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.

Порядок пенсионного обеспечения граждан, прибывших из новых регионов России

С 1 марта 2023 года на территориях Донецкой и Луганской Народных Республик, Запорожской и Херсонской областей пенсионное обеспечение граждан Российской Федерации, иностранных граждан и лиц без гражданства осуществляется в соответствии с законодательством Российской Федерации.

При обращении за назначением и пересмотром пенсий и (или) иных выплат в период с 01.03.2024 по 31.12.2025 они устанавливаются на 12 месяцев раньше дня, когда подано соответствующее обращение, но во всех случаях не ранее чем со дня возникновения права на пенсию и (или) выплату.

Для назначения и пересмотра пенсии необходимо подтверждение постоянного проживания на территории новых субъектов Российской Федерации.

При этом с 01.07.2025 вступают в силу изменения, согласно которым гражданам РФ, которые имели периоды работы и (или) иной деятельности на территории Украины и (или) территориях Донецкой и Луганской Народных Республик, работа будет учитываться без подтверждения проживания в названных субъектах.

В случае, если гражданин не имеет возможности подтвердить периоды работы или иной деятельности, они могут быть установлены на основании решения межведомственных комиссий территориальных органов Социального Фонда России.

Если указанным лицам назначены пенсии в соответствии с законодательством РФ до 01.03.2023 они могут претендовать на перерасчет их размера.

Соответствующее заявление подается в территориальные органы Социального фонда России, в т.ч. посредством портала государственных услуг или через МФЦ.

В случае несогласия принятые решения обжалуются вышестоящим должностным лицам в порядке подчиненности, в органы прокуратуры или в суд.

Мы не рыба, которую мошенники ловят на крючок

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!

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.

Новые обязанности банков по защите клиентов от мошенников

В целях защиты клиентов от мошенников внесены следующие изменения в ФЗ «О банках и банковской деятельности, вступающие в силу с 01.09.2025, обязывающие кредитные организации:

- в случаях, предусмотренных законами, предоставить органу, осуществляющему оперативно-разыскную деятельность или обеспечение безопасности РФ, запрошенные сведения с использованием единой системы межведомственного электронного взаимодействия;

- до выдачи наличных со счетов с использованием банкомата осуществить проверку наличия добровольного согласия клиента, имеющего платежную карту (признаки отсутствия такого согласия устанавливаются Банком России и размещаются на его официальном сайте). При наличии таковых на 48 часов с момента направления запроса на выдачу денег ограничить ее суммой не более 50 тыс.руб. в сутки и незамедлительно уведомить клиента о причинах ограничения;

- при получении из базы данных Банка России информации, относящиеся к клиенту и (или) его электронному средству платежа о случаях и попытках осуществления переводов денежных средств без его добровольного согласия, ограничить выдачу наличных денежных средств с использованием банкоматов на сумму не более 100 тысяч рублей в месяц, на период нахождения сведений в указанной базе данных;

- использовать иностранные мессенджеры для звонков и сообщений клиентам;

- при предъявлении доверенности на получение от имени клиента наличных денежных средств зафиксировать данный факт и обеспечить хранение копии такой доверенности в течение 5 лет с даты предъявления или выдачи наличных денежных средств;

- обеспечить клиенту - физическому лицу по соглашению с кредитной организацией и уполномоченным им лицом возможность подтверждать совершение операции по переводу денежных средств с банковских счетов (вкладов) клиента в пользу третьих лиц, получению наличных денежных средств с них, в том числе с использованием банкомата;

- обеспечить клиенту право выбора операций по переводу денег, а также банковских счетов, операции по которым требуют подтверждения уполномоченного лица;

- незамедлительно, в порядке, определенном соглашением, отправлять уведомления уполномоченному лицу;

- приостановить прием к исполнению распоряжения клиента - физического лица при совершении операции по переводу денежных средств (за исключением операции по переводу денежных средств с использованием платежных карт или сервиса быстрых платежей платежной системы Банка России) до момента получения подтверждения совершения операции по переводу денежных средств от уполномоченного лица; отказать клиенту в совершении операции по переводу денежных средств с использованием платежных карт или сервиса быстрых платежей платежной системы Банка России либо в совершении операции по получению наличных денежных средств, если соответствующая операция относится к операции, требующей подтверждения уполномоченным лицом;

- в местах оказания услуг (в том числе на своем официальном сайте в сети «Интернет» и в мобильном приложении (при его наличии) размещать информацию о праве клиента на основании соглашения наделить лицо статусом уполномоченного лица для получения подтверждения совершения таким клиентом операции по переводу денежных средств или операции по получению наличных денежных средств, о порядке наделения лица статусом уполномоченного лица и лишения лица этого статуса, требованиях к уполномоченному лицу и об условиях осуществления им своих полномочий, о стоимости услуг кредитной организации за информирование уполномоченного лица и клиента о подтверждении (либо об отклонении) соответствующей операции уполномоченным лицом либо о безвозмездности такого информирования.

Подтверждение или отклонение операции должно быть направлено уполномоченным лицом не позднее 12 часов, если более короткий срок не будет установлен соглашением.

Одновременно законом запрещено сотрудникам госучреждений, банков и операторов связи использовать иностранные мессенджеры для звонков и сообщений клиентам.

Продавцам на маркетплейсах предоставлено право пройти верификацию через Госуслуги и получить специальную отметку, что позволит покупателям быть уверенными в надежности поставщиков.

Сервису «Госуслуги» запрещено отправлять сообщения пользователям для входа в аккаунт во время телефонного разговора. Код доступа будет поступать после его завершения, что исключит возможность для злоумышленников удерживать внимание абонента и требовать назвать код из СМС.

Гражданам предоставлена возможность на Госуслугах и в МФЦ запретить заключение договоров связи без личного присутствия.

Осторожно, мошенники!

Прокуратура Нижнего Новгорода напоминает, что сотрудники банков и правоохранительных органов никогда не просят граждан принимать участие в мероприятиях, связанных со снятием и переводом денежных средств, получением кредитов, продажей квартир, передачей наличности посторонним лицам.

Телефонный терроризм!

В этот непростой для страны период находятся желающие сделать ложное сообщение о готовящемся террористическом акте: взрыве, поджоге или заминировании какого-либо общественно значимого объекта, по телефону или с использованием информационно-коммуникационных технологий.

Подобные действия преступны. Уголовная ответственность наступает с 14 лет. Наказание за них может последовать в виде лишения свободы сроком до 10 лет.

В первую очередь такая «шалость» создает реальные проблемы для обычных граждан, например, лишает возможности пользоваться общественным транспортом, посещать магазины, объекты культуры и спорта, обращаться за помощью в органы власти.

Уважаемые родители!

Разъясняйте детям преступность подобных действий и их последствия.

Об известных фактах ложных сообщений, о подозрительных предметах и лицах в общественных местах сообщайте сотрудникам полиции лично или по телефону 112.

Фонд «Защитники Отечества» членам семей пропавших без вести

Указом Президента РФ от 20.03.2025 № 157 расширены полномочия Государственного фонда поддержки участников специальной военной операции «Защитники Отечества».

В качестве направления деятельности фонда закреплены организация и оказание поддержки и помощи членам семей лиц, пропавших без вести в период участия в СВО либо признанных безвестно отсутствующими в связи с участием в СВО.

Им оказывается психолого-психотерапевтическая помощь, содействие в получении мер социальной поддержки, услуг, бесплатной юридической помощи и во взаимодействии с органами власти, государственными, муниципальными, волонтерскими организациями, содействие по вопросам, связанным с безвестным отсутствием участников СВО, в том числе касающимся проведения идентификационных генетических исследований.