счет». Если накоплений у жертвы не оказалось, злоумышленники не останавливаются на этом и убеждают человека брать кредиты.

Еще один вариант схемы – просьба помочь в поимке преступников, которые якобы использовали счета жертвы для своих противоправных действий (например, обналичивания). Используя эту легенду, мошенники также убеждают человека перевести средства на «безопасный счет» или оформить кредит.

***Информация подготовлена с использованием открытых Интернет-ресурсов, в том числе*** ***https://моифинансы.рф***

ГОСУДАРСТВЕННЫЙ ИНФОРМАЦИОННЫЙ РЕСУРС В СФЕРЕ ЗАЩИТЫ ПРАВ ПОТРЕБИТЕЛЕЙ <http://zpp.rospotrebnadzor.ru/>



**На данном портале размещено:**

* нормативная правовая база в сфере защите прав потребителей;
* сведения о случаях нарушений требований технических регламентов с указанием конкретных фактов несоответствия продукции обязательным требованиям;
* результаты проверок,
* решения судов по делам в сфере защиты прав потребителей;
* новости в сфере защиты прав потребителей;
* тематические памятки по защите прав потребителей и обучающие видеоролики;
* образцы претензий и исковых заявлений;
* ВИРТУАЛЬНАЯ ПРИЕМНАЯ, где можно задать интересующий вопрос;
* ВЕРСИЯ ДЛЯ СЛАБОВИДЯЩИХ.

**Телефон Консультационного центра по защите прав потребителей: 8 (4112) 446158 ( с 09:00 ч. до 17:15 часов, кроме субботы и воскресенья, с перерывом с 13:00 ч. до 14:00 ч.) zpp@fbuz14.ru**

**Единый консультационный центр:**

**8 800 555 49 43  (круглосуточно и без выходных дней)**

****

**ФБУЗ «Центр гигиены и эпидемиологии в РС (Я)»**

**Отдел защиты прав потребителей**



**Памятка.**

**Мошенники! Самые распространенные схемы в 2024 году**

**г. Якутск**

Подавляющее большинство россиян сталкивались в 2024 году с мошенничеством – по разным опросам от 70 до 85%. За 9 месяцев ущерб от мошенников оценивается в 150 млрд рублей, а самих фактов стало на 25% больше, чем в 2023 году. Злоумышленники постоянно модернизируют старые схемы обмана.

**«Включите демонстрацию экрана»**

Для обмана людей мошенники выдают себя за сотрудников различных государственных ведомств – Мосэнергосбыта, ЖКХ, поликлиник и других. Легенды у злоумышленников самые разные: от необходимости восстановить доступ к ресурсам до оказания технической поддержки.

Во всех случаях они предлагают потенциальной жертве перейти в WhatsApp для видеозвонка. После этого мошенники сообщают о некой технической проблеме и просят включить демонстрацию экрана. После того, как собеседник соглашается выполнить это действие, ему отправляют ссылку на приложение и просят его скачать. Злоумышленники выдают приложение за официальный ресурс ведомства, но на самом деле это вредоносный вирус SpyMax. Установка псевдо-приложения полностью лишает человека контроля над смартфоном. В это же время на телефон приходит СМС с секретным кодом от входа в банковское приложение. Злоумышленники используют его для входа в онлайн-банк, после чего переводят на свои счета все доступные на счету средства либо оформляют от имени жертвы кредиты. Вернуть контроль над смартфоном человек самостоятельно уже не может, а потому самый верный способ не оказаться в числе обманутых – не общаться с незнакомцами, не переходить по их ссылкам и не устанавливать сторонние программы.

Ни одна государственная организация не звонит через мессенджеры, не просит включить демонстрацию экрана и не рассылает ссылки на установку приложений. При возникновении даже малейшего подозрения лучше прекратить звонок.

**«Вы выиграли приз!»**

Мошенники часто используют периоды сезонных распродаж для обмана людей. Ставка делается на то, что человек, услышав слова «приз» или «подарок», потеряет бдительность. Одна из самых популярных легенд связана с розыгрышем призов от популярных маркетплейсов.

Злоумышленники создают поддельные сайты, на которых якобы можно выиграть различные ценные призы: подарочные сертификаты, технику (смартфон, ноутбук, телевизор), а также путевки на море. Чтобы участвовать в «розыгрыше», нужно угадать, в какой коробке находится приз. Какую бы коробку человек ни выбрал, она всегда будет выигрышной. Задача мошенников – сбить жертву с толку щедрым подарком. Но, чтобы его заполучить, нужно заплатить обязательную «пошлину». Ставка делается на то, что человек согласится перевести незначительную в сравнении с выигрышем сумму. После перевода денег никакого приза человек не получает.

Распространена еще одна похожая схема с розыгрышем призов. Мошенники создают в Telegram специальные боты, которые предлагают покрутить «колесо удачи» в честь распродажи. Для получения подарка нужно ввести данные банковской карты или доступа в личный кабинет на маркетплейсе. Не стоит переходить по ссылке для участия в розыгрыше призов. Она может вести на сайт, который похож на популярные маркетплейсы. Если и участвовать в розыгрышах, то только на официальных площадках, которые хорошо знакомы.

**«Вам открытка»**

Этот вид обмана рассчитан, в первую очередь, на людей старшего возраста, которые привыкли рассылать друг другу открытки в мессенджерах. Вместо обычных картинок злоумышленники присылают своим потенциальным жертвам файлы с расширением gift.

При нажатии на изображение картинка загружается и становится доступной к просмотру. В это же время происходит заражение смартфона вредоносным кодом. Проникая в устройство, вирус собирает персональные данные владельца гаджета. В дальнейшем это может привести к потере денежных средств. Еще один вариант этой схемы – рассылка фотографий с расширением .apk в Telegram. Злоумышленники сопровождают файлы сообщением: «Привет, это ты на фото?». Если кликнуть на него, телефон окажется заражен вирусом, из-за чего злоумышленники могут получить доступ к личным данным, а значит, и к деньгам. Фотография не может иметь расширение .apk, а вредоносное программное обеспечение как раз может. Не стоит скачивать изображения, которые приходят в социальных сетях. Даже если отправитель известен, это не повод безоговорочно доверять таким сообщениям. Аккаунт может быть взломан мошенниками. Если есть желание посмотреть файлы, лучше предварительно уточнить у знакомого в другом мессенджере или по телефону, отправлял ли он файл или фото. Также стоит учитывать, что приятель, сам того не ведая, может переслать вредоносную картинку.

**«Отсканируйте QR-код»**

Схема «отправьте деньги на специальный счет» - не нова. Однако мошенники не устают переупаковывать эту легенду, чтобы она заработала с новой силой. На сей раз – с применением QR-кода.

Злоумышленники звонят по телефону и говорят, что они представители различных силовых или надзорных структур: прокуратуры, Следственного комитета, Федеральной налоговой службы и других. «Сотрудник» сообщает абоненту о том, что он якобы не задекларировал какие-то суммы. Чтобы их не конфисковали, необходимо отсканировать специальный QR-код, который приходит в мессенджер. Для убедительности его снабжают эмблемой ФНС или портала Гослуслуг.

Мошенники убеждают жертву, что по QR-коду необходимо отправить деньги на «специальный счет» либо перевести в бюджет «налоговые платежи».

Чтобы не попасть в подобную ситуацию, важно запомнить - сотрудники силовых структур и других ведомств (прокуратуры, Следственного комитета, ФНС, Социального Фонда…) общаются с гражданами при личном приеме в режиме офлайн. Если в мессенджере звонит человек и представляется сотрудником прокуратуры, это не кто иной, как мошенник.

**«Вы обвиняетесь в пособничестве терроризму»**

Еще одна тактика злоумышленников – запугать потенциальную жертву. Когда человек находится во власти эмоций, он может сделать ошибку, даже если знает правила финансовой безопасности.

Мошенники звонят по телефону или в мессенджерах и сообщают абоненту, что его обвиняют в каком-то преступлении – например, пособничестве терроризму. Чтобы «снять обвинение», нужно заплатить – перевести деньги на «безопасный