока вы не отмените
- В данний момент требует небольшой платы (Новое федеральное законодательство по отмене платы вступит в силу в сентябре 2018 года)
- Вы не сможете открыть новые кредитные линии
- Останавливает доступ к вашему отчету о кредите, до тех пор, пока вы его не удалите

КОНТАКТНАЯ ИНФОРМАЦИЯ КРЕДИТНЫХ БЮРО ДЛЯ УВЕДОМЛЕНИЯ О ЗАМОРАЖИВАНИИ КРЕДИТА

- **TransUnion.com/freeze**

1-888-909-8872

- **Experian.com/freeze**

1-888-397-3742

- **freeze.Equifax.com**

1-800-349-9960

ЗАПРОС БЕСПЛАТНОГО КРЕДИТНОГО ОТЧЁТА
ШАГ 5

- Вы имеете право на бесплатный кредитный отчет раз в год из всех трёх бюро
- Запросите свой кредитный отчёт из всех трёх кредитных бюро на веб-сайте annualcreditreport.com
  или позвоните по номеру 1-877-322-8228
- Получив свой кредитный отчёт, проверьте нет ли в отчёте подозрительных и незнакомых кредитных линий
- **Подсказка:** если запрашивать бесплатний кредитный отчет каждые четыре месяца из разного кредитного бюро, то вы сможете держать под контролем вашу кредитную историю круглый год

КАК МОШЕННИКИ МОГУТ УКРАСТЬ ВАШИ ЛИЧНЫЕ ДАННЫЕ?

- Ваш мусор
- Ваша почта
- Кража вашего кошелька или сумки
- Фишинг - выудить у вас вашу личную информацию по электронной почте или по телефону
- Установление в банкоматах устройства, которое сканирует и передаёт мошенникам вашу личную информацию
- Похощение (Data Breach) вашей личной информации у провайдеров, с которыми вы имели бизнес (торговые или здравоохранительные организации и т.п.)

КАК ЗАЩИТИТЬСЯ ОТ ВОРОВСТВА ЛИЧНОЙ ИНФОРМАЦИИ?

- Купите и используйте устройство (shredder), уничтожающее документы, содержащие вашу личную информацию
- Старайтесь не доставать кредитную/дебитовую карту заранее в магазине пока стоите в очереди
- Отправляйте письма в почтовом отделении
- Никогда не давайте личную информацию по телефону или интернету (за исключением случаев, когда вы инициатор контакта)
- Не позволяйте копировать вашу водительскую лицензию
- Старайтесь не пользоваться общественным WI-FI

ПРИЗНАКИ, ЧТО КТО-ТО УКРАЛ ВАШИ ЛИЧНЫЕ ДАННЫЕ

- Вы перестали получать электронную почту
- Вам присылают медицинские или другие счета за услуги, которые вы не получали
- С вашего банковского счета снимаются деньги за товары, которые вы не покупали
- С вами связываютя долговые коллекторы относительно незнакомых долгов
- Налоговая служба информирует вас (в письменной форме) о том, что одна или несколько налоговых деклараций были поданы от вашего имени

МОШЕННИЧЕСТВО

- Попытка отдельного лица или организации получить вашу личную информацию. Например, номер дебетовой/кредитной карты или номер социального страхования
- Заставить вас купить ненужный товар или услугу

ТЕЛЕФОННЫЕ ЗВОНКИ/ АВТОМАТИЗИРОВАННИЕ ЗВОНКИ

- С помощью техники, мошенники используют трюк, известый как «спуфинг»
- Таким образом, номер звонящего абонента определяется с местным кодом вашей территирии, это заставит вас подумать что звонит кто-то знакомый, и поднять трубку

ПРИМЕРЫ МОШЕННИЧЕСТВА ПО ТЕЛЕФОНУ

- Обман бабушек и дедушек
- Коммунальные услуги
- Национальная лотерея
- Взыскание долгов
- Мошенничество с новой страховой картой Medicare
- Звонки из налоговой инспекции
- Фальшивые государственные субсидии
- Звонки из фальшивых благотворительных организаций
- Предложение перефинансировать кредитный ссуду на жильё

КАК РАСПОЗНАТЬ МОШЕННИКОВ?

- Неестественно длинная пауза после того, как вы подняли трубку, за которой следует предварительно записанное сообщение
- Просьба нажать определённую цифру на телефоне, чтобы «отказаться от будущих звонков» - **НЕ ДЕЛАЙТЕ** этого, так как это уведомит базу данных о том, что ваш номер активный, и мошенники будут продолжать звонить
- Вы выиграли приз или лотерею, но вам нужно оплатить налоги или сборы

КАК ПРЕДОТВРАТИТЬ МОШЕННИЧЕСТВО?

- Не отвечайте, когда звонят с неизвестного номера
- **ПОМНИТЕ:** если это важно, вам оставят сообщение
- Если вы подняли трубку и понимаете, что это мошенничество, не вовлекайтесь в разговор. Положите трубку
- Не поддавайтесь давлению немедленно принять решение

РАЗНОВИДНОСТИ МОШЕННИЧЕСТВА

ОТ ДВЕРИ К ДВЕРИ

- Подрядчики по благоустройству дома или двора
- Продавцы, продающие подписку на журнал
- Звонки, требующие пожертвований для несуществующей благотворительной организации или использующие имя известной благотворительной организации, но не имеющие ничего общего с ней

КАК ПРЕДОТВРАТИТЬ МОШЕННИЧЕСТВО?

- Не открывайте дверь людям, которых вы не знаете
- Не начинайте беседы с незнакомцами, стучащими в вашу дверь
- Если вы подозреваете, что это мошенничество, немедленно позвоните в местную полицию

ИНТЕРНЕТ/КОМПЬЮТЕР

- **Сайбер-преступность** - противозаконная деятельность, которая использует компьютерное устройство и сеть интернета

ИНТЕРНЕТ/КОМПЬЮТЕР

Электронный почтовый адрес

- Мошенники используют спуфинг для маскировки электронных писем как-будто они от друзей или родственников, и просят срочного перевода денег через Western Union, Money Gram или PayPal
- Новинка - мошенники нацелены на корпорации и бизнесы с поддельными запросами руководства совершить банковский перевод

КАК РАСПОЗНАТЬ МОШЕННИКОВ?

Такое электронное сообщение обычно:

- Содержит ссылку с очень небольшим количеством деталей
- Содержит грамматические и орфографические ошибки
- Запрашивает личную/финансовую информацию

КАК ПРЕДОТВРАТИТЬ МОШЕННИЧЕСТВО?

- Никогда не нажимайте на ссылки в письмах, если вы не уверены кто прослал сообщение
- Установите антивирусное программное обеспечение с автоматическим обновлением
- Установите фильтрацию спам-сообщений
- Проверьте орфографические ошибки в адресе отправителя электронной почты

ИНТЕРНЕТ-ПОКУПКИ

- Поиск в Интернете или опечатка может привести вас к веб-сайту, который похож на тот, что вы хотите посетить, но не является подлинным
- Избегайте совершения Интернет-покупок у неизвестных торговых компаний
- Старайтесь расплачиваться кредитной картой. Это предоставит вам дополнительную защиту в случае, если товар бракованный или не доставлен
- Ознакомьтесь с условиями договора купли-продажи, возврата и гарантии

КАК РАСПОЗНАТЬ МОШЕННИКОВ?

- Внимательно осмотрите веб-сайт, прежде чем вводить личную информацию
- Убедитесь, что сайт защищён – в поле ввода номера кредитной карты убедитесь, что имеется замок или ключевой символ
- Ищите SSL - «безопасный уровень сокета», обозначенный «https:»
- Пример: https://www.mass.gov/

АУКЦИОНЫ В ИНТЕРНЕТЕ

- **Помните** - аукционы организуются, чтобы помочь встретиться покупателю с продавцом
- Регулярные правила и условия защиты прав потребителей могут не применяться к аукционам
- Просмотрите условия доставки и возврата товара перед тем как делать ставки
- Убедитесь, что сайт предлагает защиту участникам торгов, в случае, если товар не доставлен, не является таким, как был описан, или не был доставлен

Куда сообщить об интернет-мошенничестве?

- **ФЕДЕРАЛЬНОЕ БЮРО РАССЛЕДОВАНИЙ:** www.ic3.gov

СОЦИАЛЬНЫЕ СЕТИ

- Farcing: создание ложных аккаунтов в социальных сетях для совершения мошенничества
- Происходит на популярных платформах социальных сетей, таких как Facebook, Twitter, Instagram, LinkedIn и Google Plus
- Используются для интернет-хулиганства, кражи личных данных, организационного шпионажа, распространения детской порнографии и взлома аккаунтов

КАК ПРЕДОТВРАТИТЬ МОШЕННИЧЕСТВО?

- Не публикуйте личную информацию на сайтах социальных сетей
- Не делитесь своей личной информацией с малознакомыми людьми в Интернете
- Будьте осторожны, принимая приглашения дружбы в социальных сетях

ЗАКОНЫ И ПРАВА КОНФИДЕНЦИАЛЬНОСТИ

Согласно Закону о конфиденциальности, федеральные агенства, агенства штата, а также городская администрация должны информировать потребителя о следующем:

- Является ли запрос номера социального страхования добровольным
- Цель запроса номера социального страхования
- Последствия в случае непредоставления номера социального страхования
- Полномочия/закон, на основании которых запрашивается номер социального страхования

ОРГАНИЗАЦИИ ТРЕБУЮЩИЕ ПРЕДОСТАВЛЕНИЯ НОМЕРА СОЦИАЛЬНОГО СТРАХОВАНИЯ

1. Налоговая полиция
2. Медицинские страховые организации

(Коммерческие страховые компании, Medicaid, Medicare)

3. Администрация ветеранов (прием пациентов в больницу)

ОРГАНИЗАЦИИ ТРЕБУЮЩИЕ ПРЕДОСТАВЛЕНИЯ НОМЕРА СОЦИАЛЬНОГО СТРАХОВАНИЯ

4. Государственные учреждения

- Школьные программы питания
- Предоставление государственной помощи
- Водительские лицензии
- Получение субсидий для детей
- Продовольственные талоны
- Компенсация по безработице
- Временная помощь нуждающимся семьям

ОРГАНИЗАЦИИ ТРЕБУЮЩИЕ ПРЕДОСТАВЛЕНИЯ НОМЕРА СОЦИАЛЬНОГО СТРАХОВАНИЯ

5. Работодатели (налоговая отчетность/зарплата/проверка прошлого)
6. Банки (денежные операции, включая создание аккаунта PayPal)
7. Коммунальные услуги
8. Департамент труда (компенсация работникам)
9. Департамент образования (студенческие ссуды)
10. Казначейство США (облигации Сбербанка США)