Информация
по наиболее распространенным способам IT-хищений
в 2023-2024 годах

Проведенный анализ совершенных преступлений показал, что жертвами мошенников становятся люди различных профессий, в том числе работники банков, образовательных и медицинских учреждений, газовой и нефтяной промышленности, государственных и муниципальных органов, индивидуальные предприниматели, пенсионеры.

Возраст лиц, ставших жертвами мошенников разнообразен. В основном это работоспособное население в возрасте от 18 до 60 лет, имеющих в основном среднее (средне-специальное) образование и осведомленные об основных способах совершения мошенничеств.

В текущем году, наряду с распространенными видами преступлений, появились новые способы совершения мошенничеств, такие как:

1. Звонки от имени сотрудников «службы безопасности Банков» и сотрудников силовых структур (МВД, ФСБ, прокуратуры) или «Госуслуг» с использованием Sip- телефонии и программ подменны абонентского номера, (с использованием мессенджеров «Ватсап», «Телеграмм», «Вайбер» когда на телефоне потерпевшего определяется официальный номер Банка, либо территориального органа МВД России, ФСБ и прокуратуры. И под предлогом:

- пресечения сомнительных операций по счетам, оформления кредитов неизвестным лицом, либо под предлогом оказания помощи в установлении и поиске преступников среди сотрудников банков, убеждают оформить «зеркальный» кредит, а затем внести денежные средства на «безопасные ячейки», либо на абонентские номера, подконтрольные неизвестным лицам;
- требования сообщить номер банковской карты, CVC-код, а затем код в СМС сообщении, необходимый для удаленного управления и хищения денежных средств со счетов граждан.

1.1. Одним из подвидов мошенничества является тот факт, когда устанавливаются те же соединения, но «мошенники» представляются сотрудниками компаний сотовой связи и сообщают «ложные сведения» о необходимости продлить договор предоставления услуг связи.

На следующей стадии мошенничества злоумышленник убеждает сообщить код, поступающий в СМС сообщениях, который необходим для входа в личные кабинеты потерпевших Банков, «Госуслуг» и в дальнейшем мошенники как правило отключают абонентский номер потерпевшего от личных кабинетов Банков клиентом которого от является или «Госуслуг», что позволяет совершать им в дальнейшем противоправные действия в тайне от потерпевшего.

1.1.2. Мошенники могу проставляться от имени представителей силовых структур и сообщать ложные сведения о подозрительных операциях на счетах и оформления переводов денежных средств на Украину с целью поддержки «ВСУ», убеждая своих жертв совершить действия, указанные в п.1-1.1.

Регистрируются случаи, когда мошенники убеждают своих «потенциальных жертв» приобрети новые мобильные устройства с функцией «Мир пэй», и подключить неизвестные счета для осуществления денежных переводов по системе «Мир пэй» через банкоматы.

1.2. Те же действия в п.1.1.-1.2., но мошенники убеждают своих жертв установить на гаджетах программы удаленного доступа, которые позволяют полностью контролировать им действия потерпевшего с установленными на мобильном устройстве приложениями и видеть в режиме он-лайн информацию, необходимую для беспрепятственного подключения к ним (приложениям), что в свою очередь ведет к причинению материального ущерба пользователю.

Мошенники, представляясь представителями госорганов или силовых структур с целью войти в доверие к своей «жертве», могут демонстрировать фото и видеоизображений поддельных служебных удостоверений структур, чьим имением они представляются.

1.3. Аферисты совершают звонки с предложением пройти флюорографию за счет ОМС, либо продлить в телефонном режиме полис ОМС. Далее предлагают выбрать клинику и якобы для подтверждения записи просят назвать код из СМС.

На самом деле эта информация дает им возможность получить доступ к Госуслугам или подтвердить списание денежных средств со счета.

Необходимо донести до сознания населения округа, что видов и способов телефонного мошенничества множество и ограничиться перечисленными нельзя, так как с развитием современного общества и его цифровизации во всех областях деятельности, мошенники используя возможности телефонии, правовые и технические пробелы при обороте электронных денежных средств создают новые предлоги и способы чтобы войти в доверие к пользователям и получить необходимую информацию, либо совершить алгоритм действий, направленные на хищение имущества путем обмана и злоупотребления доверием.

Действенным способом противостоять таким преступлениям является:

1. Прекратить телефонное соединение (в том числе через мессенджеры) с неизвестных номеров с неизвестными лицами, которые представляются сотрудниками госорганов, силовых структур, банковскими работниками, которые сообщают информацию о совершении подозрительных операциях по счетам и необходимости сообщить коды в СМС-сообщениях, выполнить определенные действия по оформлению кредитов и перечислению на

неизвестные номера телефонов, счетов, банковских карт, электронных кошельков.

2. Не сообщайте незнакомцам свои персональные данные, просто кладите трубку!

3. При любых сомнениях самостоятельно набрать номер телефона горячей линии Банка, клиентом которого являетесь.

4. Помнить, что сотрудники Банков, силовых структур, операторов сотовой связи и др., в телефонном режиме (мессенджеры) не требуют сообщать коды в смс-сообщениях при совершении банковских операций, а так же принять участие в какой-либо «специальной операции» по изобличению мошенников в той или иной организации.

5. Установить на мобильный устройствах программу антивируса и автоматического определителя номера.

6. Установить двухфакторную систему аутентификации в мобильных приложениях Банка, «Госуслуг» клиентом которого являетесь и мессенджерах, установленных на гаджетах.

7. Категорически не устанавливать на мобильные устройства программы удаленного доступа как при общении с неизвестными лицами, так и с лицами, вызывающих сомнение.

8. Не предпринимать попытки оформить он-лайн заявки на оформление кредитов, займов для предотвращения оформления кредитов неизвестными на ваше имя, а обратиться на горячую линию или ближайший офис Банка.

Следующий распространенный способ хищения с использованием it-технологий применяется мошенниками при общении в Интернете, при общении, покупке-продажи:

Под предлогом продажи либо покупки товаров на сайтах бесплатных объявлений «Авито», «Юла», а также в социальных сетях «В контакте», «Одноклассники», «Инстаграмм» мошенники убеждают пройти по «безопасной ссылке», после чего денежные средства перечисляются на подконтрольные счета злоумышленников.

Так же, мошенники используют возможность внесения предоплаты за товар и дальнейшим внесением в черный список.

Важно помнить, что перед совершением сделку купли-продажи не следует переходить по ссылкам от неизвестных лиц и не вносить предоплату.

На известных торговых интернет-площадках следует придерживаться правил «безопасной сделки».

При использовании сервиса «БлаБлаКар» мошенники также используют схему по предоплате поездки в чате сервиса или в мессенджере. Необходимо помнить, что поездки с водителем- попутчиком оплачиваются только наличными и только во время поездки. Так же не следует переходить по ссылкам, полученных от якобы водителей сервиса.

Переводить деньги заранее или просить предоплату запрещено. Билеты на автобусы можно купить он-лайн, оплатив банковской картой. Обратите

внимание на то, что билеты на проезд нужно приобретать на страницах https://www.Blablacar.ru либо https://Busfor.ru, или через официальные приложения «Blablacar» и «BusFor» для перевода денег водителю в счет оплаты за поездку необходимо использовать официальные сайты или специальные мобильные приложения Банков, даже не смотря на возможную комиссию за денежный перевод, а лучше всего передавать наличные деньги в руки водителю. Ни в коем случает нельзя переводить деньги по предоставляемым водителем ссылкам;

Следующий распространенный способ интернет мошенничеств связан с перечислением денежных средств неизвестным лицам под предлогом участия в инвестиционных проектах на незарегистрированные Центральным Банком России «инвестиционных площадках».

Объявления с предложениями принять участия в инвестировании размещаются злоумышленниками в социальных сетях, таких как «В контакте», «Одноклассники», «Инстаграмм», «Тик-Ток», на видеохостингах «Ютуб» и т.д.

Необходимо знать, что инвестиционными проектами в Российской Федерации уполномочены заниматься исключительно банки (Сбербанк, Газпром банк, Тинькоф, Альфа-Банк и т.д.).

Перечень лицензированных банков размещен на официальном сайте Центрального Банка РФ, там же и размещены правила, порядок и условия участия в инвестиционных проектах.

Чтобы избежать негативных материальных и моральных последствий и не стать жертвой мошенника, необходимо помнить, что:

Сотрудники служб безопасности банков, правовых и силовых структур, Госуслуг и операторы сотовой связи в телефонном режиме:

- Не интересуются кодами, поступающими в СМС-сообщениях при совершении финансовых операций в «Личном кабинете» клиента;
- Не просят «клиентов» перевести денежные средства на резервные счета;
- Не убеждают «клиентов» в необходимости оформления зеркальных кредитов с целью предотвращения «оформления кредита» на имя клиента неустановленными лицами;
- Не интересуются наличием банковских карт сторонних банков и суммой денежных средств, находящихся на счетах клиента;
- Не требуют перечисления денежных средств за «оформление, страхование, услуги курьера» при оформлении онлайн кредитов;

Сотрудники правоохранительных органов при общении по телефону:

- Не сообщают о каких-либо мероприятиях, проводимых МВД, ФСБ и другими силовыми структурами, направленных на изобличение мошенников среди банковских служащих, и вообще каких-либо в принципе;
- Не требуют от «клиентов Банка» выполнять какие-либо инструкции якобы сотрудников служб безопасности банков;

- Не предупреждают об уголовной ответственности за невыполнение требований, поступающих в телефонном режиме от якобы сотрудников Банков.

При поступлении на телефон входящего звонка с абонентских номеров силовых структур (МВД, ФСБ, ФССП и т.п.), которые размещены на официальных сайтах, необходимо прекратить звонок и перезвонить на указанные номера самостоятельно. Важно дозвониться самому, а не ждать, когда Вам перезвонят.

При поиске объявлений на сайтах «Юла», «Авито», «Дром», «Авто.ру» и др. обязательно ознакомиться с правилами и условиями сайта, с правилами оплаты и предоплаты за покупку товара или за использование услуг доставки товара курьерской службой. Существуют правила безопасных сделок, а именно:

- необходимо «общаться» во внутреннем чате сайта и не уходить в другие мессенджеры;
- хранить в тайне свою переписку, паспортные данные и код с карты;
- не отправлять предоплату, если не уверены в порядочности продавца;
- никому не сообщать коды из смс и пуш-уведомлений;
- игнорировать ссылки на оплату, которые присылает собеседник.

При оформлении покупок на Интернет-сайтах, осуществлять мониторинг сети «Интернет» на предмет наличия отрицательных отзывов, а также даты регистрации сайта (если сайт или страничка в соцсетях создана недавно и отсутствуют отзывы, или имеющиеся отзывы носят отрицательный характер, то вероятнее всего это мошенник). Кроме того, необходимо обращать внимание на то, что у любого продавца имеется юридический адрес или адрес фактического нахождения магазина или склада. Информацию с указанием адресов магазинов можно проверить в сети интернет, например, на сервисах Яндекс или на сайте 2ГИС.

Осуществлять покупку билетов на различный вид транспорта необходимо исключительно с помощью официальных приложений, размещенных в «Appel Store» и «Play Market», а также на официальных сайтах авиа и ж/д компаний. Важно помнить о нахождении в Интернете сайтов-двойников, которые могут иметь наименования, созвучные с официальными сайтами (нужно внимательно изучить весть сайт, перезвонить на телефон технической поддержки, уточнить у оператора всю информацию о предоставляемых услугах).

В настоящее время предлогов для того, чтобы мошенникам войти в доверие к гражданам, существует множество.

Главное помнить, что нельзя передавать свои персональные данные незнакомым людям в телефонном режиме и уточнять всю поступившую информацию самостоятельно у официальных источников, обратившись на горячую линию организации.

УУР УМВД России по ХМАО-Югре