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.