Наиболее распространенные способы совершения IT преступлений

Фишинг

Мошенники отправляют поддельные электронные письма или сообщения, которые кажутся легитимными, чтобы обмануть пользователей и заставить их раскрыть конфиденциальную информацию, такую как пароли или данные банковских карт.

Пример: Вы получаете электронное письмо, якобы от вашего банка, с просьбой срочно обновить информацию о вашем счете, иначе он будет заблокирован. В письме есть ссылка на фальшивый сайт, который выглядит как официальный сайт банка. Введенные данные попадают в руки мошенников.

Вредоносное ПО (Malware)

Это программное обеспечение, которое установлено на устройстве без ведома пользователя и может похищать данные, нарушать работу системы или получать удаленный доступ к устройству. Примеры включают вирусы, трояны, шпионские программы и программы-вымогатели.

Пример: Вы скачиваете бесплатную программу, которая на самом деле содержит вирус. Этот вирус начинает красть ваши личные данные и отправлять их злоумышленникам.

Социальная инженерия

Мошенники используют психологические манипуляции для обмана людей с целью получения конфиденциальной информации или доступа к системам.

Пример: Злоумышленник представляется сотрудником банка, полиции, прокуратуры, ФСБ, Следственного комитета, используя IP-телефонию звонит потерпевшему с подменных номеров и информирует гражданина о подозрительных финансовых операциях по его банковскому счету, попытках оформления кредита, перевода денежных средств с его счета, либо сообщает о розыске, задержании преступников, совершающих хищения денежных средств с расчетных счетов граждан, при этом извещает о необходимости соблюдения некой «тайны следствия». Далее, используя методы психологического манипулирования и пользуясь доверчивостью, злоумышленник вынуждает потерпевшего сообщать персональные данные, сведения о финансовом состояния, наличии автотранспорта в собственности. Затем, находясь под психологическим воздействием мошенника, потерпевший переводит денежные средства на якобы безопасные расчетные счета.

Совершение посягательства под предлогом оказания содействия родственнику, якобы попавшему в дорожно-транспортное происшествие или задержанному правоохранительными органами. Введенный в заблуждение человек передает денежные средства прибывшему к нему курьеру, который в дальнейшем перечисляет

полученные денежные средства на указанные мошенниками банковские счета (при этом оставляя себе определенный процент средств).

Еще одной распространенной мошеннической схемой остается предлог дополнительного заработка, участия в торгах на бирже, а также инвестирования в различные ценные бумаги. Граждан заманивают яркими вывесками, наименованиями, созвучными с названиями крупных нефте-газодобывающих компаний и холдингов, так называемыми «исключительными» предложениями и возможностью получения высокого дохода, в том числе за короткий промежуток времени. Попавшего под воздействие указанных факторов человека вынуждают вносить крупные суммы денежных средств, без возможности их вывода в дальнейшем.

Размещения «фиктивного» объявления о продаже товара по цене значительно ниже рыночной. Как правило, переписка между покупателем и мошенником ведется на торговой площадке либо с использованием популярных интернет-мессенджеров. В ходе общения мошенник входит в доверие и вынуждает потерпевшего оплатить товар полностью либо внести определенную предоплату путем электронных переводов. После оплаты контакты с покупателем как правило прекращаются, его блокируют, объявление удаляют.

Хищения денежных средств под предлогом приобретения товара у потенциальной жертвы. В данном случае переписка между продавцом и мошенником также ведется с использованием сообщений на сайте, либо с использованием мессенджеров. Продавца убеждают направить товар популярными интернет-сервисами доставки, в том числе используемыми на торговых площадках, сообщая, что товар оплачен, и для получения денежных средств необходимо перейти по ссылке, которую присылают на телефон продавца.

После перехода по ссылке продавец попадает на фишинговый сайт, аналогичный официальному сайту торговой площадки, где вносит свои персональные данные, реквизиты банковской карты и необходимую сумму. После нажатия на «окно» «Получить деньги», денежные средства списываются с расчетного счета продавца. В дальнейшем мошенники убеждают продавца, что произошел некий сбой и для возврата денежных средств необходимо обратиться в службу поддержки, перейдя по еще одной присылаемой ссылке. Продавец, перейдя по ссылке, вновь попадает на фишинговый сайт, где повторно указывает свои данные, реквизиты карты и сумму, якобы необоснованно списанную. После нажатия на «окно» «Получить деньги» с расчетного счета продавца повторно списываются денежные средства.

Аналогичным способом совершается хищение денежных средств через сервис по поиску попутчиков: мошенники размещают объявления с предложением услуги по пассажирским перевозкам. Когда пользователь откликается на объявление, мошенник в чате официального сайта поиска попутчиков просит его связаться с ним через популярный мессенджер по определенному номеру телефона. Затем, в ходе переписки клиенту предлагают оплатить поездку заранее и скидывают ему для этого ссылку на

фишинговый сайт для оплаты. После перехода на сайт, пользователь вводит реквизиты своей банковской карты, далее денежные средства списываются на счет мошенникам.

Атаки типа "человек посередине" (Man-in-the-Middle)

Хакеры перехватывают коммуникации между двумя сторонами, чтобы украсть информацию, изменить данные или подменить сообщения.

Пример: Вы подключаетесь к общественной Wi-Fi сети в кафе, не зная, что она контролируется хакером. Все ваши данные, передаваемые через эту сеть, могут быть перехвачены.

DDoS-атаки (распределенные атаки отказа в обслуживании)

Хакеры перегружают сервер или сеть огромным количеством запросов, что приводит к их недоступности для легитимных пользователей.

Пример: Ваш любимый онлайн-магазин становится недоступным из-за атаки, при которой миллионы запросов отправляются на его сервер одновременно, перегружая его.

Кража паролей

Использование различных методов, включая перебор паролей (так называемый brute force), кражу паролей с помощью кейлоггеров (программ, фиксирующих нажатия клавиш) или использование утекших данных.

Пример: Программа-кейлоггер, установленная на вашем компьютере, записывает все, что вы вводите, включая пароли к вашим учетным записям.

Эксплойты уязвимостей

Мошенники находят и используют уязвимости в программном обеспечении или системах безопасности для получения несанкционированного доступа или нанесения ущерба.

Пример: Вы используете старую версию веб-браузера с известной уязвимостью, которая позволяет хакеру взломать ваш компьютер.

Ботнеты

Мошенники контролируют сети зараженных компьютеров (ботов), чтобы проводить атаки, рассылать спам или выполнять другие злонамеренные действия.

Пример: Ваш компьютер был заражен вирусом и стал частью ботнета, который используется для рассылки спама без вашего ведома.

Сниффинг (прослушка трафика)

Хакеры используют специальные инструменты для перехвата и анализа сетевого трафика, чтобы получить доступ к конфиденциальной информации.

Пример: Хакер использует сниффер для перехвата данных, которые вы передаете через незашифрованное Wi-Fi соединение.

Криптоджекинг (Cryptojacking)

Мошенники тайно используют вычислительные ресурсы жертвы для майнинга криптовалют. Это может привести к значительному снижению производительности системы и увеличению затрат на электроэнергию.

Пример: Вы замечаете, что ваш компьютер стал работать медленнее, а счет за электроэнергию увеличился. Оказывается, что на вашем компьютере незаметно работает программа для майнинга криптовалюты.

Атаки на Интернет вещей (IoT)

Устройства Интернета вещей часто имеют слабую защиту, и злоумышленники могут использовать их для различных целей, включая создание ботнетов и проведение атак.

Пример: Хакер взламывает ваш умный термостат и использует его для атаки на другие устройства в вашей сети.

Сканирование и эксплойтинг открытых портов

Хакеры ищут уязвимые открытые порты в сетях и используют их для проникновения в системы и получения доступа к данным.

Пример: Хакер сканирует вашу домашнюю сеть и находит уязвимый роутер с открытым портом, который позволяет ему получить доступ к устройствам в сети.

Спуфинг (подмена)

Мошенники подделывают адреса электронной почты, IP-адреса или DNS-записи, чтобы обмануть системы и пользователей.

Пример: Вы получаете электронное письмо, которое выглядит как сообщение от вашего друга, но на самом деле оно отправлено с поддельного адреса и содержит вредоносную ссылку.

Кража данных с помощью USB-устройств

Физический доступ к компьютеру позволяет злоумышленникам использовать USB-устройства для копирования данных или установки вредоносного ПО.

Пример: Кто-то подключает зараженную флешку к вашему компьютеру на работе и копирует важные файлы или устанавливает вирус.

Перехват SMS (SIM Swapping)

Мошенники получают дубликат SIM-карты жертвы, чтобы перехватить сообщения и вызовы, что позволяет им обойти двухфакторную аутентификацию.

Пример: Вы теряете доступ к своему телефону, а мошенники используют ваш номер для получения доступа к вашим банковским счетам.

Эксплойты операционных систем и приложений

Злоумышленники используют уязвимости в операционных системах и приложениях, которые не были своевременно обновлены, чтобы получить доступ к системам и данным.

Пример: Хакер использует уязвимость в необновленной версии операционной системы вашего компьютера, чтобы получить контроль над ним.

Программное обеспечение для удаленного доступа (RAT)

Мошенники устанавливают RAT на устройства жертв, чтобы получать полный удаленный доступ и контроль над системами.

Пример: Вы случайно устанавливаете программу, которая позволяет хакеру удаленно контролировать ваш компьютер, включая доступ к вашим файлам и камере.

Криптографические атаки

Попытки взлома или подделки криптографических протоколов и алгоритмов для получения доступа к зашифрованной информации.

Пример: Хакер пытается взломать зашифрованное сообщение, чтобы узнать содержимое конфиденциальной информации.

Сквоттинг доменных имен (Domain Squatting)

Мошенники регистрируют доменные имена, похожие на легитимные, чтобы обманом привлекать пользователей и похищать их данные.

Пример: Вы вводите неправильный адрес вашего любимого интернет-магазина и попадаете на поддельный сайт, который крадет ваши данные.

Взлом облачных сервисов

Атаки на облачные сервисы для получения доступа к данным, хранящимся в облаке.

Пример: Хакер взламывает ваш аккаунт в облачном хранилище и получает доступ ко всем вашим фотографиям и документам.

Пакетные снифферы (Packet Sniffers)

Инструменты, используемые для захвата и анализа данных, передаваемых по сети, что позволяет злоумышленникам перехватывать конфиденциальную информацию.

Пример: Хакер использует сниффер, чтобы перехватить ваши банковские данные, передаваемые по незашифрованной сети.

Социальные сети и фальшивые аккаунты

Мошенники создают поддельные аккаунты в социальных сетях для распространения вредоносных ссылок, фишинга и социальной инженерии.

Пример: Вы получаете сообщение в социальной сети от человека, который притворяется вашим другом, и оно содержит вредоносную ссылку.

Шифрование и вымогательство (Ransomware)

Вредоносное ПО шифрует данные на устройстве жертвы и требует выкуп за их расшифровку.

Пример: Вы включаете компьютер и видите сообщение о том, что все ваши файлы зашифрованы, и вы должны заплатить выкуп, чтобы получить к ним доступ.

Программы-логгеры (Keyloggers)

Программы, которые записывают нажатия клавиш пользователя для кражи паролей и другой конфиденциальной информации.

Пример: Кейлоггер записывает все, что вы вводите на клавиатуре, включая ваши пароли и личные сообщения, и отправляет эти данные хакеру.

Кардинг (Carding)

Кража данных кредитных карт и их использование для совершения мошеннических покупок.

Пример: Ваши данные кредитной карты крадут и используют для покупок в интернет-магазинах без вашего ведома.

Внутренние угрозы (Insider threats)

Сотрудники компании могут злоупотреблять своим доступом к конфиденциальной информации или системам для личной выгоды или по другим причинам.

Пример: Сотрудник компании копирует важные данные и продает их конкурентам.

Сомнительные Wi-Fi сети (Rogue Wi-Fi networks)

Мошенники создают поддельные точки доступа Wi-Fi, чтобы перехватывать данные пользователей, подключающихся к ним.

Пример: Вы подключаетесь к бесплатной Wi-Fi сети в кафе, не зная, что она создана мошенниками для кражи ваших данных.

Подмена программного обеспечения (Software Substitution)

Установка поддельных или измененных версий легитимного ПО, которое содержит вредоносные функции.

Пример: Вы скачиваете известную программу с неизвестного сайта, и она оказывается поддельной, содержащей вирусы.

Мошенничество с техподдержкой (Tech Support Scams)

Злоумышленники притворяются представителями техподдержки и убеждают жертв предоставить доступ к их компьютерам или оплатить ненужные услуги.

Пример: Вам звонят и утверждают, что ваш компьютер заражен, и предлагают за деньги устранить проблему, получая при этом доступ к вашему устройству.

Кража учетных записей (Account Takeover)

Захват учетных записей пользователей через взлом паролей, фишинг или другие методы.

Пример: Ваша учетная запись в социальной сети взломана, и злоумышленник использует ее для рассылки спама или кражи ваших данных.

Дорожные войны (Drive-by Downloads)

Автоматическая загрузка и установка вредоносного ПО при посещении зараженных веб-сайтов.

Пример: Вы заходите на зараженный сайт, и на ваш компьютер без вашего ведома загружается вирус.

Атаки на голосовые помощники (Voice Assistant Attacks)

Использование голосовых команд для злоупотребления функциональностью устройств с голосовыми помощниками.

Пример: Кто-то использует ваш голосовой помощник, чтобы делать покупки или управлять вашими умными устройствами без вашего разрешения.

Мошенничество с благотворительностью (Charity Scams)

Создание поддельных благотворительных организаций для сбора денег или данных.

Пример: Вы видите призыв о помощи в социальной сети и жертвуете деньги, но выясняется, что эта организация не существует, а мошенники просто собирают деньги для себя.

Шантаж (Blackmail)

Угроза раскрыть конфиденциальную информацию или данные в обмен на выкуп.

Пример: Мошенник угрожает опубликовать ваши личные фотографии или переписку, если вы не заплатите выкуп.

Слежка через веб-камеры и микрофоны (Webcam and Microphone Surveillance)

Использование вредоносного ПО для скрытого наблюдения через веб-камеры и микрофоны.

Пример: Вредоносная программа получает доступ к вашей веб-камере и микрофону, позволяя злоумышленнику следить за вами без вашего ведома.

Фишинг с использованием ИИ (искуственный интеллект)

Пример: ИИ может анализировать огромные объемы данных, чтобы создать персонализированные фишинговые письма. Такие письма выглядят гораздо более правдоподобно и могут включать личные детали, что повышает вероятность того, что получатель откроет письмо и выполнит инструкции мошенника.

Deepfake видео и аудио

Пример: Технология deepfake позволяет создавать реалистичные видео и аудио, которые трудно отличить от настоящих. Мошенники могут использовать deepfake, чтобы создать фальшивые видео или аудио с участием известных лиц или даже вас самих, чтобы обманом заставить людей поверить в ложные заявления или перевести деньги.

Социальная инженерия с использованием ИИ

Пример: ИИ может анализировать профили в социальных сетях, чтобы собрать информацию о потенциальных жертвах и разработать более целенаправленные атаки. Например, ИИ может создать персонализированные сообщения от имени друзей или коллег жертвы, чтобы завоевать доверие и обманом заставить выдать конфиденциальную информацию.

Автоматизация мошеннических звонков (Robo-calls)

Пример: Мошенники могут использовать ИИ для автоматизации звонков с фальшивыми предложениями или угрозами. ИИ может имитировать человеческую речь и реагировать на ответы жертвы, что делает такие звонки более убедительными.

Поддельные отзывы и комментарии

Пример: ИИ может создавать поддельные отзывы и комментарии на различных платформах, чтобы манипулировать общественным мнением или рейтингами продуктов и услуг. Это может использоваться для продвижения мошеннических схем или дискредитации конкурентов.

Спуфинг голоса

Пример: ИИ может синтезировать голос, который имитирует голос определенного человека. Это может быть использовано для обмана системы голосовой аутентификации или для совершения мошенничества, например, звонков с поддельными запросами от имени руководителей компаний.

Создание фальшивых новостей (Fake News)

Пример: ИИ может генерировать убедительные фальшивые новости и распространять их через социальные сети и новостные сайты. Это может использоваться для манипуляции общественным мнением, дискредитации лиц или организаций и даже влияния на выборы.

Хищения с применением цифровых технологий и риски

Такие хищения несут множество рисков, которые могут серьезно повлиять на личные данные, финансовое состояние и репутацию как частных лиц, так и организаций. Вот некоторые из основных рисков:

1. Финансовые потери

Пример: Кража данных кредитных карт, банковских счетов или доступов к онлайн-банкингу может привести к несанкционированным транзакциям и значительным финансовым убыткам.

2. Кража личных данных

Пример: Утечка личной информации, такой как имена, адреса, номера телефонов, номера социального страхования и другие данные, может использоваться для создания поддельных учетных записей, кредитных карт или получения кредитов от вашего имени.

3. Нарушение конфиденциальности

Пример: Взлом электронной почты или социальных сетей может привести к раскрытию личной переписки, фотографий и других конфиденциальных данных, что может негативно сказаться на личной и профессиональной жизни.

4. Потеря интеллектуальной собственности

Пример: Кража данных, включая патенты, бизнес-планы и конфиденциальную информацию, может привести к значительным убыткам и конкурентным преимуществам для злоумышленников.

5. Репутационные риски

Пример: Компании и люди, подвергшиеся утечкам данных, могут потерять доверие клиентов и партнеров, что приведет к снижению доходов и ухудшению имиджа.

6. Законодательные и юридические последствия

Пример: Нарушение законодательства о защите данных может привести к крупным штрафам и судебным искам, что дополнительно усугубляет финансовые потери и репутационные риски.

7. Потеря данных

Пример: Атаки с применением вымогательского ПО (ransomware) могут зашифровать важные данные, и если вы не заплатите выкуп, вы можете навсегда потерять доступ к этим данным.

8. Нежелательный доступ к системам

Пример: Злоумышленники могут получить доступ к корпоративным сетям и системам, что может привести к утечке данных, нарушениям в работе и финансовым убыткам.

9. Социальная инженерия и психологические риски

Пример: Мошенники могут использовать социальную инженерию для обмана сотрудников, что может привести к утечке данных или компрометации системы.

10. Угроза физической безопасности

Пример: Кража данных с систем безопасности, таких как камеры наблюдения или системы умного дома, может поставить под угрозу физическую безопасность людей.

11. Неразрешенное использование ресурсов

Пример: Криптоджекинг, когда злоумышленники используют вычислительные ресурсы ваших устройств для майнинга криптовалют, может привести к снижению производительности и увеличению затрат на электроэнергию.

12. Компрометация критически важных инфраструктур

Пример: Атаки на критически важные инфраструктуры, такие как энергосети или системы водоснабжения, могут привести к масштабным сбоям и нарушению жизнедеятельности городов и регионов.

Эти риски подчеркивают важность внедрения надежных мер безопасности и постоянного обновления знаний о новых угрозах и методах защиты.

Способы защиты от киберпреступлений и мошенничества

1. Используйте сильные пароли

Пример: Пароль - это как ключ от вашего дома. Вместо "1234" или "password", используйте длинные и сложные пароли, например, "GrandmaKnits123!".

2. Включите двухфакторную аутентификацию (2FA)

Пример: Это как дополнительный замок на двери. Даже если кто-то украдет ваш пароль, они не смогут войти без второго кода, который приходит на ваш телефон.

3. Будьте осторожны с подозрительными ссылками и письмами

Пример: Если вам приходит письмо от "банка" с просьбой ввести ваши данные, не делайте этого. Лучше позвоните в банк и уточните.

4. Регулярно обновляйте программное обеспечение

Пример: Обновляйте ваш компьютер и телефон. Это помогает защититься от новых вирусов.

5. Используйте антивирусное программное обеспечение

Пример: Антивирус - это как сторожевой пес для вашего компьютера. Он лает, когда что-то не так, и защищает ваш компьютер от вирусов.

6. Создавайте резервные копии данных

Пример: Резервное копирование - это как копировать старые фотографии. Если компьютер сломается, ваши данные будут в безопасности.

7. Защищайте свои устройства паролями

8. Используйте VPN для безопасного интернета

Пример: VPN - это как шторка на вашем окне. Она скрывает, что вы делаете в интернете от посторонних глаз.

9. Будьте осторожны с общедоступными Wi-Fi сетями

Пример: Не подключайтесь к бесплатным Wi-Fi в кафе или парках, если не уверены в их безопасности. Лучше используйте мобильный интернет.

10. Не делитесь личной информацией онлайн

Пример: Не рассказывайте в соцсетях о том, когда вы едете в отпуск или какие у вас банковские счета.

11. Проверяйте свои банковские счета регулярно

Пример: Регулярно проверяйте выписки по счетам. Если заметите что-то странное, сразу сообщите в банк.

12. Используйте менеджеры паролей

Пример: Менеджер паролей - это как записная книжка для ваших паролей, но гораздо безопаснее. Он помогает вам создавать и хранить сложные пароли, чтобы не нужно было запоминать их все.

13. Остерегайтесь загрузки подозрительных файлов

Пример: Если вы получили электронное письмо с вложением от незнакомого человека, не открывайте его.

14. Отключайте Bluetooth и Wi-Fi, когда они не нужны

15. Регулярно проверяйте настройки конфиденциальности в соцсетях

Пример: Периодически проверяйте, кто может видеть ваши посты и личную информацию в социальных сетях.

16. Не используйте один и тот же пароль для разных сайтов

Пример: Использование одного пароля для всех учетных записей - это как использование одного ключа для всех дверей. Если кто-то украдет этот ключ, он сможет открыть все ваши двери.

17. Установите родительский контроль на устройствах детей

Пример: Родительский контроль - это как забор вокруг игрового поля. Он помогает детям безопасно использовать интернет и защищает их от нежелательного контента.

18. Обучайте себя и близких основам кибербезопасности

Пример: Проводите время, изучая основы кибербезопасности, чтобы знать, как защитить себя.

19. Остерегайтесь подозрительных телефонных звонков

Пример: Если кто-то звонит и просит личную информацию, не давайте ее сразу.

20. Проверяйте URL-адреса сайтов

Пример: Прежде чем вводить личные данные на сайте, проверьте URL-адрес. Убедитесь, что он начинается с "https" и что это правильный сайт.

21. Используйте функции блокировки и удаленного стирания данных на устройствах

Пример: Настройте функцию, которая позволяет блокировать и удаленно стирать данные с вашего телефона, если его украдут.

22. Регулярно проверяйте журналы активности

Пример: Время от времени проверяйте журналы активности на своих учетных записях, чтобы убедиться, что никто посторонний не пытался войти.

23. Настройте уведомления о подозрительной активности

Пример: Включите уведомления о входах в учетные записи с новых устройств или местоположений.

24. Остерегайтесь бесплатных предложений и подарков

Пример: Не скачивайте программы и не принимайте предложения о "бесплатных подарках", если они кажутся слишком хорошими, чтобы быть правдой.

25. Защищайте свою электронную почту

Пример: Настройте двухфакторную аутентификацию для вашей электронной почты.

26. Используйте сложные ответы на контрольные вопросы

Пример: Не используйте очевидные ответы на контрольные вопросы, такие как "девичья фамилия матери". Придумайте что-то, что трудно угадать.

27. Используйте зашифрованные мессенджеры

Пример: Для отправки конфиденциальной информации используйте мессенджеры с end-to-end шифрованием, такие как Signal. Это как отправлять письма в конвертах с замком, а не открытки.

28. Избегайте использования общедоступных компьютеров для входа в личные аккаунты

Пример: Не используйте компьютеры в библиотеках или интернет-кафе для входа в свои учетные записи.

31. Устанавливайте ограничение на транзакции по банковским картам

Пример: Установите лимиты на суммы транзакций и оповещения о любых покупках.

32. Регулярно проверяйте настройки и разрешения приложений

Пример: Периодически просматривайте, какие разрешения вы дали своим приложениям, и отзывайте ненужные.

33. Избегайте использования автоматического входа

Пример: Не включайте автоматический вход на своих устройствах и в приложениях.

34. Используйте безопасные методы оплаты

Пример: Виртуальные карты для онлайн-покупок.

35. Настройте фильтры спама

Пример: Установите фильтры спама на вашу электронную почту, чтобы не получать подозрительные и фишинговые письма.

36. Остерегайтесь фальшивых звонков о выигрыше

Пример: Если кто-то звонит и говорит, что вы выиграли лотерею, но нужно заплатить "налог" или "сбор", это скорее всего мошенничество.

37. Используйте разные электронные адреса для разных целей

Пример: Иметь отдельный адрес электронной почты для регистрации на сайтах и другой для личной переписки..

38. Удаляйте учетные записи, которые больше не используете

Пример: Закрывайте старые учетные записи на сайтах и сервисах, которыми вы больше не пользуетесь.

39. Будьте бдительны в социальных сетях

Пример: Не принимайте запросы на добавление в друзья от незнакомцев и не делитесь слишком личной информацией.

Возможность установления гражданином запрета на онлайн операции, в т.ч. на заключение договоров с кредитными организациями

1. Запрет на дистанционное оформление кредитов и займов

Пример: Гражданин может обратиться в кредитную организацию с заявлением о запрете на дистанционное оформление кредитов и займов. После этого заявления кредитные организации не смогут выдавать кредиты и займы без личного присутствия гражданина.

Законодательная база: http://publication.pravo.gov.ru/document/0001202402260017

2. Блокировка банковских карт и счетов для онлайн операций

Пример: Гражданин может обратиться в банк с просьбой заблокировать свои карты и счета для проведения онлайн операций. Это позволит предотвратить использование данных карты или счета для мошеннических транзакций.

Законодательная база: https://www.consultant.ru/document/cons_doc_LAW_115625/

3. Использование сервиса "Госуслуги" для контроля за кредитными историями

Пример: Гражданин может использовать портал "Госуслуги" для регулярной проверки своей кредитной истории. Это позволяет оперативно обнаружить попытки оформления кредита на его имя и предпринять меры по аннулированию незаконных кредитов.

Законодательная база: https://www.consultant.ru/document/cons_doc_LAW_51043/

4. Установка лимитов на операции по банковским картам

Пример: Гражданин может установить суточные или месячные лимиты на операции по своим банковским картам. Это ограничивает размер возможных потерь в случае мошеннической транзакции.

Законодательная база: https://www.consultant.ru/document/cons_doc_LAW_115625/

5. Подключение уведомлений о проведенных операциях

Пример: Гражданин может подключить услугу СМС-уведомлений или уведомлений через мобильное приложение о всех проведенных операциях по своим счетам и картам. Это позволяет быстро обнаружить несанкционированные транзакции.

Законодательная база: Внутренние правила банков, регулируемые федеральными законами и инструкциями Центрального банка РФ.

6. Обращение в Центральный банк РФ

Пример: В случае обнаружения мошеннических действий гражданин может обратиться в Центральный банк РФ с жалобой на действия кредитной организации. Центральный банк имеет полномочия для проведения расследования и принятия мер в отношении банков и кредитных организаций.

Законодательная база: https://www.consultant.ru/document/cons_doc_LAW_37570/

7. Блокировка SIM-карт для проведения банковских операций

Пример: Гражданин может обратиться к оператору сотовой связи с просьбой заблокировать возможность использования его номера телефона для проведения финансовых операций, таких как подтверждение платежей или оформление кредитов.

Законодательная база: https://www.consultant.ru/document/cons_doc_LAW_43224/

8. Обращение в Бюро кредитных историй (БКИ)

Пример: Гражданин может обратиться в БКИ с запросом на получение своей кредитной истории и при обнаружении подозрительных записей незамедлительно обратиться в кредитные организации для их аннулирования.

Законодательная база: consultant.ru/document/cons_doc_LAW_51043/

9. Ограничение доступа к личной информации

Пример: Гражданин может ограничить доступ к своей личной информации в различных интернет-сервисах и социальных сетях, чтобы уменьшить риск использования этих данных мошенниками.

Законодательная база: https://www.consultant.ru/document/cons_doc_LAW_61801/