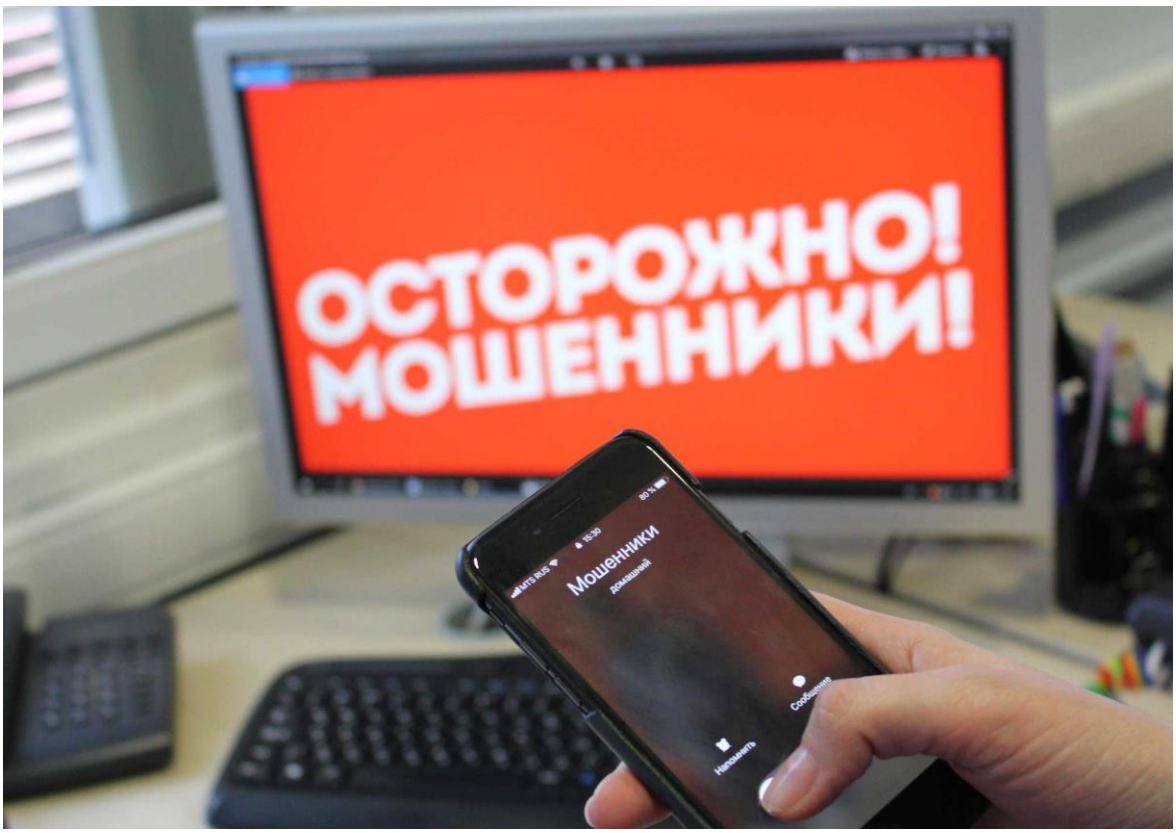
Прокуратура Михайловского района

«Правовое просвещение»

Защитите себя от интернет-мошенников: что нужно знать для того, чтобы не стать жертвой преступления



с. Поярково
24 ноября 2023 года

Современный мир - это мир новых технологий и научных открытий в IT-сфере. Все большее количество людей становится жертвами мошенников, особенно это обострилось во время пандемии COVID-19. Изощренными стали преступления в киберпространстве.

СПОСОБЫ СОВЕРШЕНИЯ МОШЕННИЧЕСТВА В БАНКОВСКОЙ СФЕРЕ

В банковской сфере мошенничество совершается различными способами, к основным из которых относятся:

- ***фишинг***, суть данного способа мошенничества заключается в том, что на электронную почту приходит письмо со ссылкой, по которой предлагается пройти для получения какого-либо блага. Эти действия совершаются чаще всего для того, чтобы получить доступ либо к банковским данным, если письмо приходит в банк, либо данным конкретного лица, сохраненным в персональном компьютере;

- ***фарминг,*** это более усовершенствованная форма фишинга. Опасность данного вида мошенничества заключается в скрытом перенаправлении потерпевшего на опасный IP-адрес. Суть его заключается в том, что изначально пользователь посещает какой-либо вредоносный сайт и скачивает там, например, нелицензированный файл или программу на персональный компьютер, после запуска которых происходит перенаправление на поддельные сайты, внешне совпадающие с заданными. Далее происходит следующее: пользователь на этих сайтах вводит свой логин и пароль, которые становятся достоянием злоумышленников, которые выводят денежные средства из обращения пользователя;

- ***кибермошенничество,*** заключается в том, что с помощью вредоносных программ происходит взлом компьютерных данных, хранящихся в различных организациях, и последующее использование этой информации в корыстных целях;

- к***ибервымогательство***, суть которого заключается в том, что с помощью вредоносных программ шифруются файлы, для восстановления которых требуется выплатить денежное вознаграждение в виде биткоинов или криптовалюты.

Говоря о киберпреступлениях в банковской сфере, следует упомянуть об атаках на информационные системы всех кредитных организаций. Данные преступные действия являются лидирующими в перечне всех киберпреступлений. Этот факт связывают в первую очередь со стремительным развитием IT-технологий, а во вторую - недостатком специалистов, способных противостоять таким действиям.

МОШЕННИЧЕСТВО ПОД ВИДОМ СОТРУДНИКОВ ФОНДА СОЦИАЛЬНОГО СТРАХОВАНИЯ

Фонд социального страхования РФ (ФСС) сообщил, что в последнее время участились случаи мошенничества с использованием Интернета и телефона.

Злоумышленники обещают некие социальные выплаты и пытаются получить доступ к банковским счетам и персональным данным граждан. В связи с этим важно помнить, что официальное название соцстраха - Фонд социального страхования РФ (ФСС РФ). В то время как мошенники иногда используют название «Федеральная служба социального страхования». Такого ведомства нет.

Официальные сайты ФСС имеют следующую структуру:

- http://fss.ru - центральный аппарат Фонда;

- https://r03.fss.ru - региональные отделения Фонда. Цифра перед fss.ru - это код региона отделения (например, r03 - Республика Бурятия, r50 - Московская область и т.д.).

Сайты с иной структурой адреса не являются официальными веб-страницами соцстраха и могут содержать недостоверную информацию.

Все электронные адреса сотрудников ФСС выглядят так: имя сотрудника + @ + fss.ru (например, m.morozov@fss.ru). Если вам на почту пришло письмо "от ФСС", но с адреса иной структуры, это однозначно мошенники.

Фонд не пользуется телефонными номерами типа 8 (800) XXX-XX-XX. Сотрудники ФСС никогда не попросят в телефонном разговоре продиктовать срок действия вашей банковской карты, контрольный код и/или СМС-код подтверждения.

Если вам поступило сообщение (по СМС или по электронной почте) якобы от ФСС с текстом вроде «Узнайте свой размер компенсации от государства», не перезванивайте по указанным номерам и тем более не сообщайте свои личные данные (реквизиты паспорта, банковской карты и пр.).

МОШЕННИЧЕСТВО ПОД ВИДОМ СОТРУДНИКОВ ФЕДЕРАЛЬНОЙ НАЛОГОВОЙ СЛУЖБЫ

Участились случаи интернет-мошенничества от имени ФНС России. Мошенники рассылают по электронной почте письма, в которых просят сообщить персональные данные с целью получения денежных средств налогоплательщика.

При этом инспекторы не вправе запрашивать информацию о компании по электронной почте. Поэтому письма от псевдоналоговиков нужно игнорировать. Не переходить по указанным в них ссылкам и не открывать вложения. Это может привести к заражению компьютера вредоносными программами. Получив такое письмо, нужно обратиться в территориальную инспекцию или на горячую линию и рассказать о случае мошенничества.

Вывод: ФНС России не отправляет информацию о задолженности или переплате налогоплательщика по электронной почте. Письма от имени налогового ведомства рассылают мошенники.

МОШЕННИЧЕСТВО ПОД ВИДОМ СОТРУДНИКОВ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Если раньше мошенники звонили и представлялись сотрудниками банков – теперь они все чаще звонят от имени сотрудников правоохранительных органов.

Как устроена схема мошенничества:

1) Вам звонит «сотрудник» банка или Центрального банка и спрашивает, оформляли ли Вы заявку на кредит. После того, как Вы отвечаете «нет», он говорит о том, что за Вас это сделали сотрудники банка, которые замешаны в мошеннической схеме.

2) Затем с Вами связывается человек якобы из МВД, прокуратуры или ФСБ и подтверждает слова и ФИО «сотрудника» банка. Вам могут прислать выписки из банка, удостоверения и другие документы с печатями, чтобы убедить Вас в том, что ситуация реальная.

3) В итоге Вам предлагают обратиться в отделение банка (или сразу в несколько банков) и подать новую заявку на кредит, чтобы предыдущая отменилась. При этом советуют «как можно меньше общаться» с сотрудниками банка в офисе.

4) Как только Вы получили деньги, Вас просят перевести их на новый «безопасный» счет. На самом деле это счет мошенников.

Как понять, что звонят мошенники, а не реальные сотрудники правоохранительных органов:

- мошенники часто ссылаются на закон о неразглашении. «Сотрудник» МВД, прокуратуры или ФСБ может сказать, что Вы не имеете права рассказывать об этом звонке, потому что он под тайной следствия.

Закон о неразглашении действительно существует, но работает по-другому: с Вас должны взять расписку, а не просто позвонить и запретить рассказывать о звонке.

- настоящие сотрудники никогда не спрашивают каким банком Вы пользуетесь. Если у Вас будут узнавать, на какую карту Вы получаете заработную плату, сколько на ней сейчас денег и когда Вы в последний раз выводили средства – это точно мошенники.

- мошенники постоянно просят Вас не вешать трубку. Это нужно, чтобы Вы не могли расслабиться и спокойно взглянуть на ситуацию. «Сотрудник» будет постоянно переадресовывать звонок на других людей: подставных консультантов банка, директора ближайшего банковского отделения или даже «вышестоящего сотрудника правоохранительного органа».

- «сотрудник» может начать угрожать ответственность перед законом.

<u>Что делать во время и после звонка?</u>

1. Ничего не говорите о себе, но узнайте, кто именно Вам звонит. Спросите имя, фамилию сотрудника, отделение, в котором он работает, его звание и должность.

2. Повесьте трубку.

3. Найдите в интернете официальный телефон отделения, которое Вам назвали, и перезвоните туда. Спросите, есть ли у них сотрудник, который Вас набирал, и о каком деле он говорил. Скорее всего Вам скажут, что это был мошенник.

Если Вы стали жертвой мошенников, сообщите об этом в правоохранительные органы, в первую очередь – в органы полиции.

ДЕЖУРНАЯ ЧАСТЬ МО МВД РОССИИ «МИХАЙЛОВСКИЙ»:
02, 8 (41637) 4-14-40

ДЕЖУРНАЯ ЧАСТЬ УМВД РФ ПО АМУРСКОЙ ОБЛАСТИ:
8 (4162) 59-41-02

ТЕЛЕФОН ПРОКУРАТУРЫ МИХАЙЛОВСКОГО РАЙОНА:
8 (41637) 4-18-58