В Красноярском крае в 2023 году зарегистрировано более 15 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий, почти 12 тыс. из которых – это хищения денежных средств у граждан. Потерпевшим преступлениями причинен ущерб в размере почти 3 млрд рублей в 2023 году и более 270 млн в текущем году.

Раскрывается чуть более 20% преступлений, что связано с их совершением участниками высокоорганизованных преступных групп, колл-центры которых дислоцируются за пределами РФ.

Потерпевшими от киберпреступлений являются граждане абсолютно всех категорий, включая как социально-незащищенные слои населения (инвалиды, пенсионеры, несовершеннолетние), так и люди, занимающие руководящие посты в организациях (предприятиях) всех форм собственности, имеющие несколько высших образований.

Злоумышленниками используются изощренные способы «выманивая» денежных средств, для чего используются различные «легенды», посредством изложения которых оказывается психологическое воздействие на граждан, которые под его воздействием выполняют все команды злоумышленников. Многие из потерпевших в дальнейшем в ходе общения с сотрудниками правоохранительных органов сообщают, что действовали «под гипнозом», в результате профессиональной манипуляции со стороны преступников.

В ходе совершения преступлений злоумышленники используют звонки с номеров, визуально приближенных к номерам телефонов правоохранительных органов, служб банков (например звонки на Вайбер с номера +900, тогда как официальный номер Сбера 900 и т.д.), представляются официальными лицами.

Наиболее распространенными способами преступлений на сегодняшний день являются:

1. СМС от работодателя.

Потерпевшему поступает смс сообщение или сообщение в мессенджере от работодателя. О том, что с ним в ближайшее время свяжется сотрудник ФСБ или иной организации, следует с ним пообщаться.

После этого звонит сотрудник с именем указанным руководителем и сообщает о попытках перевода личных сбережений на иностранные счета / финансирование территоризма / украины и тп.

В целях пресечения преступных операций потерпевшего убеждают прервать транзакции путем перевода денег (личных накоплений или путем взятия кредита) на счет, указанный злоумышленниками.

2. Злоумышленники продают Вашу квартиру или машину.

Звонившие представляются представителями службы безопасности коммерческого банка, Гос услуг, Центрального банка либо правоохранительного органа.

Сообщают о том, что персональные данные с личного кабинета утекли и теперь преступники могут от Вашего

имени продать квартиру / машину, используя электронно-цифровую подпись.

В целях защиты имущества следует срочно его продать – перевести деньги на «защищенный канал», «безопасный счет», «резервную ячейку».

3. Перевод денег на «безопасный счет», якобы для их сохранности.

Звонившие представляются либо представителями службы безопасности коммерческого банка, Центрального банка либо правоохранительного органа и сообщают, что мошенники с использованием персональных данных потерпевшего оформляют кредиты в различных банках и для того, чтобы предотвратить хищение денег с банковского счета необходимо личные сбережения срочно перевести на «безопасные счета». В ходе дальнейшего общения потерпевшему сообщают о необходимости оформления кредитов и их перевода. Также зарегистрированы случаи продажи недвижимости и перевода мошенникам вырученных средств.

Следует отметить, что общение потерпевшего со злоумышленниками является длительным, в некоторых случаях осуществляется в течение нескольких месяцев, используется как телефонная связь, так и общение посредством мессенджеров (Ватсап, Вайбер, Телеграм и т.д.).

Еще одна разновидность преступной схемы – когда **звонят якобы сотрудники правоохранительных органов и сообщают что в отношении Вас возбуждено уголовное дело в связи с финансированием экстремисткой, террористической деятельности,**

поскольку с Вашего банковского счета осуществлен перевод денежных средств в недружественное государство.

В ходе общения злоумышленники могут присылать якобы фото удостоверений, повесток, постановлений о возбуждении уголовного дела, подписок о неразглашении следственной тайны и т.д. Нужно быть предельно внимательными, не поддаваться манипуляциям и проверять сообщаемую информацию,

Кроме того, следует помнить, что «безопасных счетов» не существует, а представители Центрального Банка не осуществляют работу с физическими лицами.

4. Звонок злоумышленника **под видом мобильных операторов, которые сообщают, что срок действия вашей сим-карты истек либо истекает, а для его продления необходимо сообщить** код, который поступит в смс либо пройти по ссылке, в противном случае сим-карта будет заблокирована.

Важно знать, что у сим-карты нет срока действия, сотовые операторы перевыпускают сим-карты только по просьбе потребителей в случае физического износа, потери, необходимости другого формата.

Выполнив требования мошенников и сообщив код из смс, либо пройдя по ссылке Вы отдаете в руки злоумышленников доступ в свой личный кабинет на сайте оператора связи, после чего мошенники имеют возможность устанавливать переадресацию сообщений на нужный им номер, что позволит сменить пароль от мобильного банка и похитить денежные средства.

Вторая разновидность таких преступлений –

получение в результате сообщения кода из смс доступа к аккаунту «госуслуг», дальнейшее оформление заявок на кредиты в банках, получение к персональным данным, таким как сведения о доходах, наличие банковских счетов и т.д.

5. Сдача налоговых деклараций и справок о доходах.

Звонившие представляются сотрудниками Госуслуг, управления по делам президента, сообщают, что в рамках декларационной компании проверяют персональные данные лиц, сдавших налоговые декларации либо декларации о доходах.

Для подтверждения следует назвать паспортные данные и код из СМС.

Результат – списание денег со счетов, взятие кредита.

6. **Взлом либо копирование аккаунта пользователя в мессенджерах ватсап, вайбер, телеграмм, социальных сетей вконтакте** и дальнейшее направление сгенерированных искусственным интеллектом (нейросетью) голосовых сообщений от имени потерпевшего, которое полностью копирует его голос, используя при этом ранее отправленные сообщения владельца аккаунта.

А дальше все по типичной схеме – просьба одолжить взаймы, фото банковской карты для перевода денежных средств.

В данной ситуации важно убедиться, что вы общаетесь именно с Вашим знакомым путем звонка по мобильной сети.

Сделав это, Вы обезопасите себя и предупредите знакомого о том, что от его имени действуют мошенники.

Для того, чтобы не потерять контроль над Вашим аккаунтом никогда не переходите по незнакомым ссылкам, не скачивайте программы из неподтвержденных источников, используйте двухфакторную аутентификацию Ваших аккаунтов.

Будьте максимально внимательны, поскольку следующим этапом использования искусственного интеллекта может явиться генерация видеоизображений и рассылка видеосообщений от имени родных, коллег, знакомых и т.д.

7. **хищение денежных средств через систему быстрых платежей (СБП).**

Например, покупатель на сайте оставляет заявку на приобретение товара, ему поступает звонок якобы от сотрудника магазина, предлагается скидка на товар, но только при условии оплаты через СБП или QR-коду, затем злоумышленник присылает в мессенджер ссылку, ведущую на страницу с формой оплаты по QR-коду. Покупатель подтверждает платеж и денежные средства поступают на счет мошенника.

Важно в такой ситуации связаться со службой поддержки онлайн-магазина, через официальный сайт или приложение. Не сохранять для оплаты в личных кабинетах банковские карты, при возможности заведите отдельную карту для оплаты покупок онлайн.

8. Широко получившая последнее время схема, в результате использования которой причиняется наиболее

крупный ущерб – **заработок на бирже, заманивание прибыльными инвестициями**. Преступниками создается максимальная видимость того, что общение происходит с представителями крупной инвестиционной площадки, их сайты имеют видимое сходство с банковскими организациями (например, Газпроминвестиции, РБК-инвестиции, Тинькофф-инвестиции и т.д.), назначается личный брокер, общение с которым может осуществляться даже посредством видеозвонков. Под их руководством создается якобы личный кабинет на торговой площадке, в котором отображаются все внесенные денежные средства, и прибыль. Однако их дальнейший вывод невозможен.

Например, в январе текущего года жительница г. Сосновоборск в сети интернет увидела псевдорекламу «Газпромбанка» о дополнительном заработке, ввела свои паспортные данные на сайте. спустя несколько дней с ней связался сотрудник торговой компании и рассказал о возможном росте финансовых накоплений в ходе торгов и дальнейшего вывода прибыли. Заинтересовавшись, женщина установила инвестиционную платформу и стала сотрудничать якобы с финансовым специалистом через приложение «скайп». Первоначально внесла депозит в размере 10 тыс, после чего увидела прибыль в размере 2 тыс, которые ей поступили на банковскую карту. Это придало веру в возможность зарабатывать. Обманутая женщина вносила личные денежные средства, которые получила путем оформления кредитов в различных банках, думая, что торгует газом, нефтью, серебром, акциями «Газпрома». В дальнейшем, при оформлении сделок, система стала выдавать ошибки. Лже-

специалисты поясняли, что необходимо оформить страховку и ряд других финансовых манипуляций, однако работа на платформе была заблокирована. Действуя по инструкции мошенников, потерпевшая перевела более 6 млн. руб.

9. рассылка налоговых писем о выявлении подозрительных транзакций и активности налогоплательщика.

В поддельном сообщении предлагается пройти дополнительную проверку и предоставить сведения по запросу налоговой службы. Так мошенники могут запросить кассовые документы, счета-фактуры, отчетные документы. Далее для прохождения проверки предлагается обратиться к указанному в письме инспектору под угрозой блокировки счетов налогоплательщика.

Важно помнить, что ФНС не рассылает такого рода письма и не имеет отношения к ним, такие письма открывать не рекомендуется, как и переходить по ссылкам.

Используемые мошенниками схемы постоянно меняются, «подстраиваясь» под общественно-политическую обстановку, значимые события в государстве. Распространены также следующие способы:

- обман во время кампании по сдаче налоговых деклараций (поступление письма от злоумышленников на электронную почту от якобы сотрудников налоговой службы с требованием представить декларацию по специальной ссылке при переходе на которую

необходимо ввести личные данные и реквизиты банковской карты якобы для идентификации налогоплательщика);

-хищение денег и имущества под предлогом обновления банкнот (звонок от мошенников с указанием о необходимости проверки подлинности банкнот Банка России, для чего убеждают установить стороннее приложение, посредством которого получают удаленный доступ к телефону жертвы; также используется поквартирный обход от якобы специалистов социальных служб, которые убеждают обменять денежные купюры на поддельные);

- использование ложных аккаунтов руководителей Банка России, правоохранительных органов, содержащих реальные данные, взятые из открытых источников (фамилию, имя, отчество, фото);

- сообщение клиентам банков об утечке персональных данных;

- обещание помочь с компенсацией ранее похищенных денег;

- обмен кэшбека на рубли.

8. Схема «Ваш родственник попал в ДТП», наиболее подвержены данному виду преступлений пожилые граждане. Злоумышленник представляется либо родственником потерпевшего либо представителем правоохранительного органа и сообщает, что для освобождения от уголовной ответственности и наказания в виде лишения свободы срочно необходимо передать денежные средства.

Как защититься от кибермошенничества. Правила безопасности в киберпространстве

Введение

Благодаря технологическому прогрессу интернет стал неотъемлемой частью нашей повседневной жизни. Он предоставляет нам доступ к информации, позволяет общаться с людьми со всего мира и решать множество рабочих и личных задач. Однако вместе с преимуществами интернет несет в себе массу угроз и рисков, связанных с кибербезопасностью.

В их числе — противоправные действия с целью кражи личных данных, денежных средств, а также незаконного получения доступа к сведениям, составляющим коммерческую или государственную тайну. В связи с тем, что число подобных преступлений и ущерб от них растут с каждым годом, крайне важно знать, как действуют злоумышленники и как им можно противостоять. Мы рассмотрим основные понятия, связанные с киберпреступностью, и правила, которые помогут сохранить важную информацию и личные данные в безопасности.

Киберпреступность в России

Под киберпреступностью понимается незаконная деятельность, в рамках которой атакуются компьютерные сети, смартфоны и другие устройства. Наиболее частый мотив — получение финансовой прибыли. Для этого злоумышленники используют не только информационные технологии, но и методы социальной инженерии, когда человек добровольно передает им конфиденциальные данные или переводит свои сбережения. Кроме того, целью кибератак может быть выведение компьютеров или сетей из строя — из личных, коммерческих или политических побуждений. Этим занимаются как

отдельные лица, так и слаженные преступные группировки, которые используют продвинутые методы и хорошо подкованы технически.

Основные разновидности киберпреступлений:

- Мошенничество с использованием электронной почты и других интернет-ресурсов.
- Хищение и использование личных данных, например паролей от соцсетей и мессенджеров.
- Кража данных платежных карт и другой финансовой информации.
- Шантаж и вымогательство, в том числе с применением специальных вредоносных программ.
- Получение несанкционированного доступа к государственным или корпоративным данным.
- Онлайн-торговля запрещенными товарами.

По данным МВД, в 2023 году в России было зарегистрировано более 600 000 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Эта цифра на треть превысила показатель 2022 года[1]. Как отметил глава ведомства Владимир Колокольцев, кибератаки и факты дистанционной кражи денег у граждан фиксируются все чаще, а криминальные схемы, в том числе по выводу незаконно полученных средств, постоянно меняются[2].

«За последние пять лет количество противоправных деяний в указанной сфере возросло в два раза и сейчас составляет треть от всех зарегистрированных преступлений. Больше половины из них относится к

---

1 Краткая характеристика состояния преступности в Российской Федерации за 2023 год: https://media.mvd.ru/files/application/5040806

2 Заседание Правительственной комиссии по профилактике правонарушений 20.12.2023 https://мвд.рф/news/item/45260331/?year=2024&month=1&day=10

категории тяжких и особо тяжких. Основной массив приходится на кражи и мошенничества», — сказал глава МВД России во время заседания Правительственной комиссии по профилактике правонарушений в декабре 2023 года.

Самые распространенные способы кражи денег связаны с созданием фальшивых (фишинговых) сайтов и получением доступа к конфиденциальным данным пользователей. В полиции также отмечают рост числа киберпреступлений с применением методов социальной инженерии. Как правило, их жертвами становятся пожилые люди, которые сами сообщают сведения о себе мошенникам, представляющимся сотрудниками государственных органов или банковского сектора. Кроме того, по-прежнему фиксируются случаи крупных утечек персональных данных, которые впоследствии используются злоумышленниками в противоправных целях.

Самые распространенные схемы мошенничества:

- обзвон граждан от имени правоохранительных органов или банков
- создание фальшивых (фишинговых) сайтов для получения доступа к конфиденциальным данным пользователей
- рассылка писем о «крупном выигрыше» по электронной почте
- фальшивые сайты благотворительных организаций/туроператоров/авиакомпаний
- предложение выгодного заработка на подозрительных интернет-ресурсах
- взлом личных аккаунтов пользователей и рассылка сообщений
- Лотереи, викторины, победы в конкурсах, где нужно заплатить «налог на выигрыш» или «комиссию за доставку приза»

Владимир Колокольцев подчеркнул, что **существенная угроза кибербезопасности при этом исходит из-за рубежа**. В частности, речь идет о колл-центрах на территории Украины, сотрудники которых не только вымогают и крадут деньги у россиян, но и подталкивают их к экстремистской деятельности и совершению терактов.

«Киевскими спецслужбами используются схемы запугивания жертв несуществующим уголовным преследованием либо долговой финансовой зависимостью. Это заканчивается совершением последними преступлений против общественной безопасности», — отметил министр.

Так, за время проведения Специальной военной операции (СВО) в России выявлено уже более 400 поджогов военкоматов и диверсий на железной дороге[3]. Правоохранители отмечают, что фигурантами таких дел нередко становятся высокообразованные люди, которые сами призваны формировать законопослушное поведение. Еще одна уязвимая категория — несовершеннолетние, которых за вознаграждение вовлекают в преступную деятельность. Яркий пример — случай в Херсонской области в ноябре 2023 года, когда представители ВСУ в переписке убедили 15-летнего подростка сфотографировать для них расположение российской военной техники, после чего он был задержан.

Борьба с кибермошенниками и новые схемы обмана

Органы государственной власти прилагают большие усилия для повышения эффективности противодействия киберпреступлениям. Одно из последних нововведений — принятие закона об обмене информацией между Банком России и МВД о мошеннических операциях. Он вступил в силу в октябре 2023 года[4]. Благодаря этому существенно ускорилось расследование фактов кибермошенничества и уголовных дел[5]. Следующий шаг — вступление в силу в июле 2024 года еще одного закона[6], который усилит

---

3 С начала СВО в России выявили около 400 поджогов военкоматов и диверсий на ж/д («Интерфакс», 22.01.24): https://www.interfax.ru/russia/941302

4 Федеральный закон от 20.10.2022 № 408-ФЗ «О внесении изменений в статью 26 Федерального закона "О банках и банковской деятельности" и статью 27 Федерального закона "О национальной платежной системе"»: http://publication.pravo.gov.ru/Document/View/0001202210200013

5 Между Банком России и МВД России начнется онлайн-обмен информацией о мошеннических операциях (ЦБ РФ, 20.10.23): https://cbr.ru/press/event/?id=17142

6 Федеральный закон от 24.07.2023 № 369-ФЗ

ответственность банков по выявлению незаконных операций и существенно упростит возврат денег пострадавшим[7].

Заместитель председателя Центробанка РФ Герман Зубарев рассказал[8], что с 2023 года Банк России также стал собирать статистику о предотвращенных хищениях со счетов людей.

«Только за девять месяцев банки отбили более 20 млн попыток похитить деньги клиентов и спасли в общей сложности 3,3 трлн рублей. Результативность защитных систем от мошеннических списаний — около 98%. Тем не менее злоумышленникам удалось похитить почти 11,8 млрд рублей», — сказал зампред ЦБ РФ.

Своеобразным антирекордом ознаменовалось и начало 2024 года: в январе сразу 30 жителей Воронежской области за одни сутки перевели кибермошенникам более 30 млн рублей[9]. Как отмечают эксперты, люди продолжают попадаться на классические уловки аферистов, когда те выдают себя за сотрудников банков и правоохранительных органов, выманивая деньги под предлогом того, что счет человека якобы находится под угрозой или его родственник попал в ДТП и ему срочно нужна помощь.

По словам Германа Зубарева, мошенники постоянно совершенствуют схемы обмана. К примеру, одно из явлений, в данный момент находящихся в фокусе внимания банков и правоохранителей, — так называемое дропперство. Дропперы, или дропы, — это подставные лица, задействованные в нелегальных схемах по выводу украденных денег. Термин происходит от английского слова drop, что переводится как «скидывать» или «сливать». На дропперов оформляются банковские карты (дроп-карты), через которые

"О внесении изменений в Федеральный закон «О национальной платежной системе»" http://publication.pravo.gov.ru/Document/View/0001202307240049?index=1

7 В России банки начинают гарантировать людям защиту от телефонных мошенников («Российская газета», 31.08.23): https://rg.ru/2023/08/31/zashchitnyj-refleks.html

8 Банки отбили более 20 млн попыток похитить деньги клиентов (ЦБ РФ, 31.01.24): https://www.cbr.ru/press/event/?id=18382

9 Жители Воронежской области перевели мошенникам рекордное количество средств за сутки (BFM.ru, 31.01.24): https://www.bfm.ru/news/543226

телефонные мошенники выводят украденные с других банковских карт средства. Как правило, дропперы получают за это вознаграждение.

«К сожалению, в последнее время в дропперство активно стали втягивать подростков. С 14 лет они могут оформить банковскую карту с разрешения родителей. А мошенники распространяют в соцсетях рекламу якобы под видом банков, которым нужно выполнить «план по продажам», предлагают людям оформить любую карту и передать ее неким лицам за вознаграждение, например за 3 тысячи рублей. Затем включается сетевой маркетинг: подросткам предлагают еще 2 тысячи рублей, если они приведут друга с картой. <...> Чем это опасно? Как правило, во время расследования фактов мошенничества в первую очередь выходят на дропперов. Молодые люди, которые погнались за сиюминутной выгодой, могут стать соучастниками хищения и понести уголовную ответственность», — предупреждает Герман Зубарев.

Еще одна новая схема — создание поддельных Telegram-аккаунтов и имитация голоса близких людей жертвы или коллег по работе. *«Персонификация атак телефонных мошенников — это тренд последних месяцев. Злоумышленники стали предварительно изучать жертву — ее профиль в соцсетях, круг друзей, место работы, материальное положение. Оценивают, на какую сумму человек может оформить кредит. Часть информации о потенциальной жертве берется с сайтов, на которых человек сам оставляет данные о себе либо данные на которых становятся доступными из-за утечек. Затем мошенники ищут варианты, как наиболее эффективно наладить коммуникацию с этим человеком. Под него разрабатывается индивидуальный сценарий обмана с использованием современных технологий»*, — рассказывает зампред Центробанка. Чтобы втереться в доверие, людям пишут от имени их начальников. Мошенники даже могут использовать искусственный интеллект для создания голосовых сообщений от имени родственников и друзей потенциальной жертвы.

Параллельно совершенствуются и методы борьбы с мошенниками. Работа в этом направлении непрерывно ведется властями совместно с экспертным сообществом.

Правила кибербезопасности и цифровая грамотность

Стоит еще раз обратить внимание, что жертвой кибермошенников может стать каждый, вне зависимости от возраста, образования, социального положения и прочих факторов. Причина в том, что мошенники воздействуют на эмоции человека, а современные технологии позволяют сделать используемые приемы максимально правдоподобными.

Однако противостоять им можно, для этого следует придерживаться ряда простых правил:

- Никому и никогда не сообщайте свои паспортные данные и финансовые сведения: данные карты и ее владельца, трехзначный код с обратной стороны карты или смс-код. Сотрудники банков и госструктур никогда не запрашивают такую информацию.
- Не публикуйте конфиденциальные данные в соцсетях и на каких-либо сайтах.
- Не храните данные карт и pin-коды на компьютере или в смартфоне.
- Если с неизвестного номера звонит сотрудник банка, правоохранительных органов или государственной организации с сомнительным предложением (например, сообщением о попытке оформления кредита или подозрительной операции от вашего имени, обещанием высокого дохода по вкладу, предложением перевести средства на специальный счет и тому подобное) или по телефону запугивают и требуют быстрых действий с финансами, положите трубку.
- Если подозреваете, что вам звонит мошенник, перезвоните в банк или в контакт-центр ведомства, сотрудником которого представлялся звонящий.

- По возможности установите антивирус на все устройства и регулярно его обновляйте.
- Не используйте слишком простые пароли, а также одинаковые пароли для разных учетных записей.
- Защищайте свои аккаунты с помощью двухэтапной аутентификации в тех сервисах, где это возможно. В таком случае мошенники не смогут получить к ним доступ, даже если узнают пароль.
- Совершайте покупки в интернете только на проверенных сайтах. Сравнивайте адреса сайтов, может отличаться одна буква или точка, не попадитесь на сайт-зеркало.
- Никогда не вводите личные и финансовые данные на сомнительных сайтах и не переходите по ссылкам из подозрительных писем, которые предлагают, например, пройти опрос или получить какую-либо выплату.

Более подробная информация о методах финансовых кибермошенников и признаках, по которым их можно распознать, есть в специальном разделе на сайте Банка России, который регулярно обновляется[10].

Если же средства уже переведены мошенникам:

1. Немедленно заблокируйте карту с помощью мобильного приложения, личного кабинета на сайте банка или через контакт-центр банка по телефону.
2. В течение суток после получения сообщения о списании средств напишите заявление в отделении банка о несогласии с операцией. Также обратитесь с заявлением о хищении денег в любое отделение полиции.

Современный мир и технологии не только дарят нам бесконечный доступ к информации, но и ждут от нас умения ими пользоваться. Развитие

10 Противодействие мошенническим практикам, ЦБ РФ: https://cbr.ru/information_security/pmp/

критического мышления, соблюдение простых правил информационной гигиены, бдительность и забота об окружающих помогут избежать проблем и не стать жертвой кибермошенников.