Сколько бы в СМИ не освещалась тема «мобильного мошенничества», потерпевших по делам о мошенничестве, к сожалению, становится в все больше.

Мошенники шагают в ногу со временем и современными IT-технологиями, звонки и сообщения с подозрительными ссылками поступают через мессенджеры «WhatsApp», «Telegram» и др., что затрудняет установление данных лиц правоохранительными органами.

Наиболее распространенным видом мошенничества с использованием IT-технологий являются звонки злоумышленников, представляющихся сотрудниками банков или правоохранительных органов, с предупреждением граждан об атаке на банковский счет гражданина либо об оформлении мошенниками на имя гражданина кредита и необходимостью в связи с этим перевода денежных средств со счета гражданина на безопасный счет банка.

Желание гражданина избежать негативных последствий приводит к вовлечению его в контакт с мошенником, введенный в заблуждение гражданин сообщает злоумышленнику необходимые для совершения мошенничества коды, пароли, номера банковских карт и счетов, кодовые слова, самостоятельно под контролем мошенников оформляет на свое имя кредиты на крупные суммы, переводя денежные средства на счета, указанные неизвестными.

**Чтобы обезопасить себя и своих близких**и не стать жертвой кибермошенников, необходимо соблюдать правила цифровой или компьютерной безопасности, а именно: не использовать подозрительные интернет-сайты, не сообщать незнакомым лицам («банковским служащим», «сотрудникам правоохранительных органов» и т.д.), в том числе по телефону, паспортные данные, а также данные своих банковских карт и паролей от Интернет-банка, использовать при входе в Интернет-банк сложные пароли, затрудняющие злоумышленникам доступ к информации.

Гражданам при поступлении посредством сотовой связи просьб незнакомых лиц об оказании помощи в связи с непредвиденными обстоятельствами, связанными с их родственниками, о проведении процессуальных проверок и возбуждении уголовных дел полицией, ФСБ, прокуратурой и в связи с этим переводе крупных сумм денег с банковских счетов, нужно сохранять бдительность и не поддаваться на требования злоумышленников, создающих во время телефонных переговоров напряженную атмосферу, торопя гражданина с принятием решения.

В каждом случае прежде, чем перечислять денежные средства, необходимо принять меры к проверке поступившей информации, позвонить родственникам, в отдел полиции и т.д.

В связи с повышенной общественной опасностью мошенничества с использованием электронных средств действующим законодательством за совершение таких действий предусмотрена уголовная ответственность. Статьей 159.3 УК РФ установлена уголовная ответственность за мошенничество с использованием электронных средств платежа (платежных карт, иных технических средств).

За мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на него путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей уголовная ответственность предусмотрена ст. 159.6 УК РФ.

Уголовным кодексом Российской Федерации за преступления данной категории в зависимости от их тяжести предусмотрено наказание в виде штрафа, обязательных, исправительных и принудительных работ, либо лишением свободы на срок до 6 лет.

При обнаружении неправомерного снятия денежных средств с банковских счетов (электронных карт и кошельков) необходимо незамедлительно обращаться в правоохранительные органы. Важно помнить, что самая надежная защита от кибермошенников – это внимательность и информированность граждан.

Сколько бы в СМИ не освещалась тема «мобильного мошенничества», потерпевших по делам о мошенничестве, к сожалению, становится в все больше.

Мошенники шагают в ногу со временем и современными IT-технологиями, звонки и сообщения с подозрительными ссылками поступают через мессенджеры «WhatsApp», «Telegram» и др., что затрудняет установление данных лиц правоохранительными органами.

Наиболее распространенным видом мошенничества с использованием IT-технологий являются звонки злоумышленников, представляющихся сотрудниками банков или правоохранительных органов, с предупреждением граждан об атаке на банковский счет гражданина либо об оформлении мошенниками на имя гражданина кредита и необходимостью в связи с этим перевода денежных средств со счета гражданина на безопасный счет банка.

Желание гражданина избежать негативных последствий приводит к вовлечению его в контакт с мошенником, введенный в заблуждение гражданин сообщает злоумышленнику необходимые для совершения мошенничества коды, пароли, номера банковских карт и счетов, кодовые слова, самостоятельно под контролем мошенников оформляет на свое имя кредиты на крупные суммы, переводя денежные средства на счета, указанные неизвестными.

**Чтобы обезопасить себя и своих близких**и не стать жертвой кибермошенников, необходимо соблюдать правила цифровой или компьютерной безопасности, а именно: не использовать подозрительные интернет-сайты, не сообщать незнакомым лицам («банковским служащим», «сотрудникам правоохранительных органов» и т.д.), в том числе по телефону, паспортные данные, а также данные своих банковских карт и паролей от Интернет-банка, использовать при входе в Интернет-банк сложные пароли, затрудняющие злоумышленникам доступ к информации.

Гражданам при поступлении посредством сотовой связи просьб незнакомых лиц об оказании помощи в связи с непредвиденными обстоятельствами, связанными с их родственниками, о проведении процессуальных проверок и возбуждении уголовных дел полицией, ФСБ, прокуратурой и в связи с этим переводе крупных сумм денег с банковских счетов, нужно сохранять бдительность и не поддаваться на требования злоумышленников, создающих во время телефонных переговоров напряженную атмосферу, торопя гражданина с принятием решения.

В каждом случае прежде, чем перечислять денежные средства, необходимо принять меры к проверке поступившей информации, позвонить родственникам, в отдел полиции и т.д.

В связи с повышенной общественной опасностью мошенничества с использованием электронных средств действующим законодательством за совершение таких действий предусмотрена уголовная ответственность. Статьей 159.3 УК РФ установлена уголовная ответственность за мошенничество с использованием электронных средств платежа (платежных карт, иных технических средств).

За мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на него путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей уголовная ответственность предусмотрена ст. 159.6 УК РФ.

Уголовным кодексом Российской Федерации за преступления данной категории в зависимости от их тяжести предусмотрено наказание в виде штрафа, обязательных, исправительных и принудительных работ, либо лишением свободы на срок до 6 лет.

При обнаружении неправомерного снятия денежных средств с банковских счетов (электронных карт и кошельков) необходимо незамедлительно обращаться в правоохранительные органы. Важно помнить, что самая надежная защита от кибермошенников – это внимательность и информированность граждан.

Обычным пользователям рекомендуется соблюдать простые правила:

* Не сообщайте конфиденциальную информацию, контакты третьим лицам, если не уверенности в их надежности.
* Регулярно обновляйте операционную систему, поскольку уровень безопасности в обновленных версиях обычно выше.
* Не храните пароли в открытом доступе.
* Установите надежную антивирусную программу.
* Не подключайтесь к незащищенному Wi-Fi. Особенно это важно для онлайн-банка.
* Используйте сложные комбинации при создании паролей для входа в аккаунт.
* Создайте двухфакторную идентификацию на смартфоне.
* Не открывайте файлы, полученные с неизвестных адресов, не переходите по ссылкам.
* Не заходите в личные кабинеты с посторонних устройств.
* Начните изучать новости, [вебинары](https://neiros.ru/blog/marketing/vebinar-samyy-udobnyy-format-dlya-obucheniya-i-prodvizheniya/), отчеты и материалы о новых угрозах, информацию о которых можно найти на сайтах разработчиков антивирусных программ.
* Не оставляйте компьютер и телефон незаблокированными в общественных местах.
* Повышайте уровень цифровой грамотности сотрудников компании.
* Не используйте один и тот же пароль для всех сайтов.
* Не скачивайте подозрительные файлы на непроверенных сайтах.
* Не давайте гаджеты в руки незнакомым людям.
* Читайте соглашения о конфиденциальности при регистрации на сайтах.
* С осторожностью принимайте [файлы cookies](https://neiros.ru/blog/marketing/kuki-chto-eto-takoe-komu-i-zachem-oni-nuzhny/).

Обычным пользователям рекомендуется соблюдать простые правила:

* Не сообщайте конфиденциальную информацию, контакты третьим лицам, если не уверенности в их надежности.
* Регулярно обновляйте операционную систему, поскольку уровень безопасности в обновленных версиях обычно выше.
* Не храните пароли в открытом доступе.
* Установите надежную антивирусную программу.
* Не подключайтесь к незащищенному Wi-Fi. Особенно это важно для онлайн-банка.
* Используйте сложные комбинации при создании паролей для входа в аккаунт.
* Создайте двухфакторную идентификацию на смартфоне.
* Не открывайте файлы, полученные с неизвестных адресов, не переходите по ссылкам.
* Не заходите в личные кабинеты с посторонних устройств.
* Начните изучать новости, [вебинары](https://neiros.ru/blog/marketing/vebinar-samyy-udobnyy-format-dlya-obucheniya-i-prodvizheniya/), отчеты и материалы о новых угрозах, информацию о которых можно найти на сайтах разработчиков антивирусных программ.
* Не оставляйте компьютер и телефон незаблокированными в общественных местах.
* Повышайте уровень цифровой грамотности сотрудников компании.
* Не используйте один и тот же пароль для всех сайтов.
* Не скачивайте подозрительные файлы на непроверенных сайтах.
* Не давайте гаджеты в руки незнакомым людям.
* Читайте соглашения о конфиденциальности при регистрации на сайтах.
* С осторожностью принимайте [файлы cookies](https://neiros.ru/blog/marketing/kuki-chto-eto-takoe-komu-i-zachem-oni-nuzhny/).