Нефтеюганская межрайонная прокуратура разъясняет:

«Мошенники стали обманывать детей в играх»

В автономном округе зафиксированы неоднократные факты хищений денежных средств **граждан путем обмана несовершеннолетних в компьютерных и мобильных играх.**

Несовершеннолетним от неустановленных лиц в онлайн играх (Roblox, Minecraft, CS:GO и др.) поступают сообщения о возможности получить преимущества (внутриигровую валюту, коллекционные предметы, бонусы в развитии персонажа) после предоставления данных банковских карт родителей и доступа к приложению банка или смс – уведомлениям от кредитных организаций.

В ряде случаев для получения необходимых сведений преступники убеждали несовершеннолетних переходить на сайты, специально созданные для хищения денежных средств.

После получения необходимых данных мошенники похищали находящиеся на банковских счетах денежные средства.

Правоохранительными органами принимаются меры по установлению совершивших преступления лиц.

В целях недопущения совершения хищений денежных средств **Нефтеюганская межрайонная прокуратура рекомендует провести с детьми беседу о безопасности в сети «Интернет» и исключить доступ несовершеннолетних к сведениям, которые могут быть использованы для совершения противоправных действий.**

«Внимание: мошенники под видом учителей!»

Злоумышленники звонят и говорят, что нужно «обновить» или «дополнить» информацию в электронном журнале или обновить профиль учащегося в системе «Сферум».

Ребенку или родителю приходит смс-код, который «псевдоучитель» просит сообщить для «подтверждения» операции.

Получив код, мошенники восстанавливают доступ на портале «Госуслуги» и получают доступ к личному кабинету портала.

Будьте бдительны и напоминайте об этом детям: никакой учитель не просит смс-код от портала «Госуслуги» или других онлайн-сервисов!

«Самозапрет на выдачу кредита (займа)»

Федеральным законом от 26.02.2024 № 31-ФЗ «О внесении изменений в Федеральный закон «О кредитных историях» и Федеральный закон «О потребительском кредите (займе)» **предусмотрено право физического**

лица с 1 марта 2025 года оформить заявление о внесении в свою кредитную историю сведений о запрете (либо снятии запрета) на заключение с ним договоров потребительского займа (кредита), за исключением отдельных видов кредитов (ипотека, автокредиты, образовательные кредиты, погашение действующих займов).

Для установления (снятия запрета) физическое лицо вправе бесплатно в любое количество раз подать соответствующе заявление во все квалифицированные бюро кредитных историй через МФЦ или с использованием Единого портала госуслуг.

Многофункциональный центр предоставления государственных и муниципальных услуг обязан обеспечить оказание услуги по внесению в кредитную историю сведений о запрете (снятии запрета) при обращении физического лица в МФЦ со дня доработки и настройки автоматизированной информационной системы, но не позднее 1 сентября 2025 года.

Информация о самозапрете или о его снятии будет внесена в кредитную историю в течении дня, если кредитное бюро получило соответствующее заявление до 22 часов 00 минут по московскому времени, если позднее – на следующий календарный день.

Запрет начинает действовать на следующий день после включения информации о нем в кредитную историю физического лица.

Снятие запрета начинает действовать на второй календарный день после включения информации о нем в кредитную историю физического лица.

Обязательное условие для получения услуги – наличие ИНН. Банки и МФО до заключения договора должны будут запросить у всех квалифицированных кредитных бюро информацию о наличии запрета у клиента на выдачу кредитов. Если запрет установлен, то кредитная организация или МФО должны будут отказать в услуге.

«Подписан закон о борьбе с кибермошенниками»

Федеральным законом от 01.04.2025 № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» **в рамках борьбы с телефонным мошенничеством устанавливается:**

- самозапрет на заключение договоров об оказании услуг связи без личного присутствия;
- запрет на передачу SIM-карт третьим лицам (кроме близких родственников);
- самозапрет на международные звонки, спам - обзвоны и рассылки;
- обязательная маркировка всех исходящих телефонных вызовов от организаций.

Сотрудникам госорганов, банков, операторов связи, цифровых экосистем запрещено общаться с гражданами и клиентами через иностранные мессенджеры.

В сфере финансового рынка, в частности, ужесточаются требования к идентификации заемщиков при оформлении микрозаймов в электронной форме.

Кроме того, устанавливается обязанность кредитной организации по ограничению выдачи наличных денежных средств с использованием банкоматов на сумму до 100 тысяч рублей в месяц, **если в соответствующей базе данных есть информация о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента.**

Любой человек сможет назначить **свое доверенное лицо, к которому кредитная организация будет обращаться за подтверждением операции по выдаче наличных или оформлению кредита.**

Кредитные организации, владельцев агрегаторов и операторов обязали предоставлять с использованием СМЭВ сведения, запрашиваемые оперативниками и органами ФСБ.

Закон вступает в силу с 1 июня 2025 г., за исключением положений, для которых предусмотрены иные сроки.

«Мошенническая схема с обновлением банковских карт»

Мошенники чаще стали похищать деньги, представляясь сотрудниками банка и призывая срочно обновить мобильное приложение.

Злоумышленники звонят и представляются сотрудниками банка, убеждая установить «правильную версию» приложения.

Они настаивают на немедленном обновлении, иначе счета и карты клиента могут быть заблокированы.

Затем мошенники присылают ссылку для скачивания обновления, которая ведет на специальный ресурс.

После перехода экран блокируется, давая злоумышленникам доступ к устройству, в том числе в личный кабинет банковского приложения.

Мошенники используют перехваченные смс-коды для вывода денежных средств со счета жертвы.

Не переходите по сомнительным ссылкам: скачивайте и обновляйте приложения только через официальные магазины - App Store или Google Play.

Не доверяйте неожиданным звонкам: банки не просят обновить приложение по телефону или через мессенджеры.

При любых сомнениях позвоните в банк по официальному номеру.

Если Вы уже перешли по подозрительной ссылке, немедленно обратитесь в банк и попросите временно заблокировать личный кабинет.

Будьте бдительны к подобным попыткам обмана!

«Осторожно, мошенники!»

Несмотря на многочисленные меры борьбы с мошенничеством в сети Интернет, всё же появляются новые способы обмана.

В настоящее время распространяется мошенническая схема, по которой злоумышленники звонят ученикам от лица администрации школы в целях "подтверждения доступа в электронный журнал".

Затем обманным путём преступники получают от ребёнка доступ к аккаунту МЭШ или порталу mos.ru.

Разъясните детям, что в случае поступления таких звонков следует немедленно прекратить разговор и сообщить об этом взрослым! Администрация школы не вправе запрашивать личные данные.

Не позволяйте мошенникам обмануть себя и ваших близких!

«С 1 апреля 2025 года введен лимит на количество сим-карт для абонентов»

Федеральным законом от 08.08.2024 № 303-ФЗ внесены изменения в Федеральный закон от 07.07.2003 № 126-ФЗ «О связи».

Так, физическому лицу может быть выделено операторами подвижной радиотелефонной связи и предоставлено в пользование абонентами – юридическими лицами либо индивидуальными предпринимателями в совокупности не более 20 абонентских номеров.

Законом установлены особенности оказания услуг подвижной радиотелефонной связи иностранным гражданам или лицам без гражданства, предусматривающие возможность предоставления в пользования не более 10 абонентских номеров.

Также на операторов связи возлагается обязанность проверять достоверность сведений об абоненте и о корпоративных пользователях до начала оказания им услуг.

Проверить количество заключенных договоров об оказании услуг связи можно с использованием единого портала государственных и муниципальных услуг.

«Ошибка в расчете размера пенсии как способ мошенничества»

Поступает звонок якобы от сотрудника Пенсионного фонда с сообщением о выявлении в ходе проверки исчисленного размера пенсии неучтенного трудового стажа и предложением написать заявление о ее перерасчете.

После чего, якобы для идентификации Вас как получателя пенсии, просят сообщить код из поступившего СМС-сообщения.

Если выполнить просьбу и сообщить код, мошенники получат доступ к личным кабинетам гражданина на сервисе Госуслуг или в банке, который используют в корыстных целях.

Исключите немедленную передачу кода.

Лучше уточните фамилию, имя, отчество, должность, точное место работы и наименование организации звонящего.

Прервите разговор.

Свяжитесь с названной им организацией по телефону, найдя его на официальном сайте Социального Фонда России или по известному вам номеру своего отделения Фонда и проверьте информацию.

«Набирает обороты «фишинг» - как способ мошенничества»

Набирает обороты «фишинг» - как способ мошенничества, заключающийся в направлении посредством интернет-сайтов, социальных сетей, адресов электронной почты ссылок на различные ресурсы, которые так или иначе заинтересовывают население, побуждая перейти по ним.

В переводе с английского «фишинг» означает «рыбалка». Но для злоумышленников граждане не рыбаки, а рыба, которую можно поймать на крючок и использовать по своему усмотрению.

Чем же заинтересовывают?

Например, гарантируют получение приза от маркетплейса или скидки от любимого магазина, увеличение пенсионных начислений и других социальных выплат или дополнительный доход от какой-либо деятельности.

При переходе по ссылке, как правило, предлагают заполнить персональные данные, в т.ч. реквизиты банковских карт, что открывает мошенникам доступ к управлению имеющимися у гражданина банковскими продуктами (счетами, кредитами, ипотекой) или оформить их на него.

Каждому должно быть понятно, что передавать свои персональные данные неизвестным лицам опасно.

Государственные органы и банки никогда не запрашивают такие сведения посредством мессенджеров, социальных сетей или электронной почты.

Критически оценивайте поступающую информацию!

«Внимание! Распространенные схемы мошенничества»

Фишинговые атаки через мессенджеры и социальные сети:

• Мошенники отправляют сообщения со ссылками, ведущими на сторонние ресурсы. Чтобы воспользоваться интересующей информацией предлагают внести персональные данные - логины, пароли, данные банковской карты.

Использование поддельных сайтов маркетплейсов:

• Создаются копии известных интернет-магазинов. Покупатели переводят деньги за несуществующий товар и не получают заказ.

Звонки от «сотрудников банка»:

• Лжесотрудники банков и правоохранительных органов сообщают о «подозрительных операциях» и предлагают перевести деньги на «безопасный» счет.

Поддельный QR-код:

• Мошенники размещают поддельные QR-коды в различных местах, например, на парковках или квитанциях об оплате услуг, сканирование которых может привести к установке вредоносного программного обеспечения, или утечке персональных данных.

Ложные сообщения о компенсациях и выплатах:

• «Жертве» предлагают компенсацию или социальные выплаты, требуя предварительный платеж «за оформление».

Взлом аккаунтов в социальных сетях и требование выкупа:

• Получив доступ к личным страницам пользователей сети «Интернет», злоумышленники требуют деньги за их восстановление. Однако, выплата денег не гарантирует восстановление доступа к аккаунтам.

Как защитить себя:

• Не переходите по подозрительным ссылкам.

• Проверяйте достоверность информации через официальные источники.

• Прежде, чем приобрести товар, убедитесь, что находитесь на официальном сайте организации путем сличения всех знаков его адреса в браузерной строке.

• Знакомьтесь с отзывами об организации.

• Не сообщайте личные данные незнакомцам, кем бы они не представились.

• Используйте для защиты сложные пароли и двухфакторную аутентификацию.

• Помните, что настоящие работники банков и правоохранительных органов не информируют граждан о финансовых угрозах и не предлагают перевести деньги на «безопасный счет».

• Знайте, социальные организации не требуют предоплату за выплаты.

«Незаконная передача средств платежа – преступление»

Многим не раз доводилось видеть объявления или слышать предложения о покупке «пустых» банковских карт, оформленных на себя с передачей средств платежа, позволяющих воспользоваться картами, или просто продать данные собственной карты и банковских приложений.

Продать банковскую карту и средства платежа для управления ею – фатальная ошибка.

В дальнейшем они могут использоваться для реализации мошеннических схем, в том числе с кредитами, субсидиями или пособиями, вывода похищенных денег, продажи наркотиков и даже финансирования терроризма.

Для этих целей злоумышленники приобретают у обычных граждан за небольшие деньги банковские карты, ПИН-коды, электронные логины и пароли для банковских приложений и иные средства для приема, перевода или выдачи денежных средств.

Большинство продающих средства платежа считают, что они ничего противозаконного не делают, так как сами никаких преступлений с их использованием не совершают. Однако, согласно банковским правилам пользоваться картой может только ее владелец.

В отношении формальных владельцев банками могут быть применены меры внутреннего контроля, позволяющие отказать в совершении в том числе добросовестных операций, а потерпевшие от мошеннических действий могут предъявить к «продавцу» гражданский иск о взыскании неосновательного обогащения, ведь именно на нее перечисляются похищенные денежные средства.

За неправомерный оборот средств платежа, в т.ч. продажу карты, установлена уголовная ответственность. Максимальное наказание - 7 лет лишения свободы со штрафом 1 млн. руб.

Знайте об этом и не помогайте преступникам обманывать граждан и государство.

«Как отличить поддельный сайт»

Растет популярность онлайн-платежей, а вместе с нею число мошеннических действий в сети.

Один из самых распространенных видов мошенничества - создание сайтов-двойников.

Внешне они очень похожи на официальные сайты банков, государственных органов, платежных систем или онлайн-магазинов, в

т.ч. веб-страниц по продаже авиабилетов, турпутёвок, мест в гостиницах и санаториях.

Цель мошенников - получить доступ к личным данным или финансовым аккаунтам пользователей, чтобы использовать их в своих целях.

Часто такие сайты-двойники имеют похожий с настоящим сайтом дизайн и структуру изложения материала, а также похожие доменные имена.

Значит надо научиться распознавать их.

Прежде чем приобрести товар онлайн и вводить персональные данные проверьте адрес сайта в верхней строке браузера. Убедитесь, что он начинается с английских букв и знаков «https://» и имеет пиктограмму замка, которая гарантирует безопасную передачу информации.

- Сверьте каждый знак адреса, возможно обнаружите замену одной буквы на другую или дополнительный символ.
- Обратите внимание на дизайн сайта и его содержание. Поддельный сайт, как правило, имеет некачественный дизайн и грамматические ошибки в текстах.
- Найдите в поисковых системах, например, «Яндекс», «Гугл» или на официальных форумах отзывы. Обычно люди делятся своим опытом попадания на мошенников и предупреждают о поддельных сайтах.
- Сравните цены на товар и условия продажи на нескольких сайтах. Слишком низкая цена -признак, отличающий мошенников.
- Получив электронное письмо со ссылкой на сайт, который вы не знаете, не переходите по ней. Лучше вручную введите адрес сайта в поисковую строку браузера.
- Если веб-сайт представляет собой онлайн-магазин или компанию, убедитесь, что на нем представлены наименование юридического лица или индивидуального предпринимателя, адрес регистрации и фактический адрес организации, реквизиты расчетного счета.
- Настоящие сайты обычно имеют дополнительные функции безопасности, такие как возможность создания пользователем учетной записи с логином и паролем, опции настройки приватности, позволяющие задать правила и ограничения для доступа к персональным данным.

Разумная осторожность еще никому не повредила.

«Поручение руководителя как способ мошенничеств»

Мошенники в мессенджерах WhatsApp, Telegram и других создают аккаунт, визуально похожий на аккаунт руководителя и направляют подчиненным сообщения, например, о необходимости ответить на звонок из полиции по указанному телефону.

Поверивший и выполнивший поручение узнает историю об угрозе утраты собственных денег с предложением перевести их на «безопасный счет», который тут же и назовут.

Так поступают мошенники. Звоните руководителю, проверяйте информацию.

«Продажа банковской карты уголовно наказуема»

Многим не раз доводилось видеть объявления или слышать предложения о покупке «пустых» банковских карт, оформленных на себя с передачей данных, позволяющих воспользоваться ими или просто продать данные собственной карты.

Для использования карты мошенникам необходимо знать пин-код, трехзначный проверочный код на ее обороте, необходимый для совершения банковских операций, срок ее действия, пароль личного кабинета в интернет-банке, последние 3 или 4 цифры номера карты.

Продать банковскую карту, зарегистрированную на свое имя или ее данные – фатальная ошибка, потому что в дальнейшем они используются мошенниками для перевода и обналичивания полученных криминальным путем денег.

Например, приобретенную карту или ее данные мошенники могут использовать для подключения к финансовой пирамиде, реализации схем с кредитами, субсидиями или пособиями, обмана сервисов, заблокировавших преступника, обмана с электронными платежами и страховками, получения переводов от жертв мошеннических схем, вывода денег, украденных в интернет-банке и из электронных кошельков.

Результаты прокурорского надзора свидетельствуют, что чаще всего в незаконные финансовые операции с использованием банковских карт вовлекаются студенты различных учебных заведений.

Согласно банковским правилам пользоваться картой может только ее владелец.

В отношении формальных владельцев банковских карт, т.е. тех кто продал карту или ее данные и реально не распоряжается ею, банками могут быть применены меры внутреннего контроля, позволяющие отказать в совершении собственных финансовых операций или в заключении договора банковского счета.

За неправомерный оборот средств платежа, в т.ч. продажу карты, установлена уголовная ответственность. Максимальное наказание - 7 лет лишения свободы со штрафом 1 млн. руб.

Кроме того, потерпевшие от мошеннических действий могут предъявить к продавшему карту гражданский иск о взыскании неосновательного обогащения, ведь именно на нее перечисляются похищенные денежные средства.

Остерегайтесь подобных сделок и предупредите об этом своих близких.

«Ложный звонок от нотариуса как способ мошенничества»

Поступает звонок от якобы нотариуса, сообщающего об оформлении сейчас на ваше имя кредита по ранее подписанной доверенности.

Возмущенный абонент отвечает, что никаких доверенностей он не выдавал, после чего ему предлагают позвонить в полицию и разобраться, диктуют номер телефона для связи.

Действительно, по указанному номеру отвечает человек, представляющийся сотрудником полиции, и предлагает срочно опередить мошенников, самим оформить кредит на себя и перевести деньги на «защищенный счет».

Те, кто поверит и выполнит команды, своими руками переведут деньги мошенникам.

Чтобы не попасть в подобную ситуацию, знайте:

- без вашего личного присутствия ни один настоящий нотариус не оформляет какие-либо документы;

- «защищенные или безопасные счета» принадлежат мошенникам;

- любую информацию об угрозе потерять деньги или имущество надо проверять.

Вступив в разговор, уточняйте:

- фамилию, имя, отчество, должность, точное место работы и наименование организации звонящего;

- источник его информации о вас и наличии ваших персональных данных;

- в каком банке идет оформление кредита и где он находится. :

В сети Интернет найдите официальные сайты МВД, Нотариата, Банка, проверьте по имеющимся в них контактным номерам полученную информацию.

«Продление договора с сотовым оператором как способ мошенничества»

Очень простой, но, к сожалению, действенный способ мошенничества.

По телефону поступает звонок от якобы представителя оператора сотовой связи с сообщением об окончании срока действия вашего договора о предоставлении услуг связи и необходимости его продлить, что можно сделать дистанционно, если вы продиктуете оператору код из поступившего СМС-сообщении.

Многие, не задумываясь, соглашаются и теряют деньги.

На практике передача кода неизвестному означает получение мошенником доступа к вашему личному кабинету на портале Госуслуг, что позволяет завладеть большим объемом хранящихся там персональных данных, в т.ч. паспортных.

После этого он сможет, например, оформить на вас кредит, переведя деньги на свой счет или продать вашу недвижимость.

Получив такое сообщение, знайте, договор о предоставлении услуг сотовой связи является бессрочным и не требует продления, откажитесь от предложения.

Позвоните своему сотовому оператору по номеру телефона, указанному на его официальном сайте, проверьте информацию.

«Попытка оформить кредит от вашего имени как способ мошенничества»

Один из самых распространенных способов мошенничества выглядит следующим образом.

Представляясь якобы сотрудником службы безопасности банка, Центрального банка России, полиции или иного государственного органа, по телефону сообщают, что сейчас мошенники пытаются оформить на вас кредит и похитить деньги.

Чтобы помешать этому и поймать мошенников, предлагают опередить их и срочно самим оформить кредит, переведя полученные деньги на «безопасный» или «защищенный» счет.

Поверив и выполнив предложенные действия, в т.ч. перевод денег на продиктованный счет, Вы своими руками отдадите их мошеннику, потому что счет принадлежит ему.

Получив подобную информацию, уточните фамилию, имя и отчество говорящего, его должность и официальное наименование организации, которую он представляет, наименование кредитной организации, оформляющей на вас кредит и ее местоположение.

Выясните, откуда к нему поступила такая информация.

Прекратите разговор.

В сети Интернет на официальном сайте названной организации найдите контактный телефон и выясните, работает ли в ней ваш собеседник, давалось ли ему поручение связаться с вами и в связи с чем.

Позвоните в свой банк по телефону, указанному на оборотной стороне карты или на его официальном сайте в сети Интернет, проверьте сохранность сбережений.

Позвоните в указанный собеседником банк и проверьте информацию об оформлении на вас кредита.

Помните! Банк может инициировать общение с клиентом только для консультации по предложению собственных услуг.

Настоящие сотрудники полиции или иных государственных органов не уполномочены делать подобные предложения гражданам по телефону.

Исключите передачу кому-либо персональных данных.

Внимание: мошенники притворяются работодателями

Злоумышленники размещают в сети «Интернет» фальшивые объявления о вакансиях. Используют привлекательные условия труда и высокую зарплату.

Насторожитесь, если в объявлении:

- Подозрительно выгодные условия;
- Легкость заработка;
- Недостаточно информации и отзывов о работодателе.

Мошенники проводят собеседования по телефону или видеозвонку, что создает иллюзию правдивости. В беседе они делают вид, что вы – лучший кандидат на должность.

Киберпреступники выпрашивают ваши данные паспорта и СНИЛС будто бы для оформления на работу. Требуют реквизиты банковской карты, якобы для перевода аванса, зарплаты.

На самом деле их цель – украсть с вашей банковской карты деньги.

Вам приходит смс-сообщение и «работодатель» просит назвать код из него для подтверждения заявки на работу, но данные коды позволяют злоумышленникам сделать перевод или оплату с банковского счета либо получить доступ на портал «Госуслуги».

Относитесь скептично к предложениям, которые кажутся слишком хорошими, чтобы быть правдой. Проверяйте компанию работодателя перед тем, как откликнуться на вакансию.

Не передавайте личные данные или банковскую информацию до подписания договора с работодателем. Не сообщайте коды из смс-сообщений и используйте проверенные ресурсы для поиска вакансий!

«Внимание: активизируются киберпреступники»

Популярные схемы:

Фейковые знакомства – мошенники создают ложные профили в социальных сетях и на сайтах знакомств, разыгрывают вспыхнувшие чувства и в итоге выманивают денежные средства.

Ложные сайты доставки цветов и подарков – предлагают «скидки и эксклюзивные букеты», но после оплаты заказа прекращают общение. Фишинговые акции и скидки – предложения якобы от известных брендов, которые приведут вас на сайты, похищающие персональные данные или распространяющие вредоносное ПО.

Доставка цветов от «неизвестного поклонника», предназначенная для выманивания смс-кода и получения неправомерного доступа к «Госуслугам» и иным личным аккаунтам.

Будьте внимательны и осторожны!

«Как мошенники предлагают продлить полис ОМС»

Злоумышленники придумали новую схему мошенничества, в основном для обмана пенсионеров и инвалидов.

Мошенники звонят под видом сотрудников страховых компаний и сообщают о необходимости продления полиса ОМС.

Для дистанционного обновления предлагают скачать приложение Минздрава, которое на самом деле фейковое и позволяет получить удаленный доступ к смартфону, а также интернет-банку и порталу «Госуслуги».

Если поступил такой звонок, незамедлительно прекращайте разговор и перезвоните в службу поддержки вашей страховой компании, чтобы уточнить всю необходимую информацию.

«Внимание: Схема мошенничества с виртуальным образом карты»

Мошенники звонят человеку по телефону или через мессенджер и сообщают, что его денежные средства якобы пытаются похитить.

Для решения проблемы по «хищению» необходимо установить фейковое приложение Центрального Банка Российской Федерации.

Затем злоумышленники просят запустить приложение и ввести код подтверждения от банка якобы для авторизации. Именно так мошенники получают необходимые им данные карты.

Приложение, которое просят установить мошенники, создаёт виртуальный образ банковской карты жертвы, который злоумышленники используют для снятия денежных средств в банкоматах, поддерживающих бесконтактную технологию.

Таким образом, вместо банковской карты человека мошенник прикладывает к банкомату свой смартфон.

Не скачивайте приложения по просьбе незнакомых людей и не сообщайте никому свои персональные данные!

«Внимание: Мошенническая схема с обновлением банковских приложений»

Мошенники начали чаще похищать деньги, представляясь сотрудниками банка и призывая срочно обновить мобильное приложение.

Злоумышленники звонят и представляются сотрудниками банка, убеждая установить «правильную версию» приложения.

Они настаивают на немедленном обновлении, иначе счета и карты клиента могут быть заблокированы.

Затем мошенники присылают ссылку для скачивания обновления, которая ведет на специальный ресурс.

После перехода экран блокируется, давая злоумышленникам доступ к устройству, в том числе в личный кабинет банковского приложения.

Мошенники используют перехваченные смс-коды для вывода денежных средств со счета жертвы.

Не переходите по сомнительным ссылкам: скачивайте и обновляйте приложения только через официальные магазины – App Store или Google Play.

Не доверяйте неожиданным звонкам: банки не просят обновлять приложение по телефону или через мессенджеры.

Свяжитесь с банком самостоятельно: при любых сомнениях позвоните в банк по официальному номеру, указанному на вашей карте или на официальном сайте банка.

Блокируйте доступ при подозрениях: если вы уже перешли по подозрительной ссылке, немедленно обратитесь в банк и попросите временно заблокировать личный кабинет.

Берегите свои финансы и будьте бдительны к подобным попыткам обмана!

«Мошенники имитируют сайты служб доставки»

Новая схема мошенничества: поддельные уведомления от служб доставки. Злоумышленники начали притворяться популярными сервисами доставки, чтобы получить доступ к вашим личным данным и украсть деньги со счетов.

Сначала вы получаете ложное сообщение о том, что ваш заказ готов к отправке, хотя вы ничего не заказывали.

В последующем приходит смс-сообщение с предложением отследить посылку, чтобы узнать детали отправления. В данном сообщении находится ссылка на интернет-ресурс.

Не спешите переходить по ссылке из сообщения, поскольку ссылка ведет на фишинговый сайт, который очень похож на официальный сайт служб доставки (СДЭК, СберМаркет, Яндекс Доставка и др.).

Однако, если вы перейдете по ссылке, вас обяжут ввести номер банковской карты, паспортные данные либо логин и пароль от банковского приложения.

Получив такие данные, мошенники списывают все ваши деньги со счета на банковские счета дропперов.

Не переходите по подозрительным ссылкам из сообщений, особенно если вы не ожидаете доставок.

Проверяйте отправителя сообщений, убедитесь, что сообщение пришло с официального номера или аккаунта службы доставки.

Не вводите личные данные на сайтах, перешедших по ссылкам из сообщений.

Если у вас есть сомнения, позвоните в службу поддержки официального сервиса доставки либо воспользуйтесь личным кабинетом в официальном приложении или на сайте службы доставки.

В условиях роста подобных преступлений в отношении граждан будьте бдительны и предупреждайте своих близких о новых видах мошенничества!

«Мошенники и обманывают граждан через Telegram»

Мошенники под видом службы поддержки мессенджера Telegram похищают аккаунты граждан.

Злоумышленники присылают гражданам сообщения, создавая для этого секретный чат, который нельзя удалить, с невозможностью сделать скриншот либо переслать сообщение модератору.

«Псевдоподдержка» Telegram пишет пользователю в сообщении о том, что поступил запрос на удаление учётной записи в мессенджере и для отмены запроса надо перейти по специальной ссылке, в противном случае учётная запись будет удалена.

Данная ссылка в таком сообщении фишинговая: введя логин и пароль от своего аккаунта, гражданин самостоятельно передает доступ к нему мошенникам.

Настоящая служба поддержки мессенджера не создает секретных чатов. Будьте внимательны!

«Новые способы мошенничества с использованием искусственного интеллекта»

Мошенники научились подделывать аудио- и видеосообщения владельцев взломанных аккаунтов.

Злоумышленники с помощью искусственного интеллекта подделывают видео- и голосовые сообщения владельца аккаунта, чтобы от его имени просить денежные средства у родных и близких.

При этом внимательно изучаются переписки владельца аккаунта, чтобы все «просьбы» имели правдоподобный эффект.

Распознать «дипфейк» можно по неестественной монотонной речи собеседника, дефектам звука и видео или несвойственной мимике.

Не реагируйте на такие сообщения в мессенджерах и социальных сетях, перезвоните близкому человеку по сотовой сети самостоятельно. Если не удалось дозвониться, задайте в сообщении личный вопрос, ответ на который знает только ваш собеседник.

Не спешите переводить деньги!

«Мошенники массово начали взламывать домовые чаты»

Злоумышленники развешивают в подъездах объявления о создании нового «домового чата». Якобы в указанном чате можно найти сведения по вопросам ЖКХ и общаться с соседями.

Жертва проходит по фальшивому QR-коду, и доступ к аккаунту в Telegram оказывается в руках у мошенников.

QR-коды позволяют злоумышленникам получать доступ к учетным записям и связанным с ними каналам.

После сканирования такого кода у пользователя на мобильном устройстве откроется Telegram и появится сообщение о подключении стороннего устройства. Если установлена двухфакторная аутентификация, то мессенджер запросит пароль.

После этого злоумышленникам станут доступны все контакты и переписка.

В данном случае мошенники рассчитывают на невнимательность и невысокую цифровую грамотность граждан.

Для того чтобы избежать кражи учетной записи, рекомендуем установить двухфакторную аутентификацию в мессенджере и внимательно перепроверять ресурсы, куда их перенаправляет QR-код.

Будьте внимательны, предупредите родных и близких!

«Мошенники вымогают денежные средства»

Злоумышленники представляются известными блогерами, поэтому несовершеннолетние доверяют мошенникам и переводят денежные средства.

Мошенники часто используют различные методы, чтобы обмануть детей и подростков, предлагая им «доступ» к игровым ресурсам или эксклюзивному контенту в обмен на деньги.

Защита детей от онлайн-мошенников становится все более актуальной задачей для родителей, особенно в свете растущего числа мошеннических схем, направленных на молодежь в играх и социальных сетях.

Несколько ключевых мер, которые могут помочь родителям обеспечить безопасность своих детей в интернете:

- Объясните риски: родители должны объяснить детям, какие схемы мошенничества существуют и как их распознать.

Важно, чтобы дети знали, что не следует переходить по ссылкам от незнакомцев или вводить личные данные на подозрительных сайтах.

- Обсуждение онлайн-активности: регулярные беседы о том, что происходит в играх и социальных сетях, помогут детям чувствовать себя комфортно, делясь с родителями своими переживаниями и подозрениями.

- Родительский контроль: установите программы родительского контроля, которые помогут ограничить доступ к нежелательным сайтам и

приложениям. Это также может включать ограничения на покупки в приложениях.

- Антивирусное ПО: убедитесь, что на всех устройствах установлено надежное антивирусное программное обеспечение, которое может защитить от вредоносных программ и фишинговых атак.

- Отдельные банковские карты: привяжите к игровым аккаунтам отдельные банковские карты с ограниченной суммой, чтобы минимизировать риски в случае мошенничества.

- Мониторинг расходов: регулярно проверяйте банковские выписки и транзакции, чтобы быстро выявлять подозрительные операции.

- Создание доверительных отношений: важно, чтобы дети чувствовали, что могут обратиться к родителям за помощью, если столкнутся с подозрительными ситуациями. Поддерживайте открытость в общении, чтобы дети не боялись делиться своими проблемами.

- Поощрение отчетности: поощряйте детей сообщать о любых подозрительных действиях или предложениях, которые они получают в интернете. Это поможет им развить навыки критического мышления и осторожности.

- Установите правила: создайте «контракт» с детьми, в котором будут прописаны правила безопасного поведения в интернете, включая запреты на общение с незнакомцами и переход по подозрительным ссылкам.

Эти меры помогут родителям защитить своих детей от онлайн-мошенников и создать безопасную среду для их цифрового взаимодействия.

«Мошенники стали использовать самозапрет для обмана жителей Югры»

Жителям Югры стали поступать звонки от якобы сотрудников портала Госуслуг, бюро кредитных историй (БКИ).

Они предлагают «помощь» в установке самозапрета или исправлении технической ошибки в процессе установки. Для этого нужно перейти по направленной ссылке.

Ссылка, как правило, ведет на поддельный сайт Госуслуг.

Если человек укажет там данные для входа на госпортал, мошенники перехватят их и сами попадут в его личный кабинет.

«Получив доступ к аккаунту человека, киберпреступники используют всю личную информацию, которая там хранится, в других мошеннических схемах.

В частности, могут авторизоваться в приложении банка с помощью «Госуслуг», а затем списать деньги со счетов.

Кроме того, по ссылке может находиться файл с вирусом. Если его скачать, то преступники получат все данные с устройства с секретными кодами».

Напоминаем, работники Госуслуг, БКИ, банков не звонят гражданам по поводу «некорректных» самозапретов и не присылают никаких ссылок.

Это делают только мошенники! Никогда не сообщайте незнакомцам личные данные, любые коды, пароли и не переходите по ссылкам от неизвестных адресатов.

«У вас неправильно установлен самозапрет на кредиты»

Не обошли мошенники вниманием и главную антимошенническую меру — самозапрет на получение кредитов.

Сценарий простой: гражданину звонят от лица Госуслуг и уточняют, активировал ли он запрет.

Если человек отвечает «да», то ему сообщают, что запрет установлен неверно — например, работает только для одного банка или не охватывает онлайн-займы.

Дальше идут варианты: предложат продиктовать код из СМС, включить демонстрацию экрана и «исправить» настройки запрета на Госуслугах, либо перейти по фишинговой ссылке для оформления нового запрета.

«Поддельная аренда самокатов и велосипедов»

Появились первые пострадавшие от новой схемы: на самокаты и велосипеды мошенники наклеивают фальшивые QR-коды.

Они ведут не в официальное приложение аренды, а на поддельные сайты, откуда скачивается вредоносное ПО.

Установленное приложение маскируется под настоящее, перехватывает управление телефоном или получает доступ к банковским данным.

Особенно уязвимыми становятся подростки, которые не всегда вникают в детали, а хотят побыстрее взять в аренду велосипед или самокат.

Будьте внимательны, предупредите родных и близких!

«Злоумышленники звонят от имени руководства»

Сложные схемы набирают обороты: если раньше мошенники руководствовались принципами массовости, но простоты, то теперь готовятся дольше и бьют точнее.

Злоумышленники звонят от имени руководства компании и сообщают, что в отношении работодателя проводится проверка (например, со стороны Прокуратуры или Налоговой).

Могут даже прислать «официальный» документ. Все это — подготовка к следующему звонку от «правоохранительных органов».

Дальше в ход идут сценарии: переводы «для проверки», передача данных от Госуслуг, доступ к банковским приложениям.

Цель — убедить сотрудника, что он помогает следствию, а не становится соучастником.

Будьте внимательны, предупредите родных и близких.

«Осторожно, новая схема мошенников!»

Злоумышленники звонят человеку под видом работников поликлиники и предлагают пройти диспансеризацию.

Затем они просят назвать код из SMS, чтобы записать жертву на обследование. Так злоумышленники получают доступ к аккаунту на «Госуслугах».

Затем человеку звонит другой мошенник, который представляется сотрудником сервиса и сообщает о взломе. Он дает жертве фальшивый номер «службы поддержки» – усыпляя бдительность человека, злоумышленники водят его по разным якобы ведомствам и в конце концов доводят до фейкового Росфинмониторинга.

Тогда мошенники просят заполнить заявление и прикрепить фото банковских карт. С них они потом крадут деньги.

Будьте бдительны!!!

Записаться на диспансеризацию можно только самостоятельно — на «Госуслугах» или в регистратуре поликлиники.

«Особенности предупреждения преступлений, связанных с использованием современных информационно-телекоммуникационных технологий»

Основными видами преступлений в сфере информационно-телекоммуникационных технологий являются дистанционные кражи и мошенничества денежных средств с банковских счетов граждан.

Соблюдение требований информационной защиты – наиболее эффективный способ по предупреждению данных видов преступлений, в связи с чем, необходимо руководствоваться следующими правилами:

- при использовании Интернет-ресурсов не переходите по сомнительным ссылкам, поскольку преступники создают сайты-двойники, которые могут похитить личные данные пользователя, в т.ч. и платежные сведений.

- принять во внимание, что сотрудники банков не звонят при сомнительных операциях, а сотрудники правоохранительных органов не просят перевести денежные средства на безопасный счет.

- в случае поступления звонков от лже-знакомого (или родственника) о попадании в трудную жизненную ситуацию, принимать меры к проверке достоверности полученной информации или позвонить родственнику и задать любой вопрос, связанный с вашим знакомством.

- ограничить покупку товаров через интернет-площадки через посредников, а в случае использования последних, выбирать только проверенные сервисы.

- не передать свои технические устройства незнакомым или малознакомым лицам, не сообщать пароли и коды доступа от банковских приложений или портала «Госуслуги».

- не поддаваться ложным призывам о помощи незнакомым людям.