ОБЗОР МОШЕННИЧЕСКИХ СХЕМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МОБИЛЬНОЙ СВЯЗИ И СЕТИ «ИНТЕРНЕТ»

ЮРИЙ НОГИНОВ

Директор ОАО «РЖД» – начальник Департамента управления информационной безопасностью

Уважаемые коллеги!

В связи с тем, что по-прежнему отмечается высокая активность мошеннической деятельности с применением различных технологий, в том числе методов социальной инженерии и искусственного интеллекта, направленной на получение доступа к информационной инфраструктуре ОАО «РЖД», вовлечение работников и их родственников в противоправную деятельность либо завладение их денежными средствами, Департамент управления информационной безопасностью при активной поддержке Департамента корпоративных коммуникаций продолжает работу по распространению информационно-просветительских материалов для противодействия мошенникам и защиты интересов не только компании, но и её работников.

В 2024 году была издана брошюра «Методы информационно-психологического воздействия с использованием информационно-телекоммуникационных технологий и рекомендации по противодействию им» (№ ИСХ-777/ЦИБ от 7 июня 2024 г.), в которой подробно рассматривались многочисленные варианты применения методов социальной инженерии, рекомендации и алгоритмы действий для защиты от мошенников.

Однако за прошедшее время значительно увеличился охват процессами цифровизации сфер жизнедеятельности общества, что привело к появлению новых рисков и формированию условий для внедрения новых мошеннических схем.

В данной брошюре нами сведены воедино наиболее часто используемые мошенниками схемы обмана граждан, которые реализуются с использованием современных телекоммуникационных технологий, включая мобильную связь и сеть «Интернет». Во избежание причинения имущественного и иного вреда, а также для исключения негативного воздействия на производственные процессы компании брошюра рекомендуется к изучению широкому кругу граждан – работников ОАО «РЖД», их родственников и знакомых.

Также напоминаю, что в случаях возникновения сомнений относительно поступивших звонков и сообщений работники компании в круглосуточном режиме могут обращаться на Горячую линию по телефону 8 (800) 775-76-77.

Содержание

Введение 5

1. Мошенничество через телефонные звонки (вишинг) 7

1.1. Тема звонка: из государственных органов 7

1.2. Тема звонка: обучение 9

1.3. Тема звонка: здравоохранение 9

1.4. Тема звонка: покупки 10

1.5. Тема звонка: финансы 11

1.6. Тема звонка: телефонная связь 12

1.7. Тема звонка: жилищное хозяйство 13

1.8. Иные звонки 13

2. Распространение вредоносных ссылок на мошеннические интернет-ресурсы (фишинг и смишинг) 14

2.1. Ссылки на поддельные сайты государственных органов 14

2.2. Ссылки на поддельные сайты, связанные с обучением 15

2.3. Ссылки на поддельные сайты, связанные со здравоохранением 15

2.4. Ссылки на поддельные сайты магазинов 16

2.5. Ссылки на поддельные финансовые сайты 18

2.6. Ссылки на поддельные сайты телефонной связи 20

2.7. Ссылки на поддельные сайты жилищного хозяйства 20

2.8. Ссылки на иные поддельные сайты 21

3. Обман при продаже товаров и услуг в сети «Интернет» (скамминг) 23

4. Внедрение вредоносного программного обеспечения (фарминг) 25

4.1. Вредоносное программное обеспечение в здравоохранении 25

4.2. Вредоносное программное обеспечение в сфере финансов 26

5. Иные схемы мошенничества 27

Заключение. Правила безопасного поведения 31

Введение

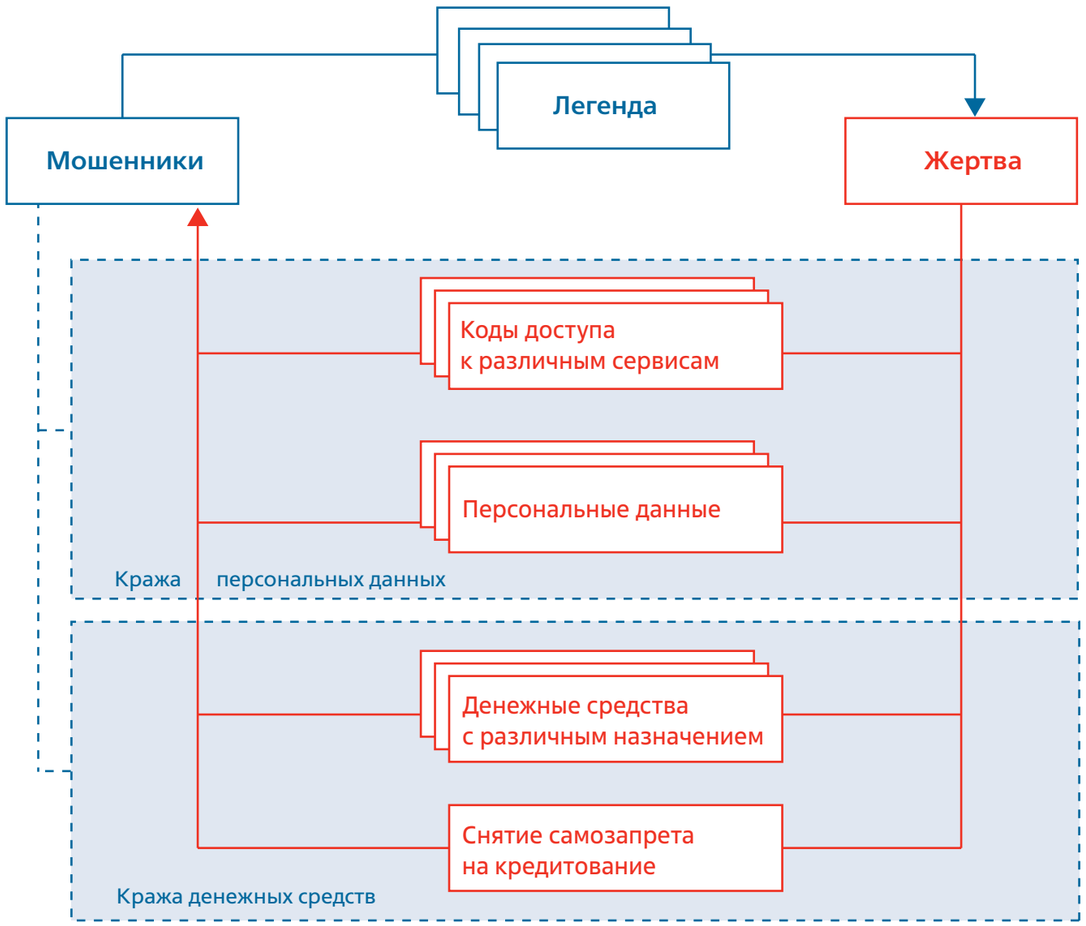
Мошенничество с использованием средств вычислительной техники может быть реализовано с помощью:

- методов социальной инженерии с использованием информационных технологий,
- атак с использованием технических средств.

Способы воздействия на жертву с применением методов социальной инженерии с использованием информационных технологий включают:

- мошенничество через телефонные звонки (вишинг),
- распространение вредоносных ссылок на мошеннические интернет-ресурсы (фишинг) и его подвид – распространение вредоносных ссылок на мошеннические интернет-ресурсы с помощью смс-сообщений (смишинг),
- обман при продаже товаров или услуг в сети «Интернет» (скамминг).

Методы социальной инженерии могут быть реализованы через любые каналы коммуникации – телефон, электронная почта, мессенджер, социальные сети, смс-сообщения и пр.



Для реализации атак с использованием технических средств применяется внедрение вредоносного программного обеспечения (фарминг).

Схемы с данным способом могут включать в себя элементы социальной инженерии и, как правило, совмещены с вишингом и фишингом, при этом принципиальным отличием фарминга от фишинга является использование вредоносного программного обеспечения.

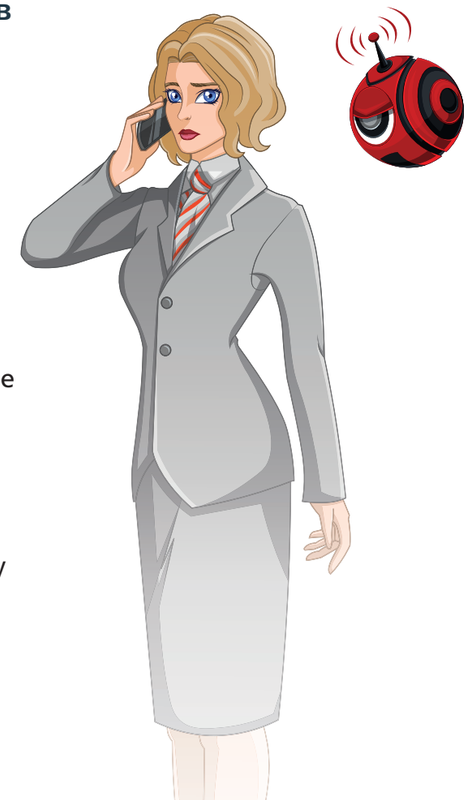
Злоумышленники постоянно меняют методы воздействия и свои легенды, но цели воздействия и схема его реализации остаются неизменными.

И если кража денежных средств не вызывает сомнений в ее конечных целях, то в отношении кражи персональных данных гражданина нередко можно услышать фразу: «Да кому нужны мои данные!». Кража денежных средств совершается мошенниками либо с целью личного незаконного обогащения, либо с целью финансирования Вооруженных сил Украины, а также экстремисткой и террористической деятельности запрещенных в России организаций.

Что касается персональных данных, то их кража осуществляется с целью последующего совершения финансовых махинаций от лица жертвы или ее склонения к совершению противоправных действий, направленных на реализацию преступных замыслов как по отношению к Российской Федерации, так и к отдельным ее гражданам.

1. Мошенничество через телефонные звонки (вишинг)

1.1. Тема звонка: из государственных органов



Представляясь сотрудниками силовой или любой другой государственной структуры, мошенники стремятся выбить у граждан «почву из-под ног» и заставить их нервничать. А чем больше нервничает человек, тем выше вероятность, что он не сможет думать рационально и легче примет на веру ложь злоумышленников. Мошенники используют подменные номера, выдают себя за сотрудников государственных органов. Для убедительности через мессенджеры демонстрируют поддельные «служебные удостоверения», копии «приказов», фальшивые повестки с вызовом для дачи показаний и другие фиктивные документы. Нередко злоумышленник просит включить демонстрацию экрана, предлагая свою помощь для ускорения процесса. Он подает заявку на восстановление доступа к личному кабинету на портале «Госуслуги» и считывает с экрана код подтверждения. Завершив разговор, мошенник с помощью полученных данных взламывает личную страницу на портале и ограничивает настоящему владельцу доступ к ней.

ЛЕГЕНДА «ФСБ РОССИИ»

Представляясь сотрудниками ФСБ России, злоумышленники убеждают жертву перевести деньги на так называемые «безопасные счета» или передать их курьеру под предлогом защиты средств от кражи или участия в оперативных мероприятиях. В некоторых случаях вымогательство происходит под предлогом «закрытия уголовных дел», якобы возбужденных против жертв или их близких.

Граждан просят сохранять конфиденциальность, угрожая уголовной ответственностью за разглашение государственной тайны или отказ от сотрудничества.

ЛЕГЕНДА «МВД РОССИИ»

Представляясь сотрудниками полиции, злоумышленники узнают у жертвы пароль для входа в личный кабинет портала «Госуслуги» или код доступа из смс-сообщения. Персональные данные из личного кабинета портала «Госуслуги» пострадавшего будут использоваться в дальнейшем при реализации других схем мошенничества, например, для получения кредита.

ЛЕГЕНДА «ФЕДЕРАЛЬНАЯ СЛУЖБА СУДЕБНЫХ ПРИСТАВОВ»

Мошенники, представляясь сотрудниками Федеральной службы судебных приставов, сообщают о наличии некоего исполнительного производства, настаивая при этом на немедленном погашении долга.

У злоумышленников могут быть персональные данные потенциальной жертвы, а сама атака на нее может занять от нескольких часов до нескольких дней. Для усиления воздействия не исключено использование злоумышленниками как голосовых, так и видеодипфейков.

ЛЕГЕНДА «ФНС РОССИИ»

Злоумышленники, представляясь сотрудниками налоговых органов, рассказывают о неуплаченных налогах, задолженности, непредставленных документах, необходимости подать декларацию или другие документы. В диалоге мошенники угрожают крупными штрафами и предлагают «помощь» с якобы электронным запросом работодателю, чтобы выгрузить сведения, записать на прием в налоговый орган. Для этого необходимо назвать код из смс-сообщения. Фактически гражданин передает мошенникам код с портала «Госуслуги», подтверждающий изменение пароля.

Еще один вариант мошенничества. Мошенники завлекают доверчивых граждан обещаниями оформить налоговый вычет всего за один день через «аккредитованного партнера ФНС». Внешне все выглядит убедительно: звонок от уверенного собеседника, ссылки на несуществующие лицензии, обещания собрать все необходимые справки самостоятельно и даже гарантия, что деньги будут списаны только после одобрения вычета. Для оформления вычета мошенники запрашивают паспортные данные, ИНН и сведения о расходах.

Самым опасным этапом мошеннической схемы становится предложение оформить «виртуальную карту с усиленной защитой» и перевести на нее все имеющиеся средства. На самом деле никакой дополнительной защиты такие карты не обеспечивают – мошенники получают их реквизиты и затем снимают все деньги.

ЛЕГЕНДА «РОСКОМНАДЗОР»

Мошенники звонят гражданам через мессенджеры, представляются сотрудниками Роскомнадзора и сообщают, что их личный кабинет на портале «Госуслуги» взломали. Для разблокировки требуется номер СНИЛС. Получив его, мошенники могут использовать СНИЛС для оформления кредитов, незаконного получения выплат или доступа к другим учетным записям жертвы.

Также жители регионов России стали получать мошеннические письма якобы от имени «Роскомнадзора» с информацией «о разъединении входящего вызова в связи с подозрением на мошенничество» и сообщением, что«если Вам поступал звонок, в котором запрашивали персональные данные, перезвоните по указанному в письме номеру телефона горячей линии». Такие сообщения отправляются длятого, чтобы заставить гражданина самостоятельно позвонить мошенникам. Если человек перезванивает на указанный номер, то мошенники под видом уточнения и подтверждения информации пытаются получить его персональные данные, код из смс-сообщения для дальнейшего доступа к личному кабинету на портале «Госуслуги».

1.2. Тема звонка: обучение

ЛЕГЕНДА «МИНПРОСВЕЩЕНИЕ»

Мошенники обзванивают выпускников и их родителей под видом сотрудников Минпросвещения. По телефону они убеждают зарегистрироваться на «портале сдачи ЕГЭ». Под предлогом «необходимости срочной авторизации» они просят продиктовать код из смс-сообщения для подтверждения личности. Так злоумышленники получают доступ к личным кабинетам, электронным дневникам, порталу «Госуслуги» и банковским приложениям.

ЛЕГЕНДА «ШКОЛА»

Мошенники звонят выпускникам и их родителям, выдавая себя за сотрудников ведомств, школ или экзаменационных комиссий, предлагают зарегистрироваться для участия в итоговой аттестации и просят продиктовать код из смс-сообщения. Таким образом, злоумышленники получают доступ к личному кабинету в электронном дневнике и порталу «Госуслуги».

Еще одной из распространенных схем является звонок от «классного руководителя» или «директора школы» с сообщением о некоем срочном инциденте. Злоумышленники могут сообщить ребенку, что его родители попали в больницу или в полицию, и потребовать срочно передать деньги «курьеру» или перевести средства на указанный счет для оказания помощи. Используя стрессовую ситуацию и создавая панику, мошенники добиваются от детей немедленного выполнения своих требований.

Кроме того, злоумышленники могут убеждать, что школа проводит специальную акцию или сбор средств на нужды класса, и просят детей передать деньги «представителю школы», который придет к ним домой, или отправить «взнос» через перевод.

1.3. Тема звонка: здравоохранение

ЛЕГЕНДА «ПОЛИКЛИНИКА»

Злоумышленники, представляясь работниками поликлиник, как действительно существующих, таки вымышленных, могут предложить записаться на диспансеризацию, флюорографию, а также к кардиологу, эндокринологу и другим дефицитным специалистам. Для того, чтобы подтвердить запись, они предлагают сверить СНИЛС или ввести код из сообщения. Указанные действия зачастую приводят к потере личного кабинета на портале «Госуслуги». После этого мошенники получают доступ ко всем личным данным жертв и могут использовать их в своих целях.

Еще одна распространенная схема – мошенники звонят под видом сотрудников поликлиники и заявляют, что бумажную медицинскую карту скоро аннулируют в рамках реновации здравоохранения. Для того чтобы человек не потерял историю лечения и не остался без доступа к врачам, злоумышленники настаивают на срочном оформлении электронной медицинской карты. Все данные они обещают перенести в раздел «Здоровье» на портале «Госуслуги» и выдать пациенту новый номер карты. Для этого просят назвать СНИЛС и код из смс-сообщения.

ЛЕГЕНДА «СТРАХОВАЯ КОМПАНИЯ»

Мошенники представляются сотрудниками страховых компаний и сообщают ложную информацию о необходимости замены полиса ОМС. Просят продиктовать код, якобы подтверждающий, что лицо стоит в очереди на замену.
После передачи кода из смс-сообщения с жертвой связываются лжесотрудники Финмониторинга и правоохранительных органов, которые заявляют о взломе личного кабинета на портале «Госуслуги», украденных персональных данных и зафиксированных попытках снятия денег и получения кредитов. Далее предлагается перевести денежные средства на безопасный счет. На этом мошенники не останавливаются и сообщают, что необходимо заплатить налоги с суммы банковских операций, поскольку на действия жертвы обратила внимание «налоговая служба».

Если человек попался на мошенническую схему, то его могут попробовать обмануть второй раз. Мошенники производят второй звонок и сообщают жертве о взломе ее аккаунта, предлагая связаться со службой поддержки по заранее заготовленному номеру. В состоянии аффекта человек звонит по указанному номеру, где ему советуют связаться с Росфинмониторингом, чтобы якобы сохранить свои деньги, где жертву просят заполнить заявление и прикрепить к нему фотографии банковских карт.

После этого происходит кража денежных средств.

1.4. Тема звонка: покупки

ЛЕГЕНДА «МАРКЕТПЛЕЙС»

Представляясь сотрудниками маркетплейсов, мошенники «предупреждают» человека о том, что срок бесплатного хранения его заказа истек, предлагают продлить его, назвав код из смс-сообщения. Затем злоумышленники используют код, чтобы получить доступ к личному кабинету жертвы на портале «Госуслуги» или к ее банковским данным для кражи средств.

Или мошенники предлагают клиентам маркетплейсам начислить кешбэк или бонусы за задержку доставки. Под этим предлогом они просят назвать им платежные данные или коды из смс-сообщений, которые затем используют для хищения товара или денег.

Также злоумышленники учли новости о возможном возвращении западных брендов и стали звонить жертвам от имени европейских и американских компаний. Россиянам предлагают восстановить бонусные карты и для восстановления просят продиктовать коды из смс-сообщений. На самом деле так мошенники получают доступ к личным данным жертвы, что помогает им украсть деньги и оформить кредиты на потерпевших.

Злоумышленники, используя находящиеся в маркетплейсах профили пользователей, звонят гражданам от лица работников пунктов выдачи маркетплейсов и предлагают доставить на дом ранее заказанные товары.

При этом человека просят назвать СНИЛС, ИНН или код из смс-сообщения от портала «Госуслуги». После звонит якобы представитель правоохранительных органов и сообщает о взломе личного кабинета на портале «Госуслуги». Он начинает убеждать человека, что его средства в опасности и единственным выходом из ситуации остается перевод на специальный счет или же передача наличных в руки сотрудников правоохранительных органов.

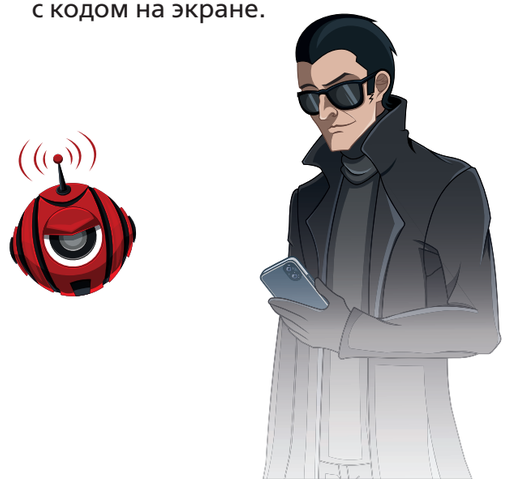
ЛЕГЕНДА «ПОЧТА РОССИИ»

«Оператор» «Почты России» под предлогом отправки письма просит сообщить код-подтверждение из полученного смс-сообщения.
На самом деле это может быть пароль для восстановления доступа к личному кабинету на портале «Госуслуги».
Получив возможность доступа в личный кабинет, мошенники различными манипуляциями вынуждают жертву перевести имеющиеся у нее средства на «безопасный счет».

Также телефонные мошенники сообщают о доставке посылки из-за рубежа, за которую нужно оплатить таможенный сбор. Для того, чтобы отказаться от посылки, которую человек не заказывал, мошенники просят назвать код из смс-сообщения. По их словам, это нужно, чтобы якобы подписать официальный отказ в базах почты. Цель мошеннической схемы – получить доступ к банковскому мобильному приложению или к личному кабинету на портале «Госуслуги».

ЛЕГЕНДА «ПОКУПАТЕЛЬ»

Еще мошенники разработали схему, в которой под ударом оказались частные лица, которые размещают объявления о продаже своих вещей в сети «Интернет». Злоумышленники звонят им под видом покупателей, говорят, что хотят проверить наличие и качество товара, предлагают перейти для общения в мессенджер и связаться с помощью видеозвонка, а затем включить функцию демонстрации экрана. В этот момент соучастник мошенника запрашивает доступ к смене номера в банковском приложении жертвы, а находящийся на связи злоумышленник видит смс-сообщение с кодом на экране.



1.5. Тема звонка: финансы

ЛЕГЕНДА «БАНК»

Гражданину звонят и убеждают, что его деньги в опасности, однако вместо перевода просят приобрести золото в виде слитков или инвестиционных монет. Затем жертве предлагают либо передать золото курьеру, либо продать в другом банке и перевести деньги на «надежный счет».

В другом варианте мошенники обращаются к теме выплат по ипотеке, к которым люди обычно относятся очень ответственно. Злоумышленники звонят гражданину и от лица сотрудника банка уверяют, что у клиента возникла просрочка, и предлагают ему урегулировать проблему. Для этого просят сообщить данные СНИЛС и коды из смс-сообщений. При этом мошенники специально обращают внимание собеседника на то, что не имеют права запрашивать персональную информацию, поэтому высылают код в смс-сообщении для подтверждения, который просят озвучить. Если ипотеки у человека нет, то звонок прерывается.

Также мошенники имитируют звонки от микрофинансовых организаций – «представитель» сообщает, что на жертву оформлен заем, но есть способ избежать исполнения обязательств, если связаться с представителем Центробанка.

ЛЕГЕНДА «САМОЗАПРЕТ НА КРЕДИТЫ»

Мошенники разработали несколько вариантов, для того чтобы убедить россиян снять самозапрет на предоставление кредитов. В одном случае мошенники, выдавая себя за сотрудников налоговой службы, сообщают о мнимой задолженности или ошибке в кредитной истории, требуя срочно снять самозапрет на кредитование, угрожая штрафами. Злоумышленники настаивают, что снять запрет необходимо как можно быстрее, чтобы не пришлось заплатить штраф.

В другом случае мошенники, представляясь сотрудниками банка, сообщают о якобы подозрительных операциях и требуют срочно снять самозапрет на кредитование для якобы защиты своих средств.

Еще злоумышленники могут представляться сотрудниками различных органов, якобы оказывающих поддержку от государства, и утверждать, что из-за самозапрета человек не может получить одобрение на льготный кредит, субсидию или выплату от государства.

1.6. Тема звонка: телефонная связь

ЛЕГЕНДА «РОСТЕЛЕКОМ»

Мошенники начали использовать вариант с якобы заменой кодов номеров домашних телефонов. В ходе телефонного разговора мошенники убеждают в том, что в настоящее время происходит замена кода городских телефонов с 499 на 495. Под предлогом скидок пенсионерам при установке оборудования они выманивают у жертвы паспортные данные якобы для уточнения возраста. Также они уговаривают жертву произнести фразу «Не возражаю против замены номера», после чего разговор прекращается. На следующий день злоумышленники, под видом сотрудников правоохранительных органов, сообщают, что жертва пытается осуществить незаконный перевод, который заблокирован, и просят помочь разоблачить недобросовестных работников кредитно-финансового учреждения, для этого предлагают снять денежные средства со своих счетов и передать доверенному курьеру.

ЛЕГЕНДА «ОПЕРАТОР МОБИЛЬНОЙ СВЯЗИ»

Злоумышленники звонят потенциальной жертве, представляются сотрудниками операторов мобильной связи и, ссылаясь на необходимость продлить договор сотовой связи или получить новогодние бонусы, пытаются получить доступ в личный кабинет абонента и выманить коды доступа к различным сервисам, включая мобильный банкинг. Когда во время такого телефонного разговора человек получает смс-сообщение с кодом для входа в онлайн-кабинет своего сотового оператора, мошенники просят озвучить им этот код. Кроме того, они просят передать код из смс-сообщений для доступа к личному кабинету на портале «Госуслуги». Подобные действия позволят злоумышленникам оформить электронную сим-карту для дальнейшего управления сервисами различных банков от имени обманутого.

Опасность состоит в том, что в случае «удачной атаки» злоумышленник получает доступ к основному средству аутентификации клиента во всех сервисах, включая банковские приложения или сервисы государственных услуг.

Еще мошенники звонят гражданам, представляясь инженерами оператора связи, и под предлогом «проверки телефонной линии» просят набрать комбинации вроде #90, #09 или другие. Нажатие этих цифр передает управление сим-картой злоумышленникам, что позволяет им совершать звонки за чужой счет и получать доступ к банковским приложениям.

1.7. Тема звонка: жилищное хозяйство

ЛЕГЕНДА «ПРИЕМНАЯ МЭРИИ»

В Москве мошенники звонят и, представляясь приемной мэра Москвы, назначают видеоконференцию с Сергеем Собяниным с целью разговорить человека и «продавить» его на выдачу конфиденциальных сведений. На этих видеоконференциях создают декорации встречи с мэром, даже присутствует человек, напоминающий издалека Собянина. Применяются нейросети, манипулятивные ходы и убедительные фразы. Злоумышленники рассчитывают, что жертвы лично никогда не встречались и не общались с мэром города, поэтому будут под большим впечатлением и доверятся. Цель – загнать человека в стресс: предлагается ситуация, когда нужно экстренно, буквально во время разговора, принять решение – назвать пароли, коды, перевести деньги.
При этом звучат юридические термины, статьи законов. В результате такой психологической атаки человек может добровольно передать мошенникам данные банковских счетов или лично отправить деньги.

ЛЕГЕНДА «УПРАВЛЯЮЩАЯ КОМПАНИЯ»

Злоумышленники звонят гражданам от имени управляющей компании и информируют их о скорой замене двери подъезда. Затем мошенники уточняют, сколько необходимо изготовить электронных ключей, как и когда удобно их получить, нужен ли запасной комплект. Успокоив, таким образом, бдительность гражданина, мошенники сообщают, что теперь у каждой квартиры будет свой код от домофона, так как общий код противоречит политике безопасности, и каждый код нужно прописать в домофоне. После обсуждения деталей звонящие просят продиктовать присланный человеку на телефон якобы персональный код для домофона, который на самом деле может являться способом удаленной оплаты, кражи денежных средств или доступом к персональным данным гражданина.

1.8. Иные звонки

Злоумышленники используют варианты с видеозвонками. Пользователю поступает видеозвонок на телефон, через WhatsApp или Telegram. Злоумышленник делает снимок экрана, создает из него кружок без звука. Затем мошенник создает новый аккаунт в Telegram и отправляет с него сообщения контактам записанного человека, а записанный кружок отправляет в качестве подтверждения того, что это реальный человек из их списка контактов.

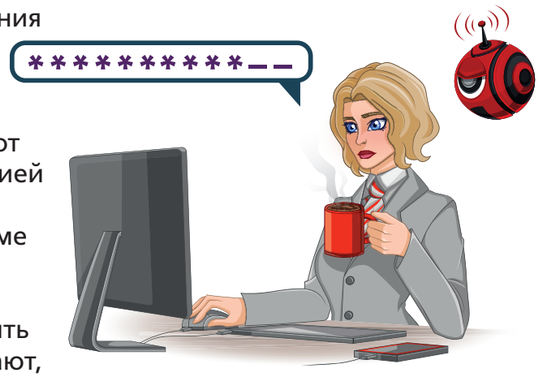
Во время видеозвонка мошенники могут делать снимки экрана, записывать голос и видео с беседой, и в дальнейшем использовать их в своих схемах. Помимо самой видеосвязи мошенник также может получить доступ к функции демонстрации экрана, что позволяет злоумышленникам увидеть коды из смс-сообщений и всплывающих push-уведомлений, поступающих во время разговора.

Кроме того, мошенники применяют методы социальной инженерии, чтобы добраться до счетов взрослых через детей. В частности, мошенники звонят ребенку, представляясь сотрудниками полиции, службы безопасности или других организаций и сообщают о «чрезвычайной ситуации» и призывают перевести деньги родителям, которым якобы угрожает опасность. Мошенники также связываются с ребенком, чтобы сообщить ему о якобы выигранном призе в онлайн-игре или о возможности купить игровую валюту.

2. Распространение вредоносных ссылок на мошеннические интернет-ресурсы (фишинг и смишинг)

2.1. Ссылки на поддельные сайты государственных органов

Злоумышленники рассылают поддельные уведомления от имени государственных органов, содержащие QR-коды для оплаты фиктивных пошлин. Целями атаки выступают кража денег и получение доступа к платежным данным жертв. Мошенники отправляют корпоративным пользователям письма с информацией о якобы вынесенном предписании в связи с нарушениями трудового законодательства. В письме содержится вложенный pdf-документ, где указаны нарушения и сообщается о выездной проверке. Избежать проверки можно, если срочно предоставить необходимые документы. Злоумышленники сообщают, что бумаги уже якобы отправлены в почтовое отделение, и предлагают оплатить их пересылку – 108 рублей. Для этого нужно отсканировать QR-код из pdf-файла. Однако в реальности эта сумма и является целью атаки, а также мошенники могут использовать украденные платежные данные в дальнейшем.



ЛЕГЕНДА «МВД РОССИИ»

Мошенники создают поддельные интернет-ресурсы в виде приемной МВД России. Указанные ресурсы предлагают подать через них обращение по вопросам деятельности МВД России и предназначены для сбора персональных данных граждан.

ЛЕГЕНДА «ФНС РОССИИ»

Мошенники направляют на электронную почту письмо, в котором выдают себя за сотрудников налоговой службы и требуют предоставить декларацию о доходах – для этого надо перейти по ссылке.

На открывающейся странице есть поля, куда человека просят ввести личные данные и все реквизиты банковской карты: номер, имя и фамилию держателя, а также трехзначный код с оборота. Это нужно якобы для подтверждения личности налогоплательщика.

На самом деле такие страницы собирают личные данные. Их достаточно, чтобы вывести с банковской карты деньги, а персональные данные использовать для следующих попыток мошенничества.

2.2. Ссылки на поддельные сайты, связанные с обучением

ЛЕГЕНДА «СДАЧА ОГЭ, ЕГЭ»

В сезон сдачи ЕГЭ и ОГЭ мошенники создают множество Telegram-каналов и сайтов под видом продажи ответов к экзаменам. Особую опасность эти сайты представляют из-за сбора персональных данных как школьников, так и их родителей. Некоторые сайты оснащены «проверкой» адресов электронной почты.

Есть риск получить файлы с вредоносным программным обеспечением для кражи паролей, передать злоумышленникам доступ к своему устройству, а также стать жертвой шантажа из-за перевода денег нежелательным организациям. В лучшем случае жертва получит прошлогодние ответы, а мошенник после перевода денег просто перестанет выходить на связь.

Кроме этого, злоумышленники направляют письма выпускникам и их родителям, выдавая себя за сотрудников ведомств, школ или экзаменационных комиссий, предлагают зарегистрироваться для участия в итоговой аттестации, перейдя по ссылке, ведущей на мошеннический сайт.

ЛЕГЕНДА «ШКОЛЬНЫЙ ОПРОС»

Этот вариант применяется в отношении родителей школьников. Злоумышленники похищают логины и пароли пользователей под видом проведения школьных опросов.

Они рассылают сообщения через мессенджеры и социальные сети от имени родительского комитета. В них содержится ссылка на сайт мошенников, где родителей просят проголосовать по тем или иным вопросам школьной жизни. Например, оценка питания в столовой. Для этого нужно авторизоваться через личный аккаунт, указав логин и пароль, после чего логин и пароль попадают в руки злоумышленников.

2.3. Ссылки на поддельные сайты, связанные со здравоохранением

ЛЕГЕНДА «ПОКУПКА ДЕФИЦИТНЫХ МЕДИКАМЕНТОВ»

Данная схема мошенничества нацелена на русскоязычных пользователей – владельцев домашних животных. Злоумышленники выманивают деньги и финансовую информацию у людей, которые хотят купить импортные лекарства для своих питомцев, на фоне новостей о сокращении поставок ветеринарных препаратов в Россию. Они создали несколько каналов в Telegram, где якобы предлагают людям приобрести необходимые лекарства у перекупщиков.

В описаниях каналов указано, что поставки лекарств якобы осуществляются из-за рубежа, а перекупщики занимаются не только розничной, но и оптовой продажей.

При этом злоумышленники уверяют, что весь товар оригинальный.

О покупке конкретного лекарства с потенциальной жертвой договариваются в личных сообщениях. После того, как человек переводит средства за выбранный товар, ему сообщают, что препарат закончился, и предлагают вернуть деньги. Для этого нужно перейти по присланной ссылке и ввести на странице реквизиты банковской карты, а также сообщить код из смс-сообщения. Однако страница на деле оказывается фишинговой. Таким образом, возврат не происходит, а злоумышленникам уходит финансовая информация человека. К тому же мошенники могут списать еще большую сумму с карты жертвы, если жертва сообщит код из смс-сообщения.

2.4. Ссылки на поддельные сайты магазинов

ЛЕГЕНДА «OZON»

Мошенники стали использовать фишинговые атаки от имени маркетплейса Ozon, чтобы получить доступ к данным граждан.

Они размещают баннеры на сайте, предлагая получить промокод на 10 тыс. рублей ко дню рождения. Однако чтобы его активировать предлагается связаться с «личным менеджером» через WhatsApp.

Для большей убедительности мошенники размещают надпись «WhatsApp Secured authentication» (защищенная аутентификация в WhatsApp). В случае перехода в мессенджер и следования инструкциям злоумышленников граждане рискуют потерять доступ к своей учетной записи и конфиденциальным данным.

ЛЕГЕНДА «WILDBERRIES»

Мошенники берут за основу существующую акцию маркетплейса Wildberries и мобильного оператора связи Т2.

В оригинальной акции пользователям предлагается подключить домашний интернет для получения сертификата на 4 тыс. рублей. Злоумышленники же предлагают пройти регистрацию на поддельном ресурсе gift-wildberries.ru.

ЛЕГЕНДА «ДЕШЕВЫЙ ТОВАР»

Также мошенники пользуются желанием покупателей приобрести товары по выгодным ценам. Жертва приобретает товар по значительно сниженной цене на известной онлайн-платформе. После оформления заказа мошенники связываются через чат с покупателем, сообщая о «временном отсутствии» товара. Они предлагают оформить заказ в одноименном магазине на другом крупном маркетплейсе по такой же или чуть более высокой цене.

Чтобы не упустить выгоду, покупатель соглашается. Затем злоумышленники отправляют ему фишинговую ссылку, которая имитирует официальный сайт маркетплейса. Ссылка может содержать незначительные отличия в написании адреса, например, замену символов (i на 1, b на d). После ввода данных и оплаты через фишинговую страницу мошенники списывают деньги, а товар покупатель не получает.

В другом варианте мошенники запрашивают у жертвы адрес доставки и персональные данные для оформления «бесплатной курьерской доставки». Получив эту информацию, мошенники присылают реквизиты для оплаты через систему быстрых платежей, что также приводит к потере денежных средств.

Кроме того, злоумышленники заманивают покупателей огромными скидками и уникальными предложениями на мошеннические сайты, мимикрирующие под маркетплейсы или страницы крупных магазинов, но после оплаты перестают отвечать. Также они используют фишинговые рассылки с предложением «суперскидок» и «выгодных акций».

ЛЕГЕНДА «РОЗЫГРЫШ БЕСПЛАТНЫХ БИЛЕТОВ»

Мошенники массово рассылают в мессенджерах сообщения с предложением поучаствовать в розыгрышах бесплатных билетов, например, на новогодние мероприятия, включая «Кремлевскую елку». Прикрепленная к сообщению ссылка ведет на фишинговый сайт, на котором предлагается ввести свои персональные и платежные данные якобы «для оплаты небольшой комиссии» за билет в случае выигрыша.

ЛЕГЕНДА «СКАЧАТЬ БЕСПЛАТНО …»

Нередки случаи, когда мошенники маскируют свои ресурсы под сайты с бесплатными фильмами, музыкой, книгами и т.д. Злоумышленники предлагают пользователям посмотреть все серии бесплатно, а на самом деле используют эти сайты для кражи персональных данных и платежной информации.

Злоумышленники постоянно меняют легенды: предлагают якобы получить доступ к взрослому контенту, протестировать премиум-подписку, скачать взломанную версию игры или проголосовать за детский рисунок. Часто мошенники используют тему благотворительности, например, предлагают перевести денежные средства на подарки детям.

ЛЕГЕНДА «ПОДПИСКА НА СЕРВИС»

Еще одна мошенническая схема реализуется при попытке оформить подписку на стриминговый сервис – вместо этого человек попадает на сайт курсов «инфоцыган» и оформляет подписку совсем на другой сервис. Например, такой вид мошенничества зафиксирован на сайте онлайн-кинотеатра «Иви».

ЛЕГЕНДА «ПОКУПКА ПОДАРОЧНОЙ КАРТЫ»

Также мошенники заманивают потенциальных жертв в Telegram-боты, которые активно распространяют в мессенджерах и соцсетях. В таком боте предлагается открыть Telegram Web App для покупки подарочной карты по акции. Для покупки якобы доступны карты номиналом 5 тыс. рублей, которые можно потратить на маркетплейсах, причем приобрести их предлагают со скидкой 50% – всего за 2,5 тыс. рублей. Потенциальным жертвам предлагают и карты других номиналов с неизменно привлекательной скидкой.

Однако на деле форма для приобретения карт является фишинговой и ввод своих платежных данных там чреват потерей денег.

ЛЕГЕНДА «ОТПИСКА ОТ РАССЫЛКИ»

Мошенники, маскируя свои письма под рассылки магазинов, стали использовать в своих целях кнопку «отписки от рассылки» в электронной почте, нажатие на которую перенаправляет пользователя на фишинговый ресурс. Таким образом злоумышленники могут получать персональную информацию о пользователе.

ЛЕГЕНДА «ДОСТАВКА ПОСЫЛКИ»

Еще мошенники при помощи сообщений о поступлении посылки получают доступ к персональным данным и платежным реквизитам. Якобы жертве приходит сообщение о поступлении посылки, информацию о которой можно узнать по ссылке. При переходе по ссылке жертва попадает на поддельный сайт сервиса по доставке, который полностью выглядит как оригинал. После этого у получателя запрашивают персональные данные и платежные реквизиты.

2.5. Ссылки на поддельные финансовые сайты

ЛЕГЕНДА «БАНКОВСКИЕ ИНВЕСТИЦИИ»

Злоумышленники трансформировали работу сайтов-зеркал, которые пользователи принимают за официальные страницы банков. Теперь на таких фишинговых сайтах потенциальных жертв встречает бот, который якобы дает доступ к инвестплатформе, рассчитывает объем необходимых вложений, запрашивает личные данные и принимает взносы.

Фишинговый сайт предлагает пройти тест и получить доступ к инвестиционной платформе банка. После его прохождения на сайте открывается чат, где якобы созданный разработчиками банка бот ведет диалог с клиентом.

Робот предлагает взять на себя всю грязную брокерскую работу: ежедневно анализировать финансовый рынок и самостоятельно совершать сделки попродаже и покупке акций «мировых компаний». Для старта работы бота-брокера пользователю предлагается лишь рассчитать дневной доход от инвестиций, отправить деньги на указанный счет и ждать прибыли. Разумеется, все вложенные средства остаются у мошенников, а «инвесторы» не получают обещанной прибыли.

Бот запрашивает информацию постепенно, начиная от имени и номера телефона, заканчивая кодом из смс-сообщения или паспортными данными. Функция использования бота позволяет охватить как можно больше людей с минимальными ресурсами.

ЛЕГЕНДА «ДОХОД ОТ АКТИВНОСТИ В МЕССЕНДЖЕРАХ И СОЦСЕТЯХ»

Злоумышленники предлагают пользователям Telegram получать доход до 350 евро в день за счет активного просмотра контента. Отличительная особенность этого сценария мошенничества – привлечение потенциальных жертв через проверку аккаунта пользователя социальных сетей и мессенджеров на наличие его премиального статуса. Схема рассчитана на русскоязычных пользователей мессенджеров и соцсетей, которые находятся за пределами Российской Федерации либо используют VPN. В качестве источника дохода мошенники указывают «капитализацию компании», а гарантию заработка объясняют «нейронными технологиями». Под предлогом проверки статуса аккаунта пользователя просят ввести имя и фамилию, но это ни на что не влияет, так как следующая страница сообщает об успешном прохождении проверки и наличии Premium-аккаунта даже тем, у кого нет Premium-подписки. «Такой статус менее чем у 2% пользователей», – сообщают мошенники и предлагают указать электронную почту и номер телефона для получения «дохода с аккаунта», который якобы формируется за счет активности: просмотра контента, лайков и комментариев. После ввода данных пользователя просят ожидать звонка «персонального менеджера». Личный «инвестиционный эксперт» на самом деле – работник мошеннического колл-центра, чья задача – убедить потенциальную жертву инвестировать деньги в «выгодный проект» под воздействием обещаний высокой прибыли. В оформлении поддельных сайтов используются фирменные цвета и товарный знак Telegram.

По аналогичному шаблону работают поддельные сайты, нацеленные на пользователей WhatsApp и Facebook. На указанные сайты потенциальных жертв заманивают через социальные сети. Как правило, злоумышленники создают аккаунты с типовыми названиями вроде «Срочные новости» и «Новости сейчас» и публикуют сообщения про высокий заработок, который пользователи якобы могут получить за счет своей активности в соцсети. Мошенники продвигают такие посты с помощью рекламы. Для этой же цели создают поддельные страницы в средствах массовой информации под шаблонным заголовком: «Раскрыт новый источник дохода … (имя любого известного российского деятеля) …». Ссылки из таких постов ведут на мошеннические сайты, оформленные в стиле Telegram, WhatsApp и Facebook.

ЛЕГЕНДА «РАСШИФРОВКА АУДИОФАЙЛОВ»

Схема с предложениями «заработать» на расшифровке аудиофайлов направлена на кражу персональных данных. Для ее применения злоумышленники создают площадки с разными названиями, но идентичным дизайном и контактами для связи. На этих площадках мошенники предлагают расшифровать аудиозаписи публичных выступлений, интервью и лекций за определенную плату. В качестве главных способов воздействия на потенциальных жертв применяются обещания высокого дохода, удобного графика и минимальных требований.

Для начала сотрудничества пользователя просят зарегистрироваться на портале, ознакомиться с инструкцией и только потом приступить к работе. Выполнив задание, автор пробует вывести сумму вознаграждения, но сталкивается с проблемой: сервис требует платно подтвердить аккаунт. «Зарплату» человек, конечно же, не получает, а переведенные деньги теряет безвозвратно.

ЛЕГЕНДА «VISA, MASTERCARD»

Злоумышленники рассылают ложные смс-сообщения якобы от Сбербанка о восстановлении полного функционала карт Visa и Mastercard, включая трансграничные платежи. В сообщениях владельцам карт предлагается пройти ограниченную по времени «валидацию». Для этого они должны пройти по ссылке, которая ведет на поддельную страницу банка с вводом регистрационных данных. Кроме того, при переходе по ней возможно распространение вредоносного программного обеспечения. Мошенники используют механизмы IP-телефонии для подмены номеров отправителя на +900 или +900#, чтобы придать сообщению правдоподобность.

ЛЕГЕНДА «ВЫПЛАТА КОМПЕНСАЦИИ»

Мошенники маскируются под госорганы, рассылая от их имени фишинговые ссылки или создавая поддельные сайты, и предлагают подать заявление для выплаты в 14 тыс. рублей, якобы для компенсации прошлогодней инфляции. Для получения денег нужно оформить необходимые документы на портале «Госуслуги». Однако ссылка ведет на мошеннические ресурсы.

2.6. Ссылки на поддельные сайты телефонной связи

Злоумышленники создают фишинговые сайты под видом порталов операторов связи и рассылают push-уведомления жертвам с просьбой подтвердить паспортные данные по ссылке, ведущей на такой сайт, для подтверждения номера. Затем пользователь переходит на портал «Госуслуги», где ему нужно ввести логин и пароль от личного кабинета. После этого мошенники получают доступ как к личному кабинету жертвы на портале «Госуслуги», так и подтвержденную информацию об абоненте.

Еще злоумышленники рассылают push-уведомления, которые настраивают через веб-сайт, не используя мобильное приложение. В них мошенники сообщают, что для продления работы мобильного номера нужно подтвердить паспортные данные. На фишинговом сайте пользователя просят заполнить анкету, включая номер телефона, ФИО и дату рождения. Затем его переводят на поддельную страницу входа на портал «Госуслуги» для дополнительного подтверждения.

2.7. Ссылки на поддельные сайты жилищного хозяйства

ЛЕГЕНДА «ОПЛАТА КОММУНАЛЬНЫХ УСЛУГ»

Мошенники стали использовать современные технологии для создания фальшивых платежных документов за жилищно-коммунальные услуги. Поддельные квитанции внешне не отличаются от настоящих. Злоумышленники рассчитывают, что гражданин, получивший такой «платежный документ», автоматически оплатит задолженность с помощью QR-кода, не проверив реквизиты.

Также злоумышленники связываются с людьми с неизвестного номера, через электронную почту, соцсети и мессенджеры, предлагая им оплатить счет за коммунальные услуги со скидкой или провести перерасчет. Для этого злоумышленники просят жертв перейти по ссылке, которая на самом деле ведет на фишинговый сайт. Для платежа человеку предлагается ввести свои персональные данные, адрес проживания и данные банковской карты. Вся эта информация после заполнения формы попадает в руки мошенников.

ЛЕГЕНДА «ГРАФИК ОТКЛЮЧЕНИЯ ГОРЯЧЕЙ ВОДЫ»

Еще мошенники рассылают россиянам фальшивые письма с предложением проверить график отключения горячей воды. Цель подобных сообщений – похищение персональных и банковских данных. В письме после фразы «Узнайте, когда отключат горячую воду по вашему адресу» или «Проверьте, когда отключат горячую воду в Вашем доме» расположена ссылка, ведущая на поддельный сайт, имитирующий официальный ресурс, предлагающий ввести персональные данные, либо на установку вредоносного программного обеспечения, ворующего логины, пароли и банковские данные.

ЛЕГЕНДА «ДОМОВОЙ ЧАТ»

Мошенники стали атаковать россиян в домовых и районных чатах. Злоумышленники размещают там сообщения с предложениями бесплатно отдать ненужную бытовую технику или мебель, но на деле распространяют фишинговые ссылки.

Заинтересовавшимся гражданам предлагают встретиться через пару дней лично, отправляют фото или видео, подтверждающее наличие предмета. Однако накануне встречи фальшивый сосед извиняется и говорит, что технику может отправить лишь с курьером. А для оформления доставки якобы нужно перейти по ссылке, которая является фишинговой.

Еще мошенники расклеивают объявления в подъездах, оформляя их максимально правдоподобно: «Вступите в чат вашего дома в Telegram!». Внизу указан QR-код. Как только человек его сканирует, он попадает на фишинговую страницу, которая выглядит как официальный сайт Telegram. На этой странице просят ввести номер телефона, код из смс-сообщения и иногда дополнительные данные. Как только данные введены, доступ к аккаунту оказывается у мошенников.

2.8. Ссылки на иные поддельные сайты

ЛЕГЕНДА «АРЕНДА ЖИЛЬЯ»

Мошенники размещают в соцсетях короткие видео с выгодными предложениями. Например, «Апартаменты в Сочи/Светлогорске. 5 минут до моря. От 3000 рублей в сутки». Для публикации злоумышленники обычно используют недавно созданные аккаунты, срок их «жизни» редко превышает 1 – 2 месяца. У такого ролика может быть много просмотров, которые накручивают при помощи специальных платных инструментов. Ролик выглядит как видеообзор квартиры или слайд-шоу из фотографий, которые находят в сети «Интернет».

Злоумышленники указывают цену на аренду ниже рыночной или обещают заманчивые скидки. «Собственник» жилья сообщает, что находится за границей и не может воспользоваться российскими картами.

Также в переписке мошенники сообщают, что предоплата не требуется: потенциальной жертве предлагают «безопасное бронирование» через известный сервис. В этом варианте злоумышленники используют поддельные ресурсы трех популярных российских сервисов для бронирования отелей и квартир. Для обмана могут выбрать любой из них. Мошенник оформляет заявку в «сервисе» и ожидает от жертвы подтверждения. У злоумышленников есть два основных подхода: в первом варианте мошенник лично отправляет клиенту ссылку на «сервис» для регистрации, а во втором – присылает данные на почту, чтобы создать видимость официальной сделки. Входящее письмо практически неотличимо от тех, что рассылает настоящий сервис. Некоторые мошенники для пущей убедительности присылают фотографии поддельного паспорта. Задача мошенников – убедить потенциальную жертву перейти по ссылке на поддельный сайт и внести 1 рубль для бронирования квартиры.

В переписке злоумышленники будут уверять, что работают «без серых схем» и «только официально», плата в один рубль нужна для «гарантии» намерений клиента, а остальную сумму автоматически спишут при заселении. Арендатор нажимает на ссылку, попадает на фишинговый сайт, вводит платежные реквизиты и отправляет средства на счет мошеннику.

Еще под предлогом съема жилья злоумышленники похищают данные карт и деньги со счетов. В ходе переписки злоумышленник предлагает жертве перейти в мессенджер, где просит дополнительные фото квартиры, адрес, а также интересуется мелочами, чтобы создать вид заинтересованного арендатора. Затем мошенник предлагает оформить договор аренды через известный профильный сервис. Он обещает самостоятельно через этот портал заполнить все документы и перевести оговоренную сумму, а арендодателю останется лишь получить деньги. После этого потенциальная жертва получает ссылку на сгенерированный в специальном Telegram-боте фишинговый ресурс, который повторяет профильный сервис. А когда арендодатель вводит там данные своей карты, злоумышленники крадут деньги с его счета.

ЛЕГЕНДА «КАДРОВЫЕ РАССЫЛКИ»

Злоумышленники маскируются под HR-отделы крупных компаний и рассылают поддельные письма от имени кадровых служб. Сообщения выглядят максимально правдоподобно. В теме письма указывается нечто важное и привлекающее внимание, например, «Обновленное руководство для сотрудников». Внутри письма используется деловой стиль, характерный для официальных корпоративных коммуникаций, и подчеркивается необходимость ознакомиться с новыми требованиями.

Главная цель фишинговой атаки – побудить пользователя кликнуть по ссылке и ввести свои данные на поддельной странице входа. Письмо использует авторитет HR-отдела и создает ощущение срочности, чтобы жертва не задумывалась о подлинности письма.

Мошенники также прибегают к психологическим приемам, вызывая у сотрудников страх неисполнения корпоративных требований, например, в письме предлагается перейти по ссылке, ведущей на поддельный сайт, имитирующий платформу для хранения документов. Когда пользователь нажимает на ссылку, его перенаправляют на страницу, якобы принадлежащую Microsoft. Здесь он видит форму для ввода корпоративных учетных данных. Вслед за ее непосредственным заполнением пользователю показывается сообщение об ошибке, а затем он перенаправляется на настоящий сайт Microsoft. Это вызывает у жертвы иллюзию незначительной проблемы, и она не подозревает о том, что данные уже скомпрометированы.

ЛЕГЕНДА «ПОДДЕЛЬНЫЕ QR-КОДЫ»

Злоумышленники создают поддельные сайты, имитирующие легитимные ресурсы, и размещают QR-коды в общественных местах. Например, на парковочные счетчики наклеиваются QR-стикеры, перенаправляющие жертв на поддельные платежные системы.

Также поддельные QR-коды появились на электросамокатах и велосипедах, которые можно взять в аренду. При сканировании такого кода жертва попадает на фишинговый сайт, через который злоумышленники завладевают личными данными и денежными средствами. Письма с QR-кодами, маскирующиеся под запросы двухфакторной аутентификации, мошенники используют для кражи учетных данных. При сканировании QR-кода с мобильного устройства весь последующий трафик между жертвой и злоумышленником проходит через сотовую сеть в обход корпоративных систем безопасности.

Отдельную угрозу представляет так называемое «QR-искусство» – изображения, в которых код замаскирован под обычную картинку. Пользователь может случайно отсканировать его камерой и перейти по вредоносной ссылке, даже не осознав этого.

3. Обман при продаже товаров и услуг в сети «Интернет» (скамминг)

ЛЕГЕНДА «МАРКЕТПЛЕЙСЫ»

Мошенники обманывают подростков, предлагая им «выгодные» покупки брендовых вещей. Детям пишут в Telegram и предлагают дешево выкупить товары с китайского маркетплейса Poizon. Сначала жертвы переводят деньги родителей за несуществующую покупку, а потом оплачивают «торговые пошлины». Обещанная посылка до заказчика не доходит.

Также мошенники выманивают у людей деньги на маркетплейсах под предлогом уплаты таможенных пошлин. Злоумышленники рассылают поддельный документ от имени Федеральной таможенной службы, где от покупателя требуют прислать дополнительные деньги. Такую же схему практикуют и при торговле через Telegram-каналы.

ЛЕГЕНДА «НОТАРИАЛЬНЫЕ УСЛУГИ»

На платформе «Авито» мошенники представляются нотариусами или некими «просветленными посредниками» и предлагают якобы нотариальные услуги в онлайн-режиме. Обещают сделать «любую бумагу» быстро, без личных встреч и лишних хлопот. Нужно только перевести им на карту стопроцентную предоплату, прислать сканы паспорта и других личных документов.

ЛЕГЕНДА «ИНВЕСТИЦИИ»

Злоумышленники используют бренд государственного фонда «Защитники Отечества» для рекламы инвестиционного мошенничества. Они создали сайты, на которых размещены ложные сообщения о запуске «социального проекта» с предложением заработать до 30 млн. рублей, «используя ресурсы и возможности России».

Все эти сайты разработаны по типовому шаблону, предположительно в рамках партнерской мошеннической программы. Пользователям предлагают инвестировать в акции российских компаний. Для придания этим сообщениям правдоподобности злоумышленники размещают поддельные комментарии от имени людей, которые якобы получили крупные выплаты.

Пользователей просят оставить для связи ФИО и контактный телефон. После того, как жертва укажет свои данные на таком сайте, ей звонит злоумышленник, который представляется персональным «менеджером». Конечной целью мошенников может быть не только хищение денег, которые под предлогом покупки акций требуется внести на депозит. Как необходимое условие открытия брокерского счета пользователю могут предложить установить мобильное приложение, которое на самом деле окажется вредоносным и получит контроль над устройством для списания денег со всех счетов. Кроме того, для вывода «доходов» с инвестплатформы у пользователя могут запросить скан паспорта. В случае согласия эта личная информация окажется у злоумышленников и может быть использована для других мошеннических атак.

ЛЕГЕНДА «ЗАРУБЕЖНЫЕ АКТИВЫ»

Объявления мошенников с предложениями решить проблему заблокированных за рубежом активов граждан массово распространяются в сети «Интернет», соцсетях и мессенджерах, а также рассылаются по электронной почте.

Для разблокировки предлагается перевести на счет сумму, равную стоимости замороженных активов. Мошенники обещают, что граждане смогут вернуть деньги в двойном размере.

ЛЕГЕНДА «СПЕЦФОНД ВПК»

Мошенники создали в сети сайт выдуманной организации «Спецфонд ВПК», используя этот предлог для похищения денег пользователей. Мошенники цинично предлагают вложить деньги в «укрепление обороноспособности» государства. В подтверждение своих слов злоумышленники приводят цитаты первых лиц и поддельные документы.

Цена одной фальшивой акции на сайте «Спецфонд ВПК» начинается от 10 тыс. рублей. «Инвестировать» на ресурсе предлагают в акции «Уралвагонзавода», концерна «Калашников» и других крупнейших предприятий с доходностью от 90% годовых.

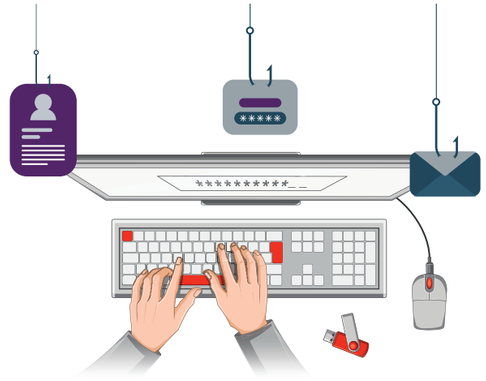
Между тем разовое хищение денег – не единственная цель создателей «Спецфонда ВПК». Злоумышленники также пытаются заполучить контроль над гаджетами потенциальных жертв через установку мобильного приложения. Оно открывает мошенникам доступ сразу ко всем счетам.

ЛЕГЕНДА «ЦИФРОВОЙ РУБЛЬ»

Стали появляться ресурсы, на которых предлагают стать участниками инвестиционной программы «Цифровой рубль Банка России». Пользователи, которые переходят на такие сайты, видят страницу с символикой цифрового рубля и чат-бот с «личным менеджером». Первые сообщения в чат-боте обещают «доход от 100 тыс. рублей уже с первых дней». При этом пользователя заранее предупреждают, что минимальная сумма «инвестиций» составляет 10 тыс. рублей.

Под предлогом расчета потенциального дохода и «удобной» суммы вклада потенциального инвестора просят ответить на ряд вопросов. Требуется указать возраст, гражданство, статус на рынке труда, финансовую цель, диапазон дохода. Затем чат-бот запрашивает имя, фамилию и контактный номер телефона, после чего на экран выводится сообщение: «Наши специалисты перезвонят вам в ближайшее время». Жертве звонит злоумышленник, который представляется персональным «менеджером», открывает доступ к «инвестиционной платформе», уговаривает внести «депозит». Итог таких инвестиций всегда один – полная потеря внесенных денег.

4. Внедрение вредоносного программного обеспечения (фарминг)



Злоумышленники рекомендуют жертве под различными предлогами установить на устройство приложение, распространяющее вредоносное программное обеспечение, направленное на хищение персональных данных. Когда жертва соглашается и устанавливает мобильное приложение, на ее устройство загружается вредоносное программное обеспечение, которое похищает все имеющиеся на устройстве данные.

Кроме того, есть и другой вариант, когда злоумышленники предлагают человеку установить программу, например, чтобы следить за здоровьем. В этом случае мошенники просят жертву самостоятельно внести все данные о себе.

4.1. Вредоносное программное обеспечение в здравоохранении

ЛЕГЕНДА «ПРИЛОЖЕНИЕ МИНЗДРАВА»

Злоумышленники звонят потенциальным жертвам, представляясь сотрудниками страховых компаний. Под предлогом необходимости продлить полис ОМС или оформить его электронную версию они убеждают собеседников установить мобильное приложение, якобы разработанное Минздравом. На деле речь идет о поддельной программе, которая предназначена для перехвата данных мобильного банка.

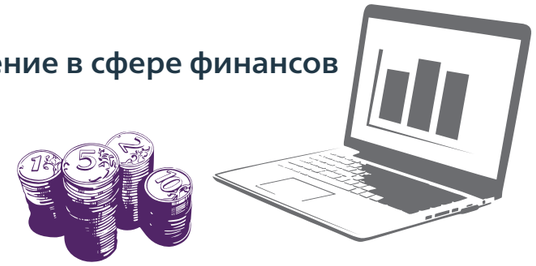
Еще мошенники звонят и убеждают установить новое «приложение Минздрава», если человек недавно проходил медицинские обследования, чтобы получить кешбэк. После того, как приложение оказывается в телефоне, мошенники дают жертве форму для ввода данных и получают доступ к банковской карте.

ЛЕГЕНДА «МЕДИЦИНСКИЕ ДОКУМЕНТЫ»

Мошенники распространяют программное обеспечение для дальнейшего шпионажа под видом медицинских файлов. Внедряемое программное обеспечение – это Havoc, легальный и достаточно редкий программный продукт для тестирования на проникновение.

В случае с медицинскими документами на устройство потенциальной жертвы загружается отвлекающий документ – некая выписка из амбулаторной карты. Параллельно идет скрытая установка загрузчика, а затем и агента Havoc. После этого Havoc дает злоумышленникам возможность удаленно выполнять команды на устройстве пользователя и выгружать данные оттуда.

4.2. Вредоносное программное обеспечение в сфере финансов



ЛЕГЕНДА «БРОКЕРСКИЙ СЧЕТ»

Брокерский счет – это специальный счет, на который инвестор кладет свои деньги для последующего вложения в ценные бумаги: акции и облигации. Чтобы открыть такой счет, нужно обратиться к лицензионному брокеру или в управляющую компанию. Список брокеров с лицензией находится в открытом доступе на сайте Центробанка Российской Федерации и регулярно обновляется.

На брокерском счете можно заработать двумя способами: за счет трейдинга (активной торговли на бирже, когда человек старается купить ценные бумаги по самой низкой цене, чтобы затем перепродать их как можно дороже) или инвестирования. Во втором случае он покупает активы, чтобы владеть ими в течение определенного срока и получать прибыль за счет выплаты дивидендов.

Чаще всего мошенники используют одни и те же приемы: чрезмерное количество рекламы, спам-рассылки и «холодные» звонки, обещание быстрой прибыли или доступа к курсам трейдинга в обмен на регистрацию или установку приложения.

Злоумышленники находят своих жертв в сети «Интернет» или социальных сетях и предлагают открыть брокерский счет. Они обещают, что те в короткие сроки смогут заработать крупную сумму денег. Однако инвестиции, которые делают россияне, не возвращаются.

Для открытия счета мошенники предлагают установить приложение по ссылке, где они ложно показывают, как растут доходы от инвестиций, в том числе в криптовалюту. Лжеброкеры могут даже оказать «помощь» и провести «консультации» при выборе инвестиционного продукта. Однако как только у человека возникает желание вывести деньги, ему начинают рассказывать о разных препятствиях и расходах на такую операцию.

К примеру, мошенники могут попросить внести дополнительные деньги на счет для полного вывода средств. Или потребовать оплаты «страховки», платы за ежедневное размещение валюты в «европейской ячейке» или срочного платного вывода средств. «Обменником» валюты может выступать некий человек, на счет которого мошенники просят совершить перевод. В некоторых случаях они вынуждают «инвестора» открыть счет в сторонней кредитной организации.

Для того чтобы вывести деньги со счета, лжеброкеры требуют найти поручителя, и даже зарегистрировать его в Минфине России, чтобы можно было «обналичить» средства. Людям предлагается написать письмо, причем на адрес пресс-службы Минфина, с указанием данных поручителя и суммы средств, которые необходимо ему передать.

ЛЕГЕНДА «БАНКОВСКИЕ ПРИЛОЖЕНИЯ»

В App Store появись поддельные приложения ВТБ и Тинькофф банка. Это фишинговые приложения, главная цель которых украсть персональную информацию. При этом оценки сервисов в App Store накручены, к ВТБ и Тинькофф банку они не имеют никакого отношения. ВТБ и Тинькофф банк находятся под санкциями США, приложения обеих кредитных организаций удалены из App Store и Google Play. При этом клиентам банков доступны ранее скачанные приложения и web-версии мобильных банков.

ЛЕГЕНДА «ПОСЫЛКИ»

Злоумышленники под предлогом получения почтового отправления убеждают потенциальных жертв установить приложение, при помощи которого затем получают доступ к телефону.

Это позволяет злоумышленникам украсть средства или личные данные жертвы, а также установить на ее устройство дополнительное вредоносное программное обеспечение.

5. Иные схемы мошенничества

ЛЕГЕНДА «ДОСТАВКА ЦВЕТОВ И ПОДАРКОВ»

Мошенники отправляют людям цветы и подарки, чтобы затем выманить код из смс-сообщения и украсть деньги с карты или даже оформить кредит. Сначала к жертве приезжает курьер, представляется сотрудником службы доставки цветов, дарит цветы от «неизвестного отправителя» и уезжает. На следующий день человеку звонят из той же службы и просят назвать цифры из смс-сообщения якобы для отчетности. Если получатель согласится, с его карты могут попытаться списать деньги или даже оформить на него кредит.

ЛЕГЕНДА «ЗАРАБОТОК ЗА ЛАЙКИ»

Мошенники обманывают россиян, предлагая им заработать деньги за лайки. Такая подработка может обернуться потерей аккаунта в мессенджере, денег и ценных данных.

Мошенники размещают объявление о заработке в сети «Интернет». Все, что требуется от пользователя, – поставить лайк на сайте (например, маркетплейса), оставить отзыв, посмотреть рекламные ролики. Задача простая, но оплата достаточно привлекательная для потенциальных жертв.

Дальше у мошенников может быть несколько вариантов обмана. В первом после выполнения задания они просят сообщить платежные данные карты для начисления вознаграждения. Естественно, жертва не получит никаких денег, а только лишится их.

Во втором варианте после начисления денег мошенники могут попросить сообщить им номер телефона и код из смс-сообщения для подтверждения личности. Аналогично злоумышленники могут увести аккаунт в Telegram. В третьем случае мошенники присылают ссылку на поддельный сайт, где надо ввести платежные данные с карты. При этом есть и более сложные схемы, когда жертве действительно производят небольшие начисления, а потом могут начать выманивать крупные суммы.

ЛЕГЕНДА «СЕРВИС ЗНАКОМСТВ»

Мошенники налаживают доверительные отношения с пользователями соцсетей и сервисов знакомств, а затем выманивают у них деньги под предлогом инвестиций или развития бизнеса. Злоумышленники применяют не только традиционные методы социальной инженерии, но и современные технологии искусственного интеллекта, включая дипфейки. Чаще всего они действуют через фальшивые аккаунты. Страницы злоумышленников наполняются персонализированным контентом, который создают с помощью нейросетей – таким образом мошенники подстраиваются под каждого конкретного пользователя и сохраняют заданную легенду.

Получив средства, мошенники либо обналичивают их, либо переводят в криптовалюту и исчезают.

ЛЕГЕНДА «ОШИБОЧНЫЙ» ПЕРЕВОД ДЕНЕЖНЫХ СРЕДСТВ»

Мошенники переводят денежные средства на банковскую карту, далее связываются с жертвой и убеждают вернуть деньги, но на другие реквизиты. Если жертва соглашается с такой схемой возврата денежных средств, то далее с ней связывается следующий участник мошеннической схемы и шантажирует, рассказывая, что денежные средства переведены «террористу» или транзитным переводом через карту жертвы были выведены украденные средства.

ЛЕГЕНДА «ПРИНУДИТЕЛЬНОЕ ОФОРМЛЕНИЕ МИКРОКРЕДИТОВ В МФО»

Неожиданные переводы на карту с неизвестных номеров могут оказаться мошенническими, независимо от того, пришли они от физического лица или от компании. Обычно схема начинается с того, что человеку на карту приходит определенная сумма. Этоможет быть несколько сотен, в редких случаях несколько тысяч рублей. После этого на телефон звонит так называемый сотрудник банка или представитель микрофинансовой организации и рассказывает, что уже одобрен кредит. Таким образом, поступившие средства являются якобы частью одобренной суммы.

Затем мошенники начинают узнавать персональные данные и реквизиты банковской карты, просят код из смс-сообщения.

Существуют два варианта развития событий – либо на жертву оформят микрокредит и действительно переведут деньги, и тогда придется платить по новым правилам до 0,8% на всю сумму в день, либо заем оформят, но денег не отправят, а переведут их себе, при этом обязательства по выплате займа будут возложены на жертву.

Возможен еще вариант, когда деньги также зачисляются на карту, но представители МФО звонят практически сразу. Оператор незамедлительно благодарит за использование услуг компании. После обнаружения факта отсутствия оформления займа соглашается на отмену микрокредита. Для этого МФО отправляет код на телефон, который необходимо сообщить оператору.

В действительности человек этим действием не отменяет микрокредит, а соглашается на него.

ЛЕГЕНДА «ВЫПЛАТА МАТЕРИАЛЬНОЙ ПОМОЩИ»

Злоумышленники от имени крупных страховых компаний предлагают ложные выплаты участникам СВО, пенсионерам и матерям-одиночкам, пытаясь заполучить их конфиденциальные данные и доступ к банковским счетам и личным кабинетам на портале «Госуслуги». Они сначала устанавливают контакт с жертвой через рекламные объявления, фишинговые сайты или массовые рассылки в социальных сетях и мессенджерах. Затем жертвам предлагают связаться с «менеджером» в мессенджере для «оформления выплат», после чего под предлогом проверки льгот запрашивают сканы паспорта и СНИЛС, реквизиты банковской карты, а также код из смс-сообщения для восстановления пароля от портала «Госуслуги».

Также специально ко Дню Победы злоумышленниками были созданы ресурсы, на которых ветеранам обещают единовременные выплаты в размере от 50 до 300 тыс. рублей. Мошенники выдают себя за сотрудников соцзащиты, муниципальных администраций или специалистов портала «Госуслуги».

При этом мошенники требуют принять решение очень быстро, чтобы не дать людям опомниться, а необходимым условием является оплата якобы «комиссии» и введение данных банковской карты.

Еще один вариант связан с обещанием выплатить дополнительную материальную помощь раненым жителям Курской, Белгородской, Брянской и Воронежской областей. Мошенники предлагают пострадавшим направить через Telegram-бот персональные данные всех членов семьи, включая фотографии, информацию о регистрации на территории указанных регионов, а также заявление в свободной форме. Для убедительности злоумышленники распространяют поддельное распоряжение полномочного представителя президента Российской Федерации в Центральном федеральном округе.

ЛЕГЕНДА «ПЕРЕРАСЧЕТ ПЕНСИИ»

Мошенники предлагают «оцифровку данных» якобы для сохранения трудового стажа и увеличения выплаты, а на самом деле выманивают доступ к порталу «Госуслуги». Они создают групповые чаты якобы от имени прошлого работодателя жертвы и имитируют обсуждение процедуры «оцифровки трудового стажа». Затем разговор заходит о неких «ключах от Роструда», которые необходимо получить. В ходе разговора подставные участники чата утверждают, что уже получили эти ключи, и убеждают жертву следовать их примеру. Как только жертва пытается выполнить указанные действия, она рискует потерять доступ к своему личному кабинету на портале «Госуслуги».

ЛЕГЕНДА «ПОЛУЧЕНИЕ СТИПЕНДИИ»

Мошенники от лица Минобрнауки предлагают студентам получить стипендию, подтвердив данные на портале «Госуслуги». С этой целью злоумышленники просят студентов актуализировать их персональные данные на сайте ВУЗа с помощью портала «Госуслуги». Затем мошенники отправляют жертве заведомо неактивную ссылку на подтверждение от портала «Госуслуги». Они предлагают помощь в авторизации, прося пароль, при этом утверждая, что логин у них уже есть.

ЛЕГЕНДА «ПОДДЕЛЬНЫЕ ВАКАНСИИ»

В популярных Telegram-каналах, публикующих вакансии, участились случаи мошенничества, связанные с предложениями удаленной работы в IT-сфере. Мошенники предлагают кандидатам заполнить Google-форму и оставить свои контактные данные или связаться напрямую с HR-менеджером. После этого соискателям назначают дистанционное собеседование через мессенджер. Во время собеседования злоумышленники могут применять фишинговые страницы, просить включить функцию демонстрации экрана или предоставить доступ к устройству.

Также злоумышленники публикуют объявления о приеме на работу, а затем под предлогом оформления требуют предоставить номер СНИЛС. С помощью СНИЛС мошенники могут оформлять фиктивные социальные выплаты, получать кредиты на имя жертвы, пользоваться медицинскими услугами и т.д.

Еще мошенники в рамках трудоустройства требуют единовременную оплату НДФЛ под предлогом «аутентификации» или «регистрации» в системе работодателя. Такое требование противоречит нормам трудового и налогового законодательства Российской Федерации.

ЛЕГЕНДА «ПОДДЕЛЬНЫЕ ТОЧКИ ДОСТУПА WI-FI»

Злоумышленники создают собственные фальшивые сети, которые внешне выглядят как реальные.

С вредоносными сетями можно столкнуться в любом общественном месте. Например, в аэропорту Шереметьево работала точка доступа с названием SVO_Free (вместо официальной сети _Sheremetyevo Wi-Fi). Вместо стандартной процедуры авторизации (введение кода, направленного смс-сообщением) мошенники предлагают авторизоваться через Telegram. Для этого необходимо в сервисном боте отправить шестизначный код, который приходит через смс-сообщение. Таким образом, злоумышленники получают доступ к аккаунту Telegram.

Мошеннические точки Wi-Fi позволяют контролировать поток сетевого трафика устройств пользователей, получать данные из него, а при некоторых манипуляциях и необдуманных действиях человека это возможно сделать даже из защищенного потока.

Использование собственных точек Wi-Fi открывает широкие возможности перед злоумышленниками. Среди прочего они могут выделять из трафика аутентификационные данные и параметры установленных сессий, которые позволяют входить в соцсети, электронную почту и мессенджеры. Также «свой» Wi-Fi дает возможность мошенникам атаковать гаджеты и заражать их вирусами.

Заключение

Правила безопасного поведения

1. Необходимо особое внимание обращать на ключевые признаки мошенничества. Если звонящий упоминает такие выражения, как «служба безопасности банка», «единый расчетный счет Центрального банка», «сообщите код из смс» или требует предоставить личные данные, следует немедленно прекратить разговор.

   Ни в коем случае нельзя сообщать код подтверждения доступа из смс-сообщений или вводить логин и пароль где бы то ни было поуказанию неизвестных лиц.

   Также признаком мошенничества является предъявление по видеосвязи удостоверений или других «подтверждающих» документов. Необходимо помнить о категорическом запрете вводить любые коды и переходить по ссылкам из писем и смс-сообщений, а также сообщать незнакомым лицам свои персональные и финансовые данные.

2. Официальные организации не звонят лично каждому клиенту. Для информирования они обычно используют собственные приложения и сайты.

   Помните, что ни одна официальная служба не требует передачи кодов из смс-сообщений или электронной почты.

3. При звонках или сообщениях от правоохранительных органов необходимо иметь в виду, что уведомления о привлечении к уголовной ответственности передаются исключительно лично и в письменной форме.

   Использование мессенджеров для прямого взаимодействия с гражданами запрещено (Федеральный закон от 1 апреля 2025 г. № 41-ФЗ)

   Гражданам рекомендовано самостоятельно перезванивать в общественные приемные для проверки информации.

4. Судебный пристав не сообщает о наличии долга и не просит скидывать какие-либо реквизиты для оплаты. Приставы отправляют должнику извещение о возбуждении исполнительного производства в письменном виде или через портал «Госуслуги» и дают ему время добровольно исполнить обязательства. Также получить квитанцию можно, придя на личный прием к судебному приставу, а затем внести оплату непосредственно по квитанции или же через портал «Госуслуги».

Если остается сомнение и тревожит, что информация якобы от имени Федеральной службы судебных приставов может оказаться правдой, то в любом случае стоит прекратить разговор и самостоятельно перезвонить по официальному номеру службы. Проверить наличие исполнительного производства можно на официальном сайте Федеральной службы судебных приставов или на портале «Госуслуги».

5. ФНС России никогда не рассылает электронные письма о задолженности с предложением оплатить ее онлайн.

6. У Минздрава нет никаких специальных приложений для клиентов. Все цифровые сервисы доступны на портале «Госуслуги». Для того чтобы защититься от схем, связанных с медицинскими документами, необходимо соблюдать ряд правил безопасности. В частности, прежде всего, использовать антивирусное программное обеспечение, а также внимательно следить за тем, что установлено на вашем смартфоне или компьютере.

   Регулярно обновляйте операционные системы на своих устройствах и следите за их «цифровой чистотой». А если вы собираетесь получить данные от медицинского центра, то лучше это делать только через его официальное приложение или же в личном кабинете.

   Если же вам пришло письмо якобы от имени клиники, то ни в коем случае не переходите по ссылкам из него и не открывайте файлы. Если в сообщении указан номер телефона, звонить по нему также не стоит – лучше воспользоваться официальными номерами и уточнить, действительно ли результаты анализов готовы и доступны в личном кабинете.

7. Если мошенники все-таки завладели вашим личным кабинетом, постарайтесь как можно быстрее восстановить доступ к нему.

8. В целях безопасности продавцы товаров при общении с покупателями должны оставаться на специализированной площадке, где есть условия для безопасной сделки.

9. Совершайте покупки только у проверенных продавцов и в магазинах с положительными отзывами. Если для оплаты необходимо ввести на странице данные банковской карты, проверьте доменное имя на опечатки или необычные символы.

   Никому не сообщайте код из смс-сообщений или push-уведомлений.

10. Не следует обращать внимания на огромные скидки, которых больше нет ни в одном магазине. Также необходимо всегда проверять адрес магазина в адресной строке и следить за официальными источниками.

    Для маскировки фишинговых страниц злоумышленники часто меняют одну букву или символ в адресе официальной веб-страницы.

11. Не стоит вводить на подозрительных сайтах личные и платежные данные.

    К таким сведениям относятся данные карты и срок ее действия, коды подтверждения из смс-сообщений, трехзначный код с обратной стороны карты (CVC/CVV-код), логин и пароль от мобильного приложения и интернет-банка.

12. Необходимо помнить, что если продавец товаров или услуг постоянно торопит совершить покупку, следует остановиться и проверить его надежность: почитать отзывы, сравнить цены с конкурентами.

13. Для защиты аккаунтов (в мессенджерах и не только) важно использовать сложные пароли и настроить двухфакторную аутентификацию.

14. Нужно помнить, что нельзя отправлять деньги по реквизитам, переданным ботом в Telegram или на сайте, а все онлайн-коммуникации с клиентом банки ведут только в собственных приложениях.

15. Чтобы распознать мошеннические сайты с предложением легкого заработка, включая схемы с расшифровкой аудиозаписей, необходимо обращать внимание на целый ряд важных индикаторов. Необходимо трезво оценивать потенциальные вознаграждения и усилия, которые придется приложить для выполнения задач. Если за простую работу, которая займет немного времени, кто-то предлагает немаленькую сумму, то это может сигнализировать о мошенничестве. Легкие деньги в сети «Интернет» очень часто сопряжены с мошеннической деятельностью, поэтому лучше воздержаться от «заманчивых» вариантов.

16. Получив заманчивое, но подозрительное предложение в домовом чате, лучше отсрочить свое общение с потенциальным мошенником на некоторое время. Дело в том, что, как правило, злоумышленники не ждут свою жертву несколько дней. Если вы увидели подозрительное объявление, не поленитесь уточнить у соседей, старшего по дому или в управляющей компании, действительно ли оно настоящее. А еще лучше – игнорируйте такие предложения, если у вас есть хоть малейшие сомнения.

17. Нужно быть особенно осторожными с просьбами о деньгах и предложениями услуг: всегда перепроверяйте информацию, задавайте уточняющие вопросы, а лучше всего – избегайте предоплат, особенно если предложение исходит от незнакомого человека.

18. Важно обращать внимание на тех, кто активно пытается привлечь внимание к срочным просьбам о помощи или срочным предложениям – мошенники часто манипулируют временем, чтобы не дать возможности все обдумать.

19. Важно загружать лишь официальные приложения для сдачи и аренды жилья. Любая просьба перейти на другой сайт под каким-либо предлогом должна стать поводом насторожиться – ведь в самом профильном приложении уже есть все необходимое для сдачи жилья, и создатели таких сервисов, зная о мошенниках, стараются защитить своих пользователей.

20. При сканировании QR-кодов необходимо проявлять такую же осторожность, как и при переходе по подозрительным ссылкам. Для тех, кто регулярно использует их, существуют специальные онлайн-декодеры, позволяющие предварительно проверить содержимое.

21. При инвестировании рекомендуется выбирать проверенных лицензионных брокеров. И если человек решит зайти вделку, начинать с 10% от капитала, не больше.

Любые финансовые предложения со стороны незнакомцев из сети «Интернет» или на другой стороне провода стоит автоматически считать мошенническими. Особенно если предлагается скачать стороннее приложение. Также стоит обратить внимание на схему оказания услуг: мошенники обычно просят проводить платежи через электронный кошелек или на карту, а не через банк-эквайер.

22. Предложение легкого и быстрого заработка должно вызвать у человека подозрения. Реальный работодатель будет платить за простую работу по рыночной стоимости.

23. Необходимо отказаться от любых предложений на оформление кредита по телефону. Мошенники будут применять психологические уловки, но стойте на своем: заявку не подавали, в заемных средствах не нуждаетесь, никакие данные по телефону передавать не будете. Однако в случае, если микрокредит таким образом все же оформлен, важно срочно обратиться в полицию с заявлением о мошенничестве и к юристу, который подскажет, как избежать проблем при взыскании «долга» с процентами.

При переводе средств от неизвестного лица лучше всего постараться узнать, от кого совершена операция. Также можно обратиться в свой банк, чтобы эту сумму вернули отправителю как переведенную ошибочно.

24. Распознать мошенническую точку Wi-Fi зачастую бывает весьма непросто. Стоит обратить внимание на имя сети. Если точка доступа принадлежат кафе или аэропорту, то у них есть соответствующие названия, но имена мошеннических сетей будут отличаться минимум на один символ. Это всегда необходимо проверять при подключении к общественному Wi-Fi.

В ситуации, когда вы видите много беспроводных сетей с похожими названиями в общественном месте, например, в кафе, необходимо обратиться к сотрудникам заведения и узнать точное название местного Wi-Fi, чтобы избежать проблем. Для того чтобы подключиться к мошеннической точке Wi-Fi, пользователям порой даже не нужно ничего делать. Порой злоумышленники создают поддельные Wi-Fi-сети, чтобы провести атаку типа Evil Twin («Злой близнец»).

Если точка Wi-Fi показалась вам подозрительной, лучше отключиться и запретить автоподключение к ней на устройстве. Затем следует поменять учетные данные на всех ресурсах, с которыми вы взаимодействовали по этой сети, а также проверить ваше устройство при помощи антивирусных программ.

При использовании общедоступных сетей Wi-Fi никогда нельзя указывать свои персональные данные. Рекомендуется взять за правило не использовать общественные точки доступа вне зависимости от того, защищены ли они паролями или нет. Если Вы уже подключились и что-то Вас насторожило, необходимо разорвать соединение, не вводить логины-пароли, не совершать оплату по карте и не переходить по ссылкам.

ДЛЯ ЗАМЕТОК

Взвешенное поведение – залог безопасности!

ГОРЯЧАЯ ЛИНИЯ
ДЛЯ КОНСУЛЬТАЦИИ РАБОТНИКОВ
ОАО «РЖД» ПРИ ПОСТУПЛЕНИИ
ПОДОЗРИТЕЛЬНЫХ ЗВОНКОВ
И СООБЩЕНИЙ

8 800 775 76 77