

ГАУ ДПО РБ «Бурятский республиканский институт
образовательной политики»
Региональный центр финансовой грамотности

ФИНАНСОВОЕ МОШЕННИЧЕСТВО

Практическое пособие для населения Республики Бурятия

Улан-Удэ, 2024

УДК 343.72(571.54)
ББК 65.261(2Рос=Бур)
Ф 59

Утверждено научно-методическим советом ГАУ ДПО РБ «БРИОП»
№ 2 от 21.05.2024 г.

Составители:

Хобраков С. Ц., к.полит.н., руководитель РЦФГ ГАУ ДПО РБ «БРИОП»
Базаржапов Б.Б., начальник отдела по борьбе с противоправным использо-
ванием информационно-телекоммуникационных технологий Министерства
внутренних дел по Республике Бурятия
Бадмаева Е.В., методист РЦФГ ГАУ ДПО РБ «БРИОП»

Ф 59

Финансовое мошенничество: практическое пособие для населения Респу-
блики Бурятия / Сост.: Хобраков С. Ц., Базаржапов Б.Б., Бадмаева Е.В. - Улан-У-
дэ: ГАУ ДПО РБ «БРИОП», 2024. – 26с.

Практическое пособие призвано помочь населению Республики Бурятия

65.261(2Рос=Бур)

©ГАУ ДПО РБ «БРИОП», 2024

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	4
О ДЕЯТЕЛЬНОСТИ РЕГИОНАЛЬНОГО ЦЕНТРА ФИНАНСОВОЙ ГРАМОТНОСТИ	5
Основные способы мошенничеств, совершенных с применением информационно-коммуникационных технологий	7
Виды и способы совершения ИТТ-преступлений.....	8
Телефонное мошенничество	11
Вирусы и программы удаленного доступа	18
Что делать, если у вас украли деньги.....	29

ВВЕДЕНИЕ

Финансовое мошенничество — это одна из самых распространенных и опасных форм преступлений в современном мире. Оно может нанести серьезный ущерб не только отдельным гражданам и организациям, но и всей экономике страны.

Мошенничество в сфере финансов — это противоправное действие, совершаемое с целью завладения денежными средствами, имуществом или другими материальными ценностями. На сегодняшний день существует множество видов финансовых мошенничеств, принципы которых часто основываются на психологических эффектах и внушении ложных надежд.

По данным экспертов в области кибербезопасности, объем мошенничества в России на сегодня оценивается в сумму от 55 до 150 миллиардов рублей в год. На социальную инженерию приходится 90 процентов всех финансовых преступлений, причем 94 процента из них — это телефонное мошенничество. По мере совершенствования системы кибербезопасности растут и возможности аферистов, которые придумывают все новые способы воровства денег с банковских карт при помощи телефона и интернета.

Тем не менее, уберечься от мошенничества совсем несложно, если вы знакомы с признаками, которые на него указывают.

В данном методическом материале рассмотрены основные способы мошенничеств, совершенных с применением информационно-коммуникационных технологий.

О ДЕЯТЕЛЬНОСТИ РЕГИОНАЛЬНОГО ЦЕНТРА ФИНАНСОВОЙ ГРАМОТНОСТИ

Региональный центр финансовой грамотности (РЦФГ) создан на базе ГАУ ДПО РБ «Бурятский республиканский институт образовательной политики» на основании Приказа министерства образования и науки Республики Бурятия от 21.01.2021 № 144.

РЦФГ координирует деятельность членов Межведомственной координационной комиссии по реализации Региональной программы повышения финансовой грамотности и формирования финансовой культуры населения Республики Бурятия, куда входят 38 министерств и ведомств Республики Бурятия.

Важный показатель деятельности РЦФГ — место во Всероссийском финансовом онлан- зачете, который проходит ежегодно. В 2023 году во Всероссийском онлайн — зачете по финансовой грамотности Республика Бурятия заняла 7 место по качеству знаний и 2 место по количеству участников.

Основное направление деятельности РЦФГ — повышение квалификации педагогических работников в области финансовой грамотности. Разработаны курсы повышения квалификации педагогических работников по 7 программам, объемом 40 учебных часов. За 2021–2023 гг. обучено 2100 педагогов Республики Бурятия.

В каждом курсе особое внимание уделяется применению интерактивных технологий, такие как деловые игры, кейс — технологии, анализ практических ситуаций, проектировочные практикумы, мастер-классы, индивидуальные и групповые консультации, а также использованию цифровых образовательных ресурсов: сайты, порталы, мультфильмы, комиксы и т.д.

Кроме того РЦФГ проводит обучение волонтеров финансового просвещения, вожатых и методистов детских оздоровительных лагерей, финансовых консультантов, сотрудников муниципальных служб, кадровых служб, библиотечной системы.

Для увеличения охвата населения мероприятиями по финансовой грамотности РЦФГ ежегодно проводит конкурсы: образовательных программ, рисунков, комиксов, видеороликов, журналистов, освещающих темы финансовой грамотности, лучший педагог по финансовой грамотности.

Ежегодно весной и осенью на базе вузов Республики Бурятия проводятся Фестивали финансовой грамотности для детей и молодежи, а так же олимпиады по финансовой грамотности среди студентов вузов, профессиональных образовательных организаций, школьников.

Охват мероприятиями по финансовой грамотности ежегодно растет за счет реализации медиапроекта «Финансовая грамотность». В 2023 году заключены договора с газетами «Номером Один» и «Информ полис», телеканалами «Ариг Ус» и «АТВ». Выпущено 6 телевизионных роликов на каналах «Ариг Ус» и «АТВ», 306 информационных статей и публикаций на сайтах, в социальных сетях, 27 статей в газетах «Номер Один» и «Информ полис». Охват населения составил 380 тысяч человек.

В 2024 году в соответствии с новой Стратегией повышения финансовой грамотности и формирования финансовой культуры до 2030 года члены МКК приняли новую Региональную программу повышения финансовой грамотности и формирования финансовой культуры жителей Республики Бурятия до 2030 года и План мероприятий реализации региональной программы на 2024 год.

Стратегическая цель программы — формирование у большинства жителей Республики Бурятия ключевых элементов финансовой культуры (ценностей, установок и поведенческих практик), способствующих финансовому благополучию гражданина, семьи и общества.

Основные целевые группы, на которые направлена программа — это экономически активное население; граждане пенсионного и предпенсионного возраста; обучающиеся образовательных организаций; субъекты малого и среднего предпринимательства.

Более подробно о деятельности РЦФГ можно посмотреть на сайте <https://finbriop.ru/>, в социальных сетях в ВК — <https://vk.com/rcfg03>, в телеграм — <https://t.me/fingram03>.

Основные способы мошенничеств, совершенных с применением информационно-коммуникационных технологий

Жулики умело манипулируют эмоциями, страхами и желаниями. Люди, столкнувшиеся с жертвами аферистов, отмечают, что пострадавшие выглядят взволнованно, растерянно и напугано.

Причем зачастую на уловки попадают не только пенсионеры или молодежь, но и взрослые образованные люди, которые не раз слышали о способах развода по телефону и были готовы отдать отпор.

К каким чувствам взывают мошенники?

— Страх — за деньги, близких, имущество или перед авторитетными лицами;

— Жадность — желание получить быструю выгоду, выигрыш, подарок;

— Любопытство — у нас есть твое фото, скорее переходи по ссылке;

— Сочувствие- желание помочь близким людям, коллегам.

А чаще всего они создают коктейль из эмоций: «Ваши деньги хотят снять со счет, нужно действовать срочно, под угрозой все накопления!». И человек в шоковом состоянии готов делать то что бы он не сделал в обычном состоянии.

Мошенники хорошо владеют приемами из психологии, актёрского мастерства, а так же приемами фотошопа и нейросетями. Они разыгрывают настоящий спектакль со множеством персонажей и реквизитом, отчего их действия выглядят очень убедительно.

Как распознать мошенников, ниже представлены признаки того, что вам звонят аферисты:

1. Пугают и торопят
2. Давят авторитетом
3. Разными способами выпытывают код из СМС
4. Просят назвать трехзначный код с оборота банковской карты (CVC)

5. Не могут предоставить информацию о счете или ответить на простые вопросы
6. Заставляют перейти по ссылке или установить приложение
7. Обещают быструю и большую выгоду

Виды и способы совершения ИТТ-преступлений

Современные телефонные мошенники — тонкие психологи с поставленной речью, обладающие даром убеждения. Как тут не поверить, если звонящий называет точные ФИО, дату рождения и даже место проживания.

На самом деле персональные данные узнать несложно. Люди, регистрируясь в онлайн-магазинах и различных порталах, указывают личную информацию, которая уходит в неизвестном направлении. Так аферисты получают доступ к огромной базе данных и используют ее в преступных целях.

Схема не новая, но до сих пор многие люди попадают в ловушку и переводят кибераферистам десятки тысяч кровно заработанных.

Суть мошеннической уловки: звонит «специалист» службы безопасности и огорошивает сообщением о якобы подозрительной операции со счетом. Кто-то пытается списать кругленькую сумму с карты, хочет оформить ипотеку или сменить номер для получения смс-уведомлений — легенд для обмана очень много. А цель всегда одна — напугать человека и украсть все его деньги.

Чтобы отменить операцию, лжесотрудник просит назвать код из СМС, сообщить номер карты, CVV-код, перейти по ссылке, которая оказывается вредоносной и поселяет в телефоне опасный вирус.

Современные телефонные мошенники — тонкие психологи с поставленной речью, обладающие даром убеждения. Как тут не поверить, если звонящий называет точные ФИО, дату рождения и даже место проживания.

На самом деле персональные данные узнать несложно. Люди, регистрируясь в онлайн-магазинах и различных порталах, указывают личную информацию, которая уходит в неизвестном направлении. Так аферисты получают доступ к огромной базе данных и используют ее в преступных целях.

Не так давно появился новый способ мошенничества по телефону.

Теперь злоумышленники не выманивают информацию о банковской карте, а просят установить специальное приложение якобы для проверки смартфона на фишинговые сервисы, через которые могут утекать личные данные и даже деньги.

Под видом антивируса жертва скачивает программу для удаленного доступа, через которую аферист подключается к устройству, крадет данные и денежные средства.

Важно: не скачивайте сторонние программы, не переходите по ссылкам в СМС с неизвестных номеров или электронных адресов.

Что делать: настоящие сотрудники службы безопасности банка почти никогда не звонят. В случае подозрительной транзакции со счетами присылают смс либо уведомление в мобильный банкинг. Но если вам все-таки поступил звонок, сразу повесьте трубку, позвоните на горячую линию банка или обратитесь напрямую в ближайшее отделение.

Звонок от следователя

Звонящий представляется сотрудником полиции или ФСБ и грозно сообщает: «Вы обвиняетесь в госизмене»; «Вам грозит штраф» или «Ваш родственник замешан в деле». Такие заявления могут выбить из колеи любого человека, особенно доверчивых пожилых людей.

В этом случае телефонные мошенники создают максимально стрессовую атмосферу: говорят в агрессивном тоне, называют по имени, знают информацию о «попавшем в беду» родственнике, обвиняют в пособничестве и угрожают тюрьмой.

Цель мошеннического сценария одна — выманить «взятку». Аферист называет «плату за спасение», просит отправить деньги на карту или пополнить криптокошелек.

Что делать: в идеале сразу класть трубку. Или можно попросить отправить всю информацию в письменной форме на почтовый ящик. Преступника не устроит такой сложный и долгий путь, и он сам не захочет продолжать разговор.

Другой способ — позвоните в отделение полиции и узнайте, обвиняетесь ли вы по какой-либо статье.

Звонок из Социального фонда и соцслужб

В последнее время популярностью пользуется еще один вид развода. В основном он нацелен на пенсионеров. Кибераферисты приговариваются соцработниками и предлагают обновить социальные карты.

Пенсионеры с радостью соглашаются на такую помощь — ведь им самим сложно вникнуть в технические нюансы. Они называют код и номер банковской карточки. Украд данные, злоумышленники получают доступ в мобильный банк и могут легко списать все денежные накопления.

Важно: не сообщайте номер карты, код из смс и тем более паспортные данные незнакомцам по телефону. При необходимости лучше обратиться в отделение банка и на месте решить финансовые вопросы.

А чтобы не переживать за сохранность денег, расплачивайтесь специальным стикером от банка.

В настоящее время можно выделить **3 группы** мошенничеств, совершаемых с применением информационно-телекоммуникационных технологий:

1. **Телефонные мошенничества** — мошенничества с использованием средств сотовой связи;

2. **Кибермошенничества** — вирусное заражение смартфона для получения доступа к данным, системам онлайн банкинга для последующего похищения денежных средств со счета;

3. **Мошенничества, совершаемые в сети интернет** — мошенничества при покупках или продажах через сеть Интернет (онлайн магазины, соц.сети), оказание услуг, а также финансовые пирамиды, фиктивные инвестиции.



Телефонное мошенничество

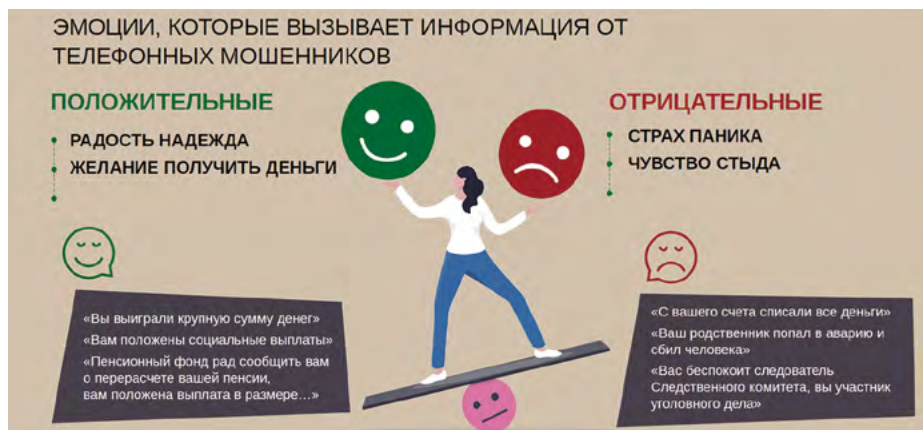
Первый вид телефонные мошенничества — это мошенничества с использованием средств сотовой связи

Телефонное мошенничество:



Обман в ходе телефонного разговора

«СРОЧНЫЙ ЗВОНОК» — в ходе телефонного разговора злоумышленники представляются: сотрудниками банка, правоохранительных органов, социальных служб, специалистами портала «Госуслуги», близкими родственниками, сообщают о проблемной ситуации, требующей незамедлительного реагирования.



Например: третьи лица пытаются оформить кредит, по банковской карте/счету производятся/совершены подозрительные операции, банковский счет заблокирован, близкий родственник попал в беду, необходимы деньги и др., после чего предлагают потерпевшему в целях решения проблемы совершить следующие действия:

- Произвести операции по указанию злоумышленника через банкомат или в режиме онлайн через приложение;
- Скачать под видом антивирусного или иного приложения для безопасности, программу удаленного доступа;
- Снять денежные средства с банковского счета/карты, оформить кредит, а после перевести денежные средства на «специальный безопасный счет»;
- Сообщить номер банковской карты, CVC — код, коды из СМС сообщений;
- Передать денежные средства третьему лицу.

Примеры:

1. Гр. В. позвонили неустановленные лица, представились сотрудниками полиции, сообщили, что мошенники оформили на его имя кредит в сумме 300 000 рублей. Для отмены всех операций необходимо подать встречную заявку для понижения кредитного потенциала и перевести деньги на «застрахованные, безопасные» банковские счета. Заявитель оформил онлайн-кредит, перевел деньги злоумышленникам.



2. Гр. Д. позвонили неустановленные лица, которые представились сотрудниками полиции, в ходе разговора сообщили, что родственник попал в аварию ему требуется дорогостоящая операция, для ее проведения срочно необходимо перевести денежные средства (передать курьеру).

Способы защиты от телефонных мошенничеств:

- Не отвечайте на звонки с незнакомых номеров;
- Прервите разговор, если разговор касается финансовых вопросов;
- Не торопитесь принимать решения;
- Позвоните своим близким родственникам и проверьте информацию в «Интернете»;

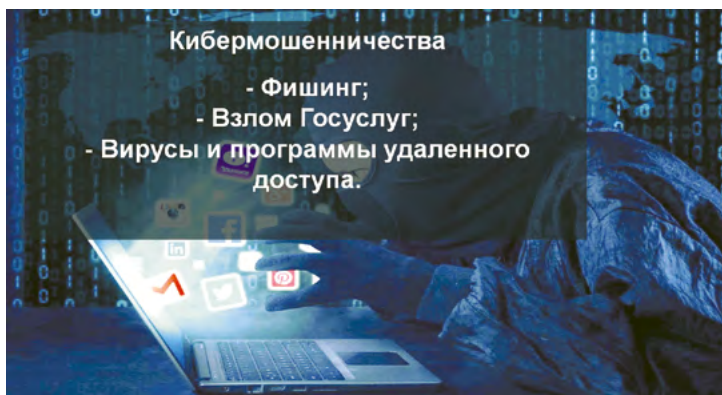
- Не перезванивайте по незнакомым номерам;
- Самостоятельно позвоните в полицию, банк или организацию;
- Не сообщайте сведения о картах особенно CVV/CVC-коды, не производите манипуляции при помощи банкомата;



Второй вид — Кибермошенничество

В настоящее время выделяют **3 вида** кибермошенничеств:

- «Фишинг» (сайты двойники);
- Взлом Госуслуг;
- Вирусы и программы удаленного доступа.



Фишинг — сайт двойник или зеркальный сайт

Преступником создается сайт «двойник», визуально схожий на какой-либо известный официальный сайт (в названии имеются отличия).

При проверке необходимо обратить внимание на домен (имя) сайта: мошенники заменяют буквы символами — например, ЦИФРА 1 вместо БУКВЫ «l» (onL1ne вместо onLine); Имя сайта максимально приближено к оригиналу (onLLine.sberbank.ru вместо onLine.sberbank.ru). Фейковый сайт может располагаться в нестандартной зоне, например rzd.INFO или rzd.NET, когда оригинал: rzd.RU;

ФИШИНГ

Мошенники создают сайты двойники с целью:

- Списания денег путем выманивания у жертв банковских сведений для совершения ПЛАТЕЖЕЙ/ПЕРЕВОДОВ;
- Взлома аккаунтов социальных сетей, портала Госуслуг и др.;
- Заражения устройств жертвы «Вирусом».

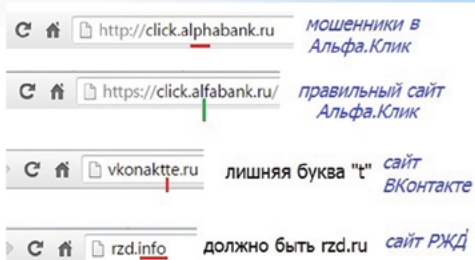
Пример: Гр. А. в сети интернет нашел ссылку на сайт по приобретению билетов со скидками в кинотеатры г. Улан-Удэ. Перейдя по ссылке забронировал билеты на 2 персоны и произвел оплату, в результате чего произошло списание денежных средств в сумме 8978 рублей.

Взлом личного кабинета портала «Госуслуги», социальных сетей: «В контакте», «Одноклассники», мессенджеры «Телеграмм», «Вайбер», «Ватсап»

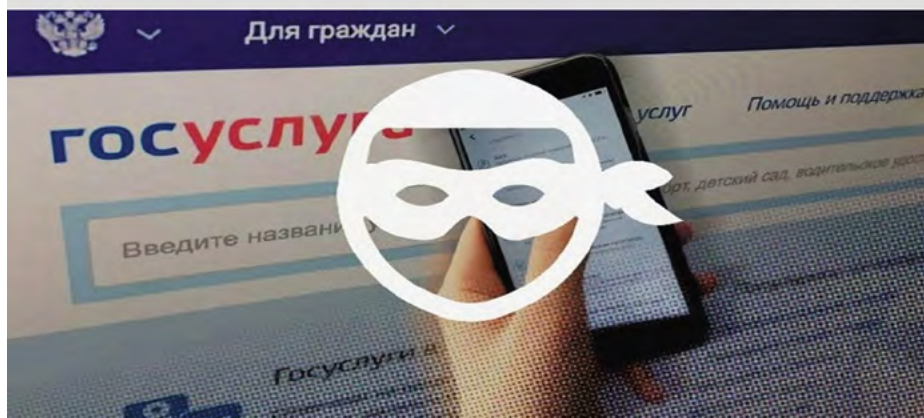
КАК РАСПОЗНАТЬ САЙТ ДВОЙНИК

▶ ПРИ ПРОВЕРКЕ ОБРАТИТЕ ВНИМАНИЕ НА ДОМЕН (ИМЯ) САЙТА:

- ▶ Мошенники заменяют буквы символами – например, **ЦИФРА 1** вместо **БУКВЫ «l»** (onL1ne вместо onLine);
- ▶ Имя сайта максимально приближено к оригиналу (onLLine.sberbank.ru вместо onLine.sberbank.ru);
- ▶ В некоторых случаях для написания домена используются буквы похожие на латинские из алфавита другого языка;
- ▶ Фейковый сайт может располагаться в нестандартной зоне, например rzd.INFO или rzd.NET, когда оригинал: rzd.RU



Взлом личного кабинета Госуслуг



Злоумышленниками осуществляется неправомерный доступ (взлом) к личным кабинетам портала «Госуслуги», с последующим оформлением микрозаймов.

Взлом аккаунтов в социальных сетях/мессенджерах осуществляется с целью хищения денежных средств под предлогом их займа

у находящихся в друзьях пользователей. Получившие доступ к аккаунту, злоумышленники вымогают средства под угрозой распространения личной переписки/фотографий компрометирующего характера.

Как мошенники получают доступ к Госуслугам

- ▶ Телефонный звонок от «оператора сотовой связи». -Сообщают что необходимо продлить срок действия сим-карты или обновить паспортные данные.
- ▶ Телефонный звонок от «сотрудника портала Госуслуг». -Сообщают о подозрительной активности.
- ▶ В целях подтверждения личности, а так же под другим предлогом требуют сообщить/продиктовать СМС-код который поступит на телефон с портала Госуслуг.

В ЭТО ВРЕМЯ мошенники зная абонентский номер жертвы. На сайте Госуслуг открывают вкладку: «Восстановление пароля».

госуслуги

Восстановление пароля

Номер телефона
890000000000

Указывают номер жертвы и ждут когда, им сообщать код из СМС.

Для аккаунтов где установлен вход на портал по смс-коду, мошенники просят повторно сообщить код, якобы первый код не действителен и не проходит. На самом деле повторно приходит КОД для изменения номера телефона.

госуслуги

Изменение номера телефона
+7 924

Новый номер телефона
+7 () - - - -

Пример: Гр. С. на сотовый телефон поступил звонок от оператора сотовой связи «МТС», который сообщил что заканчивается срок действия договора, предложил продлить дистанционно, сообщив поступивший код в смс — сообщении. После поступил звонок от работника портала «Госуслуги» и сообщил, что мошенники пытаются взломать личный кабинет, и для предотвращения мошеннических попросил продиктовать пришедшие в СМС коды. В результате взлома личного кабинета на портале «Госуслуги» на гр. С. оформлены микрозаймы.

Способ защиты:

1. НИКОМУ НЕ СООБЩАЙТЕ КОД ИЗ СМС-СООБЩЕНИЯ ПОСТУПИВШИЙ С ПОРТАЛА ГОСУС.ПУТ.

2. Действующие
АО "БАНК * * * * *
- действует до 28.11.54
Цель запроса
« Формирование финансовых и нефинансовых предложений
- Согласия
- В ЛИЧНОМ КАБИНЕТЕ, ЗАЙТИ В «ПРОФИЛЬ»;
– ВЫБРАТЬ РАЗДЕЛ «СОГЛАСИЯ И ДОВЕРЕННОСТИ»;
– ОТОЗВАТЬ СОГЛАСИЯ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ У БАНКОВСКИХ ОРГАНИЗАЦИЙ.

3. НАСТРОИТЬ ВХОД НА ГОСУСЛУГИ ПО ПАРОЛЮ И КОДУ ИЗ СМС-СООБЩЕНИЯ.

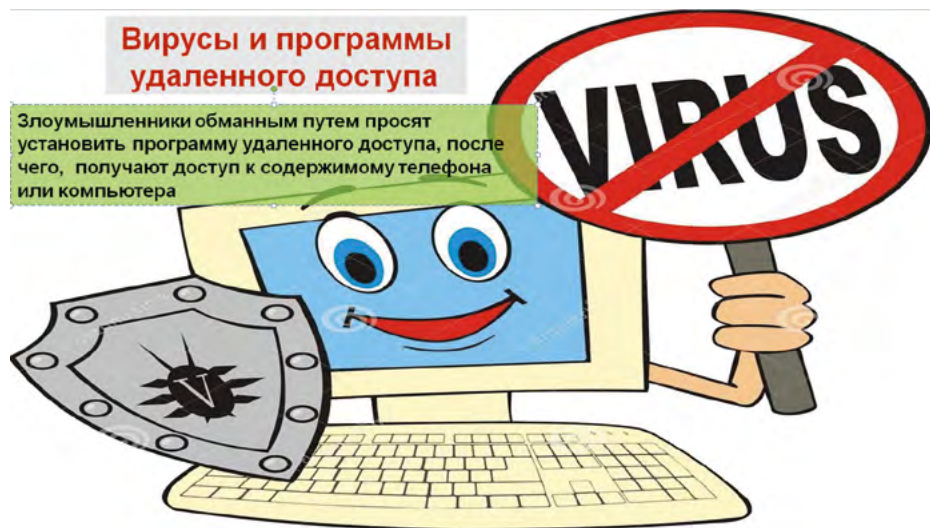
4. РЕГУЛЯРНО, РАЗ В ПОЛГОДА, МЕНЯТЬ ПАРОЛИ ДОСТУПА.

Вирусы и программы удаленного доступа

Потерпевшим по указанию злоумышленника, устанавливается программа удаленного доступа, под видом антивируса, после чего, преступник получает доступ к содержимому телефона или компьютера потерпевшего.

Вирусы и программы удаленного доступа

Злоумышленники обманным путем просят установить программу удаленного доступа, после чего, получают доступ к содержимому телефона или компьютера



В результате взлома мессенджера («ватсап», «вайбер», «телеграм») производится рассылка всем контактам с интернет-ссылкой следующего содержания: «Проголосуй за моего племянника», после перехода по указанной ссылке на телефон устанавливается вирус (программа шпион) которая в последующем может быть использована для совершения вышеперечисленных мошенничеств.

Способы защиты:

— При проверке необходимо обратить внимание на домен (имя) сайта: мошенники заменяют буквы символами — например, ЦИФРА 1 вместо БУКВЫ «l» (onL1ne вместо onLine). Имя сайта максимально приближено к оригиналу (onLLine.sberbank.ru вместо onLine.sberbank.ru). Фейковый сайт может располагаться в нестандартной зоне, например rzd.INFO или rzd.NET, когда оригинал: rzd.RU; 4

**В целях безопасности
рекомендуется использовать: «Программы по
блокировке спам-звонков» и «Антивирусы»**

**«ПРОГРАММЫ ПО БЛОКИРОВКЕ
СПАМ-ЗВОНКОВ»:**

- ▶ Наиболее популярные приложения: «Who Calls», «Truecaller», «Не звони мне», «Call Blocker», «Яндекс антиспам».
- ▶ У всех операторов сотовой связи имеется услуга «Антиспам»

«АНТИВИРУСЫ»:

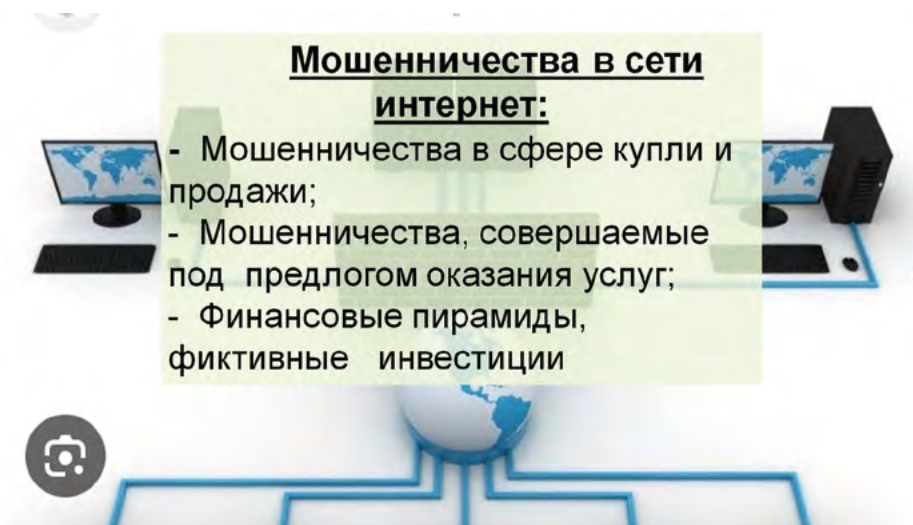
- ▶ Популярные «Касперский», «Avast», «ESET», «NORTON».
- ▶ У антивирусов имеется функция защиты от фишинговых сайтов, подозрительных ссылок;
- ▶ Защита от утечки данных;
- ▶ Функция «Антивор» для удаленной блокировки, очистки и поиска телефона

Никому не сообщайте код из СМС-сообщения, поступивший с портала «Госуслуги». Настройте вход на портал «Госуслуги» по паролю и коду из СМС-сообщения. Регулярно, раз в полгода, меняйте пароли доступа;

— В целях безопасности рекомендуется использовать программы по блокировке спам-звонков, и «Антивирусы».

3-й вид мошенничества, совершаемые в сети интернет

Мошенничества при покупках или продажах через сеть Интернет (онлайн магазины, соц. сети), оказание услуг, а также финансовые пирамиды, фиктивные инвестиции.



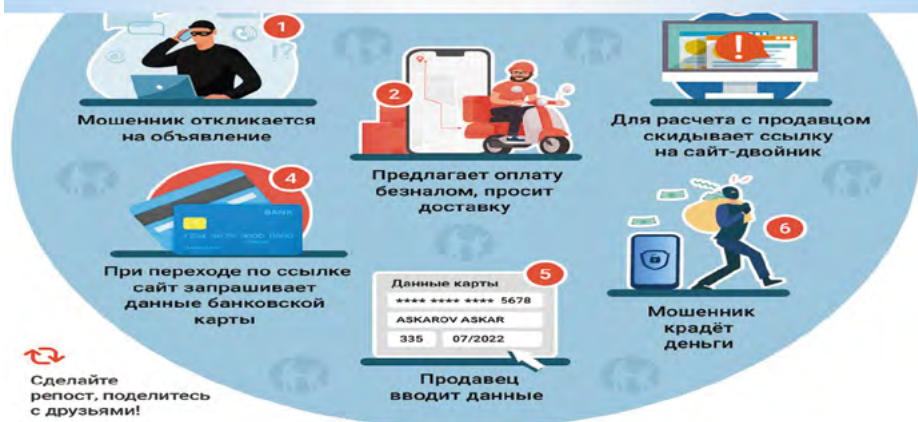
В настоящее время выделяют **3 способа** мошенничества, совершаемые в сети интернет:

- Мошенничества в сфере купли и продажи;
- Мошенничества, совершаемые под предлогом оказания услуг;
- Финансовые пирамиды, фиктивные инвестиции.

Мошенничества в сфере купли и продажи:

Преступления, совершенные с использованием или применением социальных сетей. Преступником в сети «Интернет» создается сообщество (группа) по продаже какой — либо продукции (Авито, Дром и т.д.).

Мошенничества в сфере купли и продажи



Мошенник откликается на объявление и предлагает оплату безналичным путем, просит доставку, для расчета с продавцом скидывает ссылку на сайт — двойник. При переходе по ссылке сайт запрашивает данные банковской карты, далее продавец вводит данные, а мошенник крадет деньги с банковской карты.

Мошенник покупатель

СХЕМА ОБМАНА:

- ▶ 1. Мошенник откликается на объявление.
- ▶ 2. Предлагает оплату безналичным способом, просит осуществить доставку;
- ▶ 3. Под предлогом осуществления безопасной сделки скидывает продавцу ссылку на сайт двойник;
- ▶ 4. При переходе по ссылке сайт запрашивает данные банковской карты (номер карты, защитный CVV-код карты, код из СМС);
- ▶ 5. Продавец (жертва) вводит требуемые данные карты.
- ▶ 6. Мошенник **КРАДЕТ ДЕНЬГИ**.

Следующая схема: мошенник — продавец. Продавец — мошенник размещает заманчивое предложение, как правило, цена на товар гораздо ниже рыночной. Продавец просит внести предоплату или оплатить полную сумму, после оплаты, продавец перестает выходить на связь.

Мошенник - продавец

СХЕМА ОБМАНА:

- ▶ 1. Продавец-мошенник размещает в сети интернет заманчивое объявление о продаже товара.
- ▶ 2. Жертва откликается на объявление, оговаривают условия купли-продажи.
- ▶ 3. Продавец-мошенник просит внести предоплату или оплатить полную стоимость товара;
- ▶ 4. Жертва совершает оплату/предоплату.
- ▶ 5. Продавец -мошенник перестает выходить на связь.

Для того чтобы не попасть на уловки мошенников проверьте продавца/покупателя при помощи различных сервисов, например на сайте «Доверие в сети».

Проверьте продавца/покупателя при помощи различных сервисов. Например на сайте «Доверие в сети»

 [Регистрация](#) [Статьи](#) [Топ 100 сайтов](#) [Логин](#)

ПРОВЕРКА НА МОШЕННИЧЕСТВО

Сайты

Соцсети

Телефоны

Адрес сайта

Примеры:

1. Гр. И. на сайте «Авито» выложила объявление о продаже детской коляски, после с ней связался покупатель который пояснил, что хочет его приобрести для себя безопасным способом через «Авито-доставка». После чего он скинул в мессенджере «Ватсап» ссылку для безопасной сделки. Пройдя по ссылке потерпевшая указала реквизиты своей банковской карты на которую должна была поступить оплата. Далее ей на сотовый телефон пришел пароль, который она также указала в ссылке, в результате со счета были списаны денежные средства в сумме 9700 рублей.

Мошенник продавец

Признаки мошенничества

		Отказ от личной встречи		Отказ от наложенного платежа
	Заниженная стоимость товара		Требование предоплаты	
	Необходимо перейти по ссылке на сайт (двойник) для безопасной сделки		Настойчивые просьбы быстрее оплатить товар	

► *Насторожитесь если номерная емкость телефона продавца не соответствует региону его местонахождения

2. Гр. В. на сайте «Авито» увидел объявление о продаже двигателя по цене ниже рыночной стоимости. В ходе телефонного разговора с продавцом последний попросил перевести задаток, так как у него имеются еще клиенты на данный двигатель. Гр. В. перевел продавцу денежные средства в сумме 25 000 рублей по указанному в объявлении абонентскому номеру, после чего объявление было снято с публикации, продавец перестал выходить на связь. 5

Мошенничества совершенные под предлогом оказания услуг, заработка

Преступником используются различные программы (приложения) («вайбер», «ватсап», «телеграмм») для того, чтобы вступить в переписку с потерпевшим.



Пример: 1. гр. А. размещает объявление о поиске работы на различных сайтах (Авито.вакансии, hh.ru и др.) после чего с ним связываются и предлагают удаленную работу, далее ему рекомендуют пройти верификацию или подтвердить личность через приложение дистанционного банковского обслуживания, действуя по указанию злоумышленников, гр. А. предоставляет доступ к своим счетам.

МОШЕННИЧЕСТВА ПОД ПРЕДЛОГОМ ОКАЗАНИЯ УСЛУГ



- ▶ Поиск работы через интернет;
- ▶ Поиск услуг по доставке товаров.

ПОСЛЕ РАЗМЕЩЕНИЯ ОБЪЯВЛЕНИЯ О
ПОИСКЕ РАБОТЫ:

- поступает звонок менеджера;
- проводит опрос, оговаривает условия работы.

ДАЛЕЕ МОШЕННИКИ ПРЕДЛАГАЮТ:

- пройти платные курсы;
- зарегистрироваться на сайте, с подтверждением личности посредством ввода СМС-кода;
- зарегистрировать банковскую карту для получения заработной платы, подтверждая кодом из СМС.

**НА САМОМ ДЕЛЕ СМС-КОД НЕОБХОДИМ
ДЛЯ ВХОДА В БАНКОВСКОЕ
ПРИЛОЖЕНИЕ, ЛИБО ЛИЧНЫЙ КАБИНЕТ
ПОРТАЛА ГОСУСЛУГ**

Так же имеются случаи мошенничества под предлогом заработка от продаж на популярных марке «Вайлдберриз» и «Озон», либо под предлогом накрутки рейтинга положительных отзывов.

WB

Мошенники предлагают:

ozon

- Зарабатывать на оценке товара (ставить «лайки»);

- «закупать» товар для реализации, при этом денежные средства на «закуп» впоследствии поступают мошенникам.

- Перейти по ссылке на сайт маркетплейса, при этом вы попадаете на сайт двойник, где при регистрации требуется внесение персональных данных, в том числе коды из СМС-сообщений

Финансовые пирамиды, фиктивные инвестиции

Злоумышленники под видом участия в торгах на «бирже», создают сайты, на которых в личных кабинетах размещают информацию о приросте денежных средств, вложенных потерпевшим под видом инвестиций.

Как себя обезопасить:

- ▶ Поиск информации о компании в открытых источниках. Если не имеется никаких сведений — это повод насторожиться.
- ▶ Не совершайте платежи/переводы в адрес потенциального работодателя (даже если вам объясняют их необходимость для будущей работы — например, плата за вводное обучение, рабочую форму или рабочие инструменты).
- ▶ Не сообщайте/не указывайте коды из поступивших смс-сообщений;
- ▶ Не выполняйте действия в «Банковских приложениях» по чьей либо просьбе/указанию (Например для открытия «Рабочего счета» и др.)

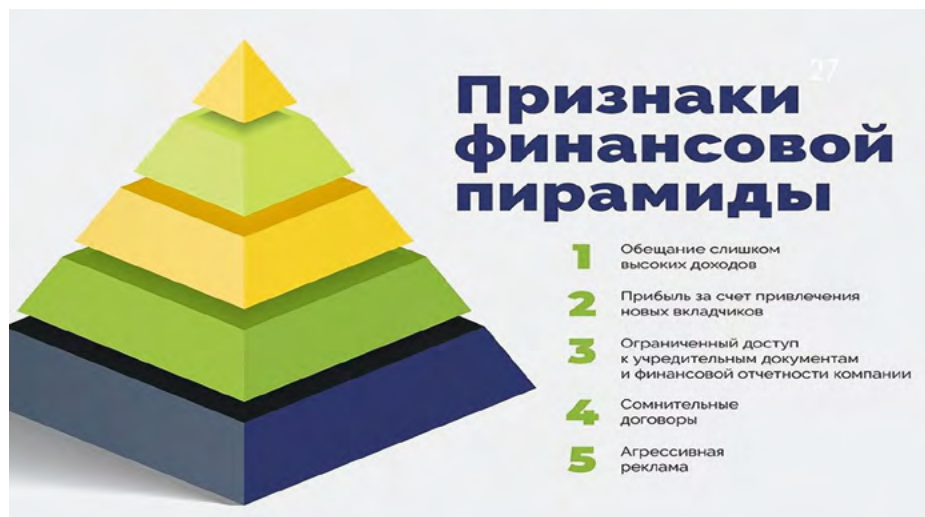
Пример:

1. Гр. А. оформил дебетовую и кредитную банковскую карты АО «Тинькофф банк» и подключил услугу «Инвестиции». Далее на сотовый телефон гр. А. позвонил мужчина, который представился сотрудником банка АО «Тинькофф банк» и предложил заработать на инвестициях, установив приложение «Bybit» для обмена денежных средств на криптовалюту, и приложение «Терминал» для пополнения счета. После установки приложения заявитель перевел с денежные средства в сумме 10 000 руб. на счет приложения «Терминал», где через некоторое время увидел, что сумма повысилась на 1 800 руб. Далее гр. А. предложили получить еще больше прибыли, заявитель вновь внес денежные средства в сумме 180 000 руб., 600 000 руб., и 500.000 руб. После пришло уведомление о том, что приложение «Терминал» заблокировано, для разблокировки необходимо внести 1 000 000 руб.

Гр. А. оформил несколько кредитов в ПАО «Сбербанк», АО «Тинькофф банк» на супругу в сумме 1 986 000 руб. и совершал переводы злоумышленникам, полагая, что инвестирует свои денежные средства.



Способы защиты:



— Покупайте и продавайте из рук в руки, не осуществляйте предоплату, называйте только абонентский номер для перевода денежных средств, этого достаточно для осуществления перевода. Настаивайте на наложенном платеже без предоплаты, проверяйте данные покупателя и продавца в интернете, не переходите по неизвестным ссылкам;

— Не совершайте платежи/переводы в адрес потенциального работодателя, даже если вам объясняют их необходимость для будущей работы, например, плата за обучение, рабочую форму или рабочие инструменты. Не выполняйте действия в «Банковских приложениях» по указанию посторонних лиц, например для открытия «Рабочего счета» и др.;

— Проверяйте брокерскую компанию на сайте Банка России на наличие лицензии, не доверяйте рекламе о биржах в социальных сетях, внимательно читайте пункты договора (если он составляется). Не верьте заманчивым и убедительным словам о высоких доходах при низком риске.

Как себя обезопасить:

- ▶ **Проверить брокерскую компанию на сайте Банка России на наличие лицензии;**
- ▶ **Не доверять рекламе о биржах в социальных сетях;**
- ▶ **Не верить заманчивым и убедительным обещаниям о высокой доходности и отсутствии риска**

Внимание! **Как не стать жертвой мошенников**

- Не отвечайте на подозрительные звонки, не перезванивайте на незнакомые номера;
- Прервите разговор если он касается финансовых вопросов;
- Проверьте информацию в Интернете или обратитесь за помощью к близким родственникам, самостоятельно позвоните в банк или организацию;
- Не сообщайте сведения о банковских картах, CVV/CVC-коды;
- Не кому не перечисляйте денежные средства;
- Не переходите по ссылкам, не устанавливайте приложения поступившие по ссылке в СМС-сообщениях;
- В случае утери или кражи телефона с подключенной услугой «Мобильный банк» необходимо обратиться в контактный центр Банка для блокировки услуги, также необходимо заблокировать SIM-карту;

Что делать, если у вас украли деньги

Если данные вашей карты попали мошенникам, срочно заблокируйте счет.

Если это пароль или логин от онлайн — банка — смените данные и заблокируйте счет. Также позвоните на горячую линию банка, чтобы убедиться что вы приняли все возможные меры предосторожности.

А если деньги уже списали — обратитесь в полицию. Напишите заявление, дайте подробную информацию о происшествии: данные звонящего, скриншоты переписки, запись звонка, списанную сумму. Основание — статья 159 УК РФ. Заявление рассматривают в течении трех суток с возможностью продления до месяца, если это необходимо для принятия мотивированного решения.

Если деньги еще не успели снять, вы все равно хотите сообщить полиции о факте мошенничества, напишите заявление, ссылаясь на статью 30 УК РФ. Возможно, правоохранители с вашей помощью смогут выйти на злоумышленников.

Одна из старейших мошеннических схем, применяемых до сих пор, нацелена прежде всего на пожилых людей: это трюк с «попавшим в беду родственником». Скорее всего, почти все о нем слышали: звонящий в крайне эмоциональном тоне убеждает, что близкий вам

человек стал виновником ДТП, попался с наркотиками или совершил какое-либо другое серьезное правонарушение. Как следует, запугав собеседника и добившись желаемого психологического эффекта, преступник затем заговорщицки намекает, что «можно договориться» — и родственник избежит положенного наказания. Затем трубку передают «сотруднику силовых структур», который развивает напор и уточняет детали.

В зависимости от наглости мошенников сумма может варьироваться от 10–15 тысяч рублей до миллиона и даже больше. Деньги потребуют либо перевести сразу на карту, либо передать посреднику (обычно их нанимают из молодых и не особенно одаренных людей; в среднем курьер успевает поучаствовать в двух-трех делах, после чего попадаетесь полицейским и отвечает перед законом по полной, тогда как организаторы аферы могут находиться за границей).

Если вы заметили признаки мошенничества, лучше не рискуйте и перед тем, как принимать какое-либо решение, тщательно все изучите. Будьте осторожны и старайтесь работать только с доверенными и надежными организациями. Аферисты постоянно разрабатывают новые способы обмана, используя разнообразные методы и технологии. Однако существует несколько простых шагов, которые вы можете предпринять для защиты своих финансовых средств.

Первый и, возможно, самый важный шаг — это своевременное обеспечение безопасности своих банковских карт. Никогда не сообщайте данные своих карт третьим лицам. Храните карты в надежных местах или носите их с собой. Ограничьте количество карт, которые вы используете регулярно, и периодически проверяйте баланс на своих счетах.

Кроме того, для того чтобы убедиться, что ваши средства находятся в надежных руках, подключите СМС-банк. Это поможет вам оперативно получать информацию о статьях расходов и операциях, проводимых по вашей карте. Подумайте о том, чтобы установить ограничения на оплату, снятие наличных и переводы на другие карты.

В настоящее время многие мошеннические схемы происходят через интернет. Поэтому очень важно сохранять свои личные данные и не делиться ими с незнакомыми людьми. Никогда не переходите по подозрительным ссылкам и не открывайте приходящие на ваш элек-

тронный адрес сообщения и статьи от неизвестных отправителей.

Не забывайте проверять организации, с которыми вы сотрудничаете, даже если дело касается оказания бытовых услуг. Убедитесь, что они имеют соответствующие лицензии и разрешения на предоставление услуг.

Никогда не следует идти на компромисс, когда речь заходит о вашей финансовой безопасности. Всегда помните о своих правах, защищайте свои финансовые интересы и будьте бдительны, чтобы избежать финансовых мошенничеств.

Практическое пособие для населения Республики Бурятия

ФИНАНСОВОЕ МОШЕННИЧЕСТВО

Составители:

Хобраков Солбон Цыренжапович

Базаржапов Бато Баторович

Бадмаева Елена Владимировна