ПРОКУРАТУРА СВЕРДЛОВСКОЙ ОБЛАСТИ

ПАМЯТКА
ПО КИБЕРБЕЗОПАСНОСТИ.
СХЕМЫ ОБМАНА ГРАЖДАН

г. Екатеринбург 2025 г.

Цифровой мир открывает огромные возможности, но и создает новые риски. Преступные схемы постоянно совершенствуются, появляются все новые способы обмана граждан.

В зоне особого риска дети, подростки и пожилые люди.

В данной памятке описаны наиболее распространенные и актуальные на сегодняшний день преступные модели, приемы и методики, реализуемые киберпреступниками

- Фишинг
- Аренда аккаунтов
- Вредоносное программное обеспечение (вирусы)
- Спящие клиенты
- Рабочий чат с руководителем
- Предложения от оператора связи
- Инвесторы и инвестиции
- Собеседование с работодателем
- Помощь родственнику (другу, знакомому)
- Звонок из банка
- Звонок из ФСБ
- Звонок из деканата
- Начинающий фотограф
- Лжериелторы
- Случайный перевод на карту

Помните: чем меньше личной информации Вы раскрываете, тем труднее вас обмануть.

Большинство преступных схем сводятся к получению преступниками сведений, которые позволяют совершить хищение:

- финансовая информация: номер карты, срок действия, CVC/CVV-код, логины и пароли от интернет-банка, коды из SMS, пуш-уведомления подтверждения.

- персональные данные и документы: паспортные данные, ИНН, СНИЛС, фото документов

- аутентификационные коды: любые разовые пароли из SMS, push-коды, QR-коды подтверждения.

- приватная информация: адрес, номера родственников, маршрут поездки, точное местоположение в режиме реального времени.

ВАЖНО
Никто из официальных структур — ни банк, ни «Госуслуги», ни полиция — не попросит у вас коды доступа или паспорт по телефону или в чате.

КОД ДОСТУПА СПРАШИВАЮТ ТОЛЬКО ПРЕСТУПНИКИ!

1. ФИШИНГ

Фишинг (англ. phishing от fishing «рыбная ловля, выуживание») - один из наиболее частых способов хищения в сети Интернет, суть которого заключается в распространении ссылок на поддельные сайты и ресурсы. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными приёмами побудить пользователя ввести свои логин и пароль, которые он использует для доступа к оригинальному сайту и (или) финансовую информацию.

Фишинговые ссылки могут поступать через все каналы: социальные сети, личный и рабочий e-mail, мессенджеры, SMS, а также чаты на сайтах знакомств и подобных ресурсах.

РАСПРОСТРАНЕННЫЙ ПРИМЕР ФИШИНГА
мошенники размещают в сервисе для совместных поездок BlaBlaCar привлекательные предложения, чаще всего от имени водителя-девушки. После согласования поездки они отправляют ссылку на поддельный сайт, который внешне похож на оригинальный.

Граждан просят авторизоваться для «бронирования», в том числе ввести данные платежных средств. После введения кода со счетов списываются деньги, а переписка с «водителем» прекращается.

ПРИЗНАКИ ФИШИНГОВЫХ ССЫЛОК

- Ссылка в виде цифр:
http:// 178.148.232.27

- Ссылка с символом «@»:
http://bank. ru@zlo. ru.

- Ссылки с двумя и более адресами:
https://bank. ru/rd.php?go=https://zlo. ru

- В адресе сайта есть www, но нет точки или стоит дефис:
wwwbank. ru или www-bank. ru.

- В начале адреса сайта есть http или https, но нет «://»:
httpsbank. ru или httpbank. ru.

- Если при наведении указателя мыши ссылка выглядит по-другому. Например в тексте письма написано tele2. ru, а при наведении мыши в нижнем углу браузера отображается teie2. ru.

- Одна из букв заменена на цифру. Например вместо буквы «О» стоит цифра «0» или вместо маленькой латинской буквы «l» (L) стоит большая буква «I» (i) или вместо латинской буквы «b» стоит латинская буква «d».

ВАЖНО

Правило № 1:
Лучше не открывать ссылки от незнакомцев.

Правило № 2:
Ссылки от знакомых, присланные вам без объяснения или с подозрительными объяснениями, лучше сразу не открывать и проверить, действительно ли это ваш знакомый.

Правило № 3:
Если после перехода по подозрительной ссылке у вас запрашивают конфиденциальную или личную информацию, предлагают скачать файл (особенно архив) – немедленно уходите с сайта.

Правило № 4:
Всегда пользуйтесь современным антивирусом, который может распознать фишинговую ссылку.

Правило № 5:
Проверяйте ссылку не только перед переходом по ней, но и когда вы уже перешли на сайт. Сайт, на который вы попали, может отличаться от того, что было написано в ссылке.

2. АРЕНДА АККАУНТОВ

Сегодня в сети можно встретить многочисленные предложения сдать свой аккаунт в мессенджерах в аренду за вознаграждение.

Это очередной способ «легкого» заработка, который может привести к серьёзным последствиям.

Мошенники развернули массовое приобретение или аренду аккаунтов в мессенджерах.

Их целевой аудиторией становятся дети и подростки, для которых выплачиваемое вознаграждение может показаться значительным.

Злоумышленники вовлекают молодежь в тематических каналах, в чатах онлайн-игр, в сообществах, распространяющих информацию о популярных блогерах или мероприятиях, и уверяют, что аренда аккаунта – это «серый» или даже легальный способ заработка.

ВАЖНО
через арендованные аккаунты обманывают людей, шантажируют, вербуют участников запрещенных организаций и даже организуют террористическую деятельность.

3. ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ (ВИРУСЫ).

Владельцы современных смартфонов часто становятся жертвами вирусов и вредоносного програмного обеспечения.

Такой софт проникает в пользовательские устройства после перехода владельцев по подозрительным ссылкам или в случае загрузки мобильных приложений из непроверенных источников.

Одним из наиболее распространённых на сегодняшний день вирусов для операционных систем смартфонов являются вредоносные программы, основной функционал вирусов которых заключается в сборе маркетинговых данных, демонстрации рекламных сообщений в фоновом режиме на пользовательском устройстве, а также в перенаправлении пользователей на вредоносные веб-ресурсы.

Другой вид вредоносных программ, необходим злоумышленникам для отслеживания пользовательских действий и получения геолокационных данных в скрытом режиме.

В последние годы пользователи телефонов часто сталкиваются с вирусами-троянами, которые крадут персональные данные пользователей и отправляют платные SMS-сообщения с телефонного номера владельца устройства.

Для обнаружения такого вредоносного программного обеспечения следует отсортировать мобильные приложения на своём устройстве по частоте использования и оценить их активность в потреблении трафика и расходе аккумулятора.

В том случае, если у какого-то неизвестного мобильного приложения наблюдается слишком большая активность, с высокой долей вероятности эта программа является вредоносной.

ВАЖНО

Пользователям стоит проверить, какие именно мобильные приложения располагают доступом к контактам и геолокационной информации. Если подобные разрешения не нужны для нормального функционирования приложения, то, вполне вероятно, они применяются в шпионских целях.

4. СПЯЩИЕ КЛИЕНТЫ

Киберпреступники приобретают старые сим-карты, которые уже были использованы и поступили в повторную продажу. Затем они используют эти сим-карты для восстановления доступа к учетным записям различных онлайн-сервисов.

ВАЖНО
Для избежания многомиллионного кредита, взятого другим человеком, необходимо первым делом открепить неиспользуемый номер телефона от портала «Госуслуг», онлайн-банка и других своих аккаунтов.

Сделать это самостоятельно можно, если сим-карта, которой не планируется больше пользоваться, все еще установлена в телефоне. Связано это с тем, что на этот номер придет код, подтверждающий действия.

Сменить номер телефона достаточно просто, на портале «Госуслуги» нужно перейти в раздел «Настройки и безопасность» и нажать «Изменить» напротив прикрепленного номера телефона.

Если же сим-карты на руках уже нет, то сменить номер на портале «Госуслуг» самостоятельно уже не получится. Для этого необходимо обратиться в МФЦ.

5. ПРЕДЛОЖЕНИЕ ОТ ОПЕРАТОРА СВЯЗИ

1. Под видом специалистов компаний сотовой связи мошенники звонят гражданам и утверждают, что действующий договор заканчивается и его необходимо продлить, иначе номер передадут другому абоненту.

Преступники уверяют, что идти никуда не нужно, все можно сделать по телефону, уверяет злоумышленник. Достаточно продиктовать код из смс.

Таким образом человек не продлевает договор, который на самом деле является бессрочным, а предоставляет данные для входа в личный кабинет на портале «Госуслуги» и всю информацию о себе.

2. Гражданину предлагают сменить тарифный план, заменить sim-карту и т.д. Чтобы подтвердить действие, абоненту нужно продиктовать код из смс.

С помощью этого кода злоумышленник получает доступ к личному кабинету пользователя на официальном сайте оператора. А уже там он настраивает переадресацию сообщений и звонков с номера жертвы на свой.

Это позволяет преступнику подтверждать операции: вывод средств с банковских карт абонента, оформление кредита и т.д.

6. РАБОЧИЙ ЧАТ С РУКОВОДИТЕЛЕМ

Мошенники активно используют доверие внутри коллективов, создавая поддельные рабочие чаты.

Сотрудник получает приглашение в групповой чат в мессенджере с названием его реальной организации, филиала или отдела. Название выглядит правдоподобно.

В чате могут присутствовать аккаунты, выдающие себя за его коллег, а иногда даже приглашаются настоящие коллеги, не подозревающие о подмене.
Это создает иллюзию легитимности.

В чате появляется аккаунт, имитирующий руководителя (директора, завуча, главврача и т.д.). От него поступает срочное указание, например: зарегистрироваться в определенном «корпоративном» боте для важной задачи или получения данных; обновить учетные данные и т.д.;

- Для завершения действия система (часто тот же бот) присылает на телефон сотрудника SMS или push-уведомление с кодом подтверждения.

- В этот момент поддельные аккаунты «коллег» начинают массово отправлять в чат «свои» коды подтверждения. Затем «руководитель» публично их хвалит за оперативность.

- Сотрудник, видя «пример коллег» и «одобрение начальства», находясь в условиях искусственно созданной срочности и группового давления, теряет бдительность и также публично отправляет свой конфиденциальный код в чат.

Почему под прицелом – образование и медицина?
Мошенники не случайно выбирают эти сферы.

Информация о сотрудниках (ФИО, должности, иногда даже фотографии) часто публикуется на официальных сайтах учебных заведений и больниц/поликлиник.
Это дает злоумышленникам готовый «справочник» для создания правдоподобных фейковых аккаунтов и персонализации атаки.

ВАЖНО
Как защитить себя?
- Не передавать никому и никогда код из SMS или push-уведомлений (даже если Вас убеждают, что это очень срочно и необходимо, а также абсолютно безопасно).
- Проявлять бдительность при общении в мессенджерах. Ваши собеседники могут оказаться не теми людьми, за которых себя выдают (особенно, если Вы не можете удостовериться в их личности).
- Не вступать в подозрительные чаты, проверять реальность их существования.

7. ИНВЕСТОРЫ И ИНВЕСТИЦИИ

Злоумышленники связываются с потенциальными «инвесторами» через социальные сети или звонят им под видом сотрудников известных инвестиционных компаний. Предложение заманчивое – нужно лишь открыть «брокерский» счет и инвестировать для начала небольшую сумму. При этом, обещается, что доход многократно превышает вложения**.**

Для открытия такого счета мошенники требуют установить специальное приложение на смартфон, планшет или компьютер.

Далее программа имитирует якобы рост доходов от инвестиций, в том числе в криптовалюту.
Для увеличения объема инвестиций и получения сверхприбыли граждан убеждают взять займы и продать имущество.

Как только у «инвестора» возникает желание вывести деньги со счета – начинаются проблемы.

Лжеброкеры говорят, что сделать это сложно.
Нужно пополнить счет еще раз на определенную сумму, оплатить «страховку» или ежедневное размещение валюты в «европейской ячейке» либо найти поручителя, чтобы можно было «обналичить» средства.

В итоге инвестор теряет свои деньги (в т.ч. кредитные), заодно и надежду на будущие миллионы.

Вариант мошеннической схемы – участие в уникальном инвестиционном онлайн-проекте известного банка. Завлекают потенциальных жертв при помощи писем на электронную почту.

После предложат пройти опрос: указать заработок, предпочитаемый способ хранения средств и контактные данные для связи, а также дадут доступ к специальному приложению. Далее понадобится ввести данные банковской карты (с нее преступники и спишут деньги).

ВАЖНО
Рационально оценивайте свои возможности и риски.

Проверьте сайт инвестиционной компании или брокера, а также наличие лицензии Банка России.

Откажитесь от услуг компании или ее представителей, если они просят перевести деньги за услуги на карту физического лица (либо через электронный кошелек).

Обязательно заключите договор и запрашивайте отчет об оказании брокерских услуг.

Не верьте обещаниям гарантированного высокого дохода в короткие сроки.

8. СОБЕСЕДОВАНИЕ С РАБОТОДАТЕЛЕМ

Собеседование с будущим работодателем – волнительная процедура. Порой мошенники пользуются растерянностью соискателей и крадут личные данные прямо во время онлайн-встречи.

Под видом будущего работодателя мошенники проводят собеседование, где они просят кандидата заполнить анкету прямо во время зума.
Один из ее пунктов – номер карты и другие ее данные.
На нее злоумышленники обещают производить оплату.

Чтобы ничего не пропустить, они включают запись экрана. Некоторые мошенники просят указать информацию по нескольким банковским картам, если какую-то якобы не примет бухгалтерия.

Вместо пополнений с банковской карты соискателя в будущем происходят списания, а на работу его так и не устраивают.

Находясь в поиске работы, можно не только потерять деньги, но и нарушить закон, став дроппером.

В последнее время именно этот мошеннический сценарий становится популярным, а его жертвами становятся студенты и пенсионеры.

Дропперы или дропы (от английского drop — бросать, капать) – подставные лица, которые задействованы в нелегальных схемах по выводу средств с банковских карт.

Часто жертва не осознает, что вовлечена в преступную схему. Ведь объявление о работе, на которую она устраивается, не выглядит подозрительно. А будущий работодатель после собеседования предоставляет договор, оговаривает условия труда, сроки выполнения работы и другие нюансы.

ВАЖНО
Внимательно изучайте предложение от будущего работодателя и отзывы о нем.

Не вверьте обещаниям легкого заработка с минимальной затратой собственного времени.

При общении сохраняйте холодную голову, не поддавайтесь эмоциям, а главное – следите за данными, доступ к которым предлагается предоставить.

9. ПОМОЩЬ РОДСТВЕННИКУ (ДРУГУ, ЗНАКОМОМУ)

Еще одна тактика злоумышленников – рассылка сообщений с просьбой одолжить денег близким или друзьям. Порой мошенники играют на чувствах жертвы и сообщают, что ее родственник попал в беду.
Если раньше преступникам приходилось разыгрывать театральный спектакль, подделывая голос, то теперь за них это делают алгоритмы искусственного интеллекта.

Злоумышленники взламывают аккаунт пользователя, скачивают голосовые сообщения и на их основе генерируют монолог для дальнейшего обмана.

Существует и другой сценарий – просьба проголосовать за детей или племянников в детском конкурсе. За ссылкой для голосования, которую мошенники отправляют со взломанного аккаунта владельца, скрыт вирус, который откроет им доступ к вашему гаджету.

ВАЖНО
Не переходите по неизвестным ссылкам, даже если получили их от близких или знакомых.

Договоритесь с родственниками о пароле или секретном вопросе, который нужно назвать, если разговор кажется подозрительным. Такой шаг поможет раскусить намерения мошенника.

10. ЗВОНОК ИЗ БАНКА

Мошенники под видом специалистов техподдержки финансовых организаций предлагают установить на смартфон приложение для поиска вирусов.
Это вредоносное программное обеспечение, которое дает доступ к телефону жертвы и его данным.

Еще один популярный сценарий – помощь в сохранении денежных средств.

Преступники под видом сотрудников Банка России сообщают жертве о том, что кто-то пытается похитить деньги с ее счета. Чтобы их спасти, надо перевести средства на «безопасный» счет в ЦБ РФ. По легенде это временная мера – на период поиска преступников. А потом всю сумму человеку якобы возместят наличными.

ВАЖНО
Пользуйтесь только официальными ресурсами финансовых организаций.

Если вам звонят сотрудники банка и разговор с ними кажется подозрительным, перезвоните на официальный номер, размещенный на сайте финансовой организации.

11. ЗВОНОК ИЗ «ФСБ»

Часто мошенники звонят или пишут гражданам от имени сотрудников ФСБ, прокуратуры, Следственного комитета, полиции, Росфинмониторинга и т.д.

Самая распространенная уловка – предложение получить какую-либо государственную выплату. Схема классическая: Вы нам данные карты, мы вам – деньги.

Есть и другие сценарии.
Например, звонок от следственных органов или Росфинмониторинга с угрозой блокировки счета, по которому зафиксированы сомнительные операции. Чтобы этого избежать, мошенники требуют оплатить штраф. Для убедительности они могут прислать квитанцию на официальном бланке ведомства.

Также они могут сообщить о наложении ареста на квартиру в связи с попыткой ее незаконного переоформления в собственность иных лиц
В связи с этим, нужно срочно совершить сделку по ее отчуждению (в пользу мошенников, разумеется).

ВАЖНО
Помните, что подобные ведомства не оказывают платных услуг по оформлению документов и переоформлению квартир, а также не рассылают подобные письма и не звонят в мессенджерах.

12. ЗВОНОК ИЗ ДЕКАНАТА

Студенту звонят от имени деканата с требованием проверки данных или регистрации в специальном сервисе. Для совершения данного действия необходимо назвать код авторизации.

Цель злоумышленников – получение доступа к аккаунту на "Госуслугах".

После получения доступа к аккаунту туда будут подгружены поддельные доверенности, в банки будут направлены заявки на оформление кредитов.

Цель злоумышленников – психологическое воздействие, создание паники и снижение критичности мышления.

Когда гражданин убежден во взломе, подключаются фейковые сотрудники Росфинмониторинга, следственных органов и т.д.

Цель злоумышленников - убедить в том, что гражданин контролирует ситуацию и, если просто следовать инструкциям, то неприятных последствий удастся избежать.

ВАЖНО
Никогда и никому не передавайте код из СМС –
это ключ к вашему аккаунту и Вашим данным.

13. НАЧИНАЮЩИЙ ФОТОГРАФ

Преступники под видом начинающих фотографов связываются с моделями в соцсетях и предлагают свои услуги на выгодных условиях.

Затем лжефотографы отправляют жертвам ссылки на сайты «проверенных студий». Там предлагают выбрать время и дату съемки, оплатить аренду, услуги стилиста и реквизит.

После этого жертву направляют на другой домен, якобы относящийся к платежному сервису.
Указав данные карты, модель получает SMS с подтверждением и одноразовым кодом, который она вводит на мошенническом сайте.

Таким образом злоумышленники получают нужные им данные и выводят деньги с чужого счета.

14. ЛЖЕРИЕЛТОРЫ

Аналогичным образом действуют преступники, размещающие объявления о сдаче квартир и комнат в аренду. При согласовании объекта, периода и стоимости аренды, человеку поступает фишинговая ссылка на оплату.

15. СЛУЧАЙНЫЙ ПЕРЕВОД НА КАРТУ

Если на банковскую карту поступили средства от неизвестного отправителя, это может быть простой ошибкой. Но в отдельных ситуациях может быть началом мошеннической схемы.

ВАЖНО

1. Проверить счет: убедиться, что деньги действительно зачислены на счёт. Сообщение о зачислении средств может оказаться подделкой.

2. Связаться с банком: немедленно сообщить в банк о неожиданном поступлении средств. Банк зарегистрирует обращение и проведёт проверку.

3. Не тратить поступившие средства.

4. Не осуществлять самостоятельный возврат. Если с Вами свяжется отправитель денежных средств с просьбой вернуть деньги на другие реквизиты - не соглашаться. Это может быть мошенническая схема (например, с последующим шантажом в связи с переводом «террористу» или транзитным переводом украденных денег через карту). Все операции по возврату должны осуществляться через банк.

5.Сохранять записи общения: фиксировать все контакты с предполагаемым отправителем, включая звонки и сообщения.

ЗАЩИТИТЬСЯ ОТ КИБЕРПРЕСТУПНИКОВ МОЖНО ПРИДЕРЖИВАЯСЬ СЛЕДУЮЩИХ ПРАВИЛ:

1. Не передавать никому и никогда код из SMS или push-уведомлений

2. Устанавливать длинные и надежные пароли, усиленные биометрией и двухфакторной аутентификацией. Регулярно менять их.

3. Устанавливать оригинальные пароль, PIN-код и другие виды защиты для блокировки компьютера и телефона.

4. Выполнять регулярное резервное копирование данных на внешний жесткий диск.

5. Избегать публикации личной информации в соцсетях (номер телефона, фото, домашний и рабочий адреса, номера кредитных и банковских карт, местоположение).

6. Не принимать заявки в соцсетях от незнакомых и сомнительных людей.

7. При установке нового приложения проверять, к каким данным на устройстве запрашивается разрешение.

8. Регулярно обновлять программы, приложения и операционные системы. Старые версии могут быть более уязвимы для атак.

9. Отписываться от ненужных рассылок и подписок.

10. Не переходить по объявлениям и ссылкам, которые обещают скидки, призы и денежные выигрыши.

11. При использовании публичных сетей Wi-Fi быть аккуратным при открытии мобильного банка. Злоумышленники часто используют такие сети в своих целях.

12. Контролировать покупки в сети «Интернет».
Под видом онлайн-магазина могут быть мошенники.

13. Открепить неиспользуемый номер телефона
от портала «Госуслуг», онлайн-банка и других своих аккаунтов.

14. При продаже старых гаджетов отформатировать и очистить жесткий диск.

15. Использовать хорошее антивирусное программное обеспечение, регулярно проводить автоматическую проверку устройства на вредоносные программы.

*при подготовке настоящего материала использованы результаты обобщения практики прокурорского надзора прокуратуры Свердловской области, а также публикации Управления по организации борьбы с противоправным использованием информационно-коммуникацмонных технологий МВД России, (https://t.me/cyberpolice_rus, https://vk.com/cyberpolice_rus, https://t.me/cyberpolicerus_bot)