S.A.F.E.

Senior Anti-Fraud Education

Senior = *Пожилой человек*

Anti = *Против*

Fraud = *Мошенничество*

Education = *Образование*

Распознайте мошенническую схему до того, как станете ее жертвой

NEW YORK STATE OF OPPORTUNITY. | Division of Consumer Protection

Защита прав и информирование потребителей Нью-Йорка

Подразделение Департамента штата Нью-Йорк (New York Department of State)

Andrew M. Cuomo, Губернатор

Rossana Rosado, Государственный секретарь штата

Как пожилым людям защитить себя от мошенников

Пожилые люди часто становятся жертвами мошенников. Преступники выбирают их, так как зачастую они уязвимы и одиноки и могут стать легкой добычей правонарушителей. Очень важно знать о мошеннических схемах, чтобы не стать их жертвой. Ниже приведены шесть наиболее распространенных схем, которые используют мошенники в отношении пожилых людей, а также советы о том, как обезопасить себя.

* * * * *

• Мошенничество с медицинским оборудованием

Пожилые люди неоднократно сообщали о получении автоматических звонков, которые известны как robocalls. Ответившему на звонок человеку предлагается бесплатное устройство медицинской сигнализации, а также купоны со скидками. При этом для получения бесплатного устройства достаточно нажать цифру «1» и указать адрес, а также данные кредитной карты. После нажатия цифры «1» звонок переводится на оператора, который использует тактику запугивания, чтобы получить персональные и финансовые данные. Кроме того, в сообщении говорится о возможности нажать другую клавишу, чтобы отказаться от звонков в будущем. Однако в случае нажатия такой клавиши мошенники получают соответствующее уведомление о действующем номере телефона, который в дальнейшем может быть использован для реализации преступных схем.

• Мошенническая схема с использованием информации о родственниках

В этом случае мошенники звонят или пишут электронные письма пожилым людям с просьбой выслать деньги. Они представляются близкими родственниками, оказавшимися в трудной ситуации и нуждающимися в деньгах. Часто звонки поступают ночью, поэтому пожилому человеку может быть сложно сориентироваться. Информация звучит очень правдоподобно, поскольку мошенники используют искусные методы получения персональных данных с помощью социальных сетей и поиска в интернете. В некоторых случаях мошенник представляется сотрудником полиции, адвокатом или врачом, звонящим от лица такого родственника, попавшего в трудную ситуацию. Во всех случаях мошенники просят перевести деньги немедленно и, как правило, безналичным способом.

• Мошенническая схема Ghosting

Схема Ghosting является одним из способов кражи персональных данных. Воры собирают персональные данные о скончавшихся людях из некрологов, получают такие данные в похоронных бюро, больницах, из украденных свидетельств о смерти и на веб-сайтах. После получения подобной информации, особенно номеров социального страхования, они используют ее для установления кредитных отношений, открытия счетов, получения ссуд, пособий и даже налоговых возмещений по декларациям, поданным с использованием подложной информации. Родственники умершего не несут материальной ответственности в результате такой кражи персональных данных, если их имена не фигурируют в украденных счетах. Необходимо обязательно уведомить Управление социального обеспечения (Social Security Administration) о смерти вашего родственника.

• Мошенническая схема с информацией о якобы невыполненной обязанности в качестве присяжного

В таком случае мошенники представляются сотрудниками правоохранительных органов или судов и уведомляют жертву о неисполнении обязанностей присяжного. В связи с этим они сообщают о необходимости уплаты штрафа, чтобы избежать ареста. Во многих

случаях, если жертвы сообщают мошенникам о том, что они не получали никакой информации о необходимости выполнить обязанности присяжного, звонящий подчеркивает важность исполнения гражданского долга в качестве присяжного независимо от получения уведомления. Мошенники также запугивают жертву для получения персональных данных, например номеров социального страхования и даты рождения, которые могут быть использованы для хищения персональных данных или иных мошеннических действий.

• Мошенническая схема с уведомлением о похоронах (Funeral Notification)

В рамках схемы funeral notification мошенники направляют электронные письма с темой «funeral notification» и сообщают о церемонии прощания, которая якобы будет проводиться в честь близкого человека получателя письма. Такие письма имеют видимость отправленных из действующих похоронных бюро и содержат инструкцию по переходу по ссылке для «получения более подробной информации». Затем адресат перенаправляется на сторонний сайт, с которого загружается malware, или вредоносное программное обеспечение. Программное обеспечение нарушает работу компьютера и позволяет мошенникам получить доступ к информации пользователя, которая затем может быть использована для мошеннических действий. Если вы получили такое письмо, немедленно удалите его.

• Лотерейные мошеннические схемы

К сожалению, многие лотереи проводятся мошенниками, которые стремятся получить персональную информацию или взломать ваш счет. Они рассказывают о разных призах и затем просят указать персональные данные или заплатить взнос за участие в розыгрыше. Зачастую такая схема направлена на пожилых людей, которые платят взнос и получают поддельные призовые чеки, а затем сдают эти чеки в банк. К сожалению, чеки отклоняются банком как фальшивые. А мошенники тем временем уже присвоили деньги, уплаченные в качестве взноса или налогов на призы. Помните, что действующие законно лотереи не требуют уплаты взноса.

• Мошенническая схема с подложной информацией об IRS

Помните об одной из самых хитроумных схем, существующих на сегодняшний день. Она называется «фишинг». Согласно данным

Федеральной налоговой службы (Internal Revenue Service, IRS), жертвами такой схемы стало не менее 20 000 налогоплательщиков. Представляясь служащими IRS, преступники требуют немедленной уплаты просроченных сумм налогов с помощью дебетовой карты или посредством безналичного перевода. Это позволяет им избежать поимки. Правонарушители могут даже знать последние четыре цифры номера социального страхования жертвы. Кроме того, по сообщениям пострадавших, после звонка мошенники направляют электронное письмо. Если вам неожиданно звонит сотрудник IRS, скорее всего, это мошенник. Иногда сложно определить, является ли звонок мошенническим, однако помните о том, что IRS, как правило, о любых действиях заранее уведомляет по почте. При этом сотрудники службы никогда не требуют немедленной уплаты средств во время разговора по телефону. Если вы сомневаетесь, перезвоните по номеру, который указан на веб-сайте IRS или в телефонном справочнике: 1-800-829-1040.

• Мошенническая схема с бесплатными субсидиями

Иногда мошенники предлагают бесплатные субсидии в печатной рекламе или по телефону. Например, бесплатные субсидии рекламируются в соответствующих разделах новостей и журналов. В рекламе сообщается, что читатели могут получить субсидию на оплату любых расходов, начиная от ремонта, расходов на образование и заканчивая неоплаченными счетами или предпринимательскими издержками. В других случаях люди сообщают о телефонных звонках от лиц, которые представляются сотрудниками государственных учреждений или организаций. Звонящие используют правдоподобно звучащие имена и обещают бесплатные субсидии на том основании, что вы вовремя уплатили налоги, или для их направления на погашение долга. Они всегда следуют одной схеме: поздравляют вас с тем, что вы имеете право на субсидию, а затем просят указать персональные или финансовые данные. Они подтверждают имя и фамилию, почтовый адрес, а затем просят указать наименование вашего банка, номер счета и код банка, чтобы списать средства за обработку заявления. Независимо от использованного метода схема одна: гарантированный прием вашего заявления и заверение в том, что вам не придется возвращать средства. Помните о том, что такие схемы незаконны. Мошенники стремятся всего лишь получить доступ к средствам на ваших счетах.

Советы как избежать мошенничества

- Если вам поступил неожиданный звонок, не нажимайте никакие клавиши и повесьте трубку. Если вы ответили на звонок, обязательно узнайте личность говорящего и компанию. Также возьмите номер телефона звонящего.
- Никогда не указывайте персональные или финансовые данные по телефону. Такими данными могут быть ваши имя и фамилия, дата рождения, номер социального страхования, адрес и номер Medicare.
- Свяжитесь со своей телефонной компанией, чтобы заблокировать номера robocall. Не следует платить за блокировку номеров robocall, поскольку высвечиваемые номера мошенников часто меняются.
- Установите межсетевой защитный экран и антивирусное/антишпионское программное обеспечение, чтобы защитить электронную почту от посягательств со стороны мошенников. Также регулярно обновляйте программное обеспечение.
- Пользуясь электронной почтой, не открывайте вложения в письмах от незнакомцев или подозрительных письмах. Иногда такие вложения содержат программы, которые позволяют мошенникам получить доступ к вашему компьютеру.
- Не указывайте в некрологах дату рождения, девичью фамилию или иные персональные данные умершего родственника, поскольку такая информация зачастую используется мошенниками.
- Не нажимайте и не открывайте файлы, которые пришли в незнакомых электронных письмах, чтобы избежать закачки нежелательных вредоносных программ.

- Не реагируйте на обещания гарантированных лотерейных призов в обмен на уплату взноса.
- Как правило, IRS сообщает о неоплаченных налогах, направляя сперва письмо по почте, а не по телефону или электронной почте.
- IRS никогда не просит совершить оплату безналичным путем или с использованием предоплаченной дебетовой карты.
- Позвоните в IRS по номеру 800-829-1040, если вы считаете, что у вас есть задолженность по налогам.
- Защитите свои персональные данные: храните их в надежном месте. Не храните важные номера счетов или данные в кошельках или смартфонах.
- Помните, что телефонные звонки могут быть обманчивыми. Для манипуляций с высвечиваемым на телефоне кодом района мошенники используют сложные технологии и устройства.
- Не платите деньги за «бесплатные» государственные субсидии. Если вас просят заплатить деньги для получения государственной субсидии, это мошенничество.
- Никогда не пользуйтесь электронным переводом средств и не платите за товар или услуги с помощью платежного поручения. Если предприятие осуществляет свою деятельность законно, оно принимает банковские карты или чеки. Это даст вам возможность остановить процесс платежа.
- Никогда не платите наличными и не выплачивайте полную сумму за ремонт до завершения работ. Подрядчик, осуществляющий деятельность на законных основаниях, примет небольшой авансовый платеж, начнет работы и не потребует выплату всей суммы заранее.

S.A.F.E.

Senior Anti-Fraud Education

Распознайте мошенническую схему до того, как станете ее жертвой

Если вы стали жертвой мошенников:

- Позвоните в местное отделение полиции или офис шерифа, чтобы заявить о преступлении.
- Предупредите соседей и местные организации о том, что в вашем районе работают мошенники.
- Обратитесь в подразделение по защите прав потребителей (Division of Consumer Protection) по адресу www.dos.ny.gov, прокуратуру штата (Attorney General's Office) по адресу www.ag.ny.gov и (или) местное учреждение по защите прав потребителей, чтобы они могли предупредить других людей и предложить свою помощь.
- Фиксируйте суммы утраченных средств на случай уголовного судопроизводства: эта информация необходима для вынесения решения о возмещении вам ущерба.

Division of Consumer Protection

Защита прав и информирование потребителей Нью-Йорка

Подразделение Департамента штата Нью-Йорк (New York Department of State)

1-800-697-1220 www.dos.ny.gov

@nysconsumer /nysconsumer

06/16-RU