

# Основные виды IT-преступлений и их профилактика

К наиболее распространенным видам дистанционных мошенничеств относятся:

– «**ФИШИНГ**» – вид дистанционного мошенничества, при совершении которого злоумышленники (в ходе телефонного разговора, посредством направления электронного письма или смс-сообщения) получают личные конфиденциальные данные о банковской карте, номере счета, логины и пароли для входа в интернет-банк, а также пароли безопасности, позволяющие произвести списание находящихся на банковской карте денежных средств. Жертвами указанного вида мошенничества зачастую становятся незащищенные, малообразованные, доверчивые слои населения. Представляясь зачастую сотрудниками кредитных организаций, преступники вводят в заблуждение граждан относительно совершаемых несанкционированных списаний денежных средств, осуществляемых покупках и т.п., после чего просят назвать конфиденциальные сведения с целью пресечения возможного совершения преступления. Граждане, доверяя полученной информации, желая обезопасить свои денежные средства от преступных посягательств, сообщают запрашиваемую информацию, в результате чего злоумышленники похищают принадлежащие им денежные средства.

Банк России, Министерство внутренних дел Российской Федерации, Генеральная прокуратура Российской Федерации

## КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА

Фишинг – вид мошенничества, когда у человека крадут персональные данные или деньги с помощью сайтов-подделок. Часто мошенники делают сайты, которые как две капли воды похожи на сайты реальных организаций

### КАК МОЖНО ОКАЗАТЬСЯ НА ФИШИНГОВОМ САЙТЕ?

По ссылкам из интернета или электронной почты, СМС, сообщений в соцсетях или мессенджерах, рекламе, объявлениях о лотереях, распродажах, конкурсах или от государства

Хакеры часто взламывают чужие аккаунты, и фишинговая ссылка может прийти даже от знакомых

### КАК РАСПОЗНАТЬ ФИШИНГОВЫЙ САЙТ?

- Адрес отличается от настоящего лишь парой символов
- В адресной строке нет **https** и знака закрытого замка
- Дизайн скопирован некачественно, в текстах есть ошибки
- У сайта мало страниц или даже одна – для ввода данных карты

### КАК УБЕРЕЧЬСЯ ОТ ФИШИНГА?

- Установите антивирус и регулярно обновляйте его
- Сохраняйте в закладках адреса нужных сайтов
- Не переходите по подозрительным ссылкам
- Используйте отдельную карту для покупок в интернете, кладите на нее нужную сумму прямо перед оплатой

Подробнее о правилах безопасности читайте на [ru.sberbank.ru](https://ru.sberbank.ru)

Финансовая культура

в соцсетях и мессенджерах мошенники ищут жертв в интернете все время

- ссылки и файлы в соцсетях
- или знакомых пользователей соцсетей от банка
- или неизвестных пользователей известной компании

## ЦЕННИК ВНЕШНИХ ФАЙЛОВ И ССЫЛКИ

## Как распознать фишинговые письма и сообщения

- Броская тема
- Неперсонализированное приветствие («дорогой друг», «уважаемый клиент»)
- Неожиданные заманчивые предложения
- Срочные требования, запугивание, которыми злоумышленники нагнетают обстановку, чтобы вы запаниковали и потеряли бдительность
- Необычные символы, опечатки и ошибки
- Странный адрес отправителя

Если вы получили подозрительное письмо, не переходите по ссылкам из него и не скачивайте приложенные файлы.

## Как отличить фейковый сайт

Внешне фишинговый сайт похож на оригинальный, но его можно распознать по нескольким признакам:

- лишние символы или слова в адресе сайта
- в адресной строке нет символов **https** и иконки закрытого замка, а значит, отсутствует безопасное соединение
- устаревший дизайн, видоизменённый логотип бренда
- отсутствуют контактная информация, пользовательское соглашение, условия оплаты и доставки

## Способы защиты от фишинга

- Не переходите по подозрительным ссылкам
- Не скачивайте файлы от неизвестных отправителей
- Проясняйте спорные вопросы через другие средства связи
- Придумывайте сложные пароли, не используйте последовательные комбинации символов и простые слова (12345, qwerty, password)
- Включите двухфакторную аутентификацию для защиты аккаунтов
- Заведите отдельную карту для оплаты интернет-покупок, где будете держать небольшую сумму
- Используйте антивирус
- А главное – всегда будьте бдительны

## МОШЕННИКИ ИСПОЛЗУЮТ ФЕЙКОВЫЕ ССЫЛКИ ДЛЯ КРАЖИ TELEGRAM-АККАУНТОВ ПОД ПРЕДОГЛОМ «ПОВЫШЕНИЯ БЕЗОПАСНОСТИ»

Мошенники разработали новую схему для захвата учетных записей Telegram. Теперь они используют фейковый аккаунт «Службы безопасности Telegram Security Messenger», чтобы получить доступ к вашей учетной записи.

Суть схемы: сначала вы получаете множество запросов на получение кода для входа в мессенджер. Затем, с поддельного аккаунта Telegram Security Messenger вам предлагается перейти по ссылке для «повышения безопасности».

Переход по данной ссылке приводит к немедленному получению мошенниками доступа к вашему аккаунту. Будьте бдительны и предупредите близких о потенциальной угрозе.

**МОШЕННИКИ НАЧАЛИ РАССЫЛАТЬ ФИШИНГОВЫЕ ПИСЬМА ПОД ВИДОМ ЛОГИСТИЧЕСКОЙ КОМПАНИИ**

ЦИФРОВАЯ РОССИЯ

**kaspersky**

В «Лаборатории Касперского» сообщили, что летом 2024 года злоумышленники начали красть данные учетных записей корпоративных почт под видом известной транспортной компании.

**Преступники оповещают пользователей о скорой доставке и присылают PDF-файл,** в котором якобы содержатся счет и другие важные транспортные документы.

В случае, **если сотрудник откроет вложенный файл, его автоматически перебросит на фишинговую страницу,** где для просмотра содержания документа требуется пройти авторизацию через корпоративную почту.

Впоследствии **полученная информация может использоваться для получения доступа к корпоративным сведениям,** в частности для осуществления вымогательства и продажи конфиденциальных данных.



- «**ФАРМИНГ**» – процедура скрытого направления на ложный IP-адрес, то есть направление пользователя на фиктивный веб-сайт, чаще всего используемый для приобретения товаров и услуг (ozon.ru, avito.ru, aliexpress.ru, joom, biglion, купинатор, кассир.ру, билетер, сайты по продаже билетов на ж/д и авиатранспорт и др.);
  - «**ДВОЙНАЯ ТРАНЗАКЦИЯ**» (при оплате товаров и услуг продавец сообщает об ошибке, предлагает повторить операцию, а в дальнейшем денежные средства списываются дважды по каждой из проведенных операций)
  - «**ТРАППИНГ**» (манипуляции с картридером банкоматов, позволяющие либо не возвращать карту владельцу, либо списывать все данные карты для дальнейшего их использования).
- Основные схемы телефонного мошенничества:**

## 1. Обман по телефону.

**ВАША КАРТА ЗАБЛОКИРОВАНА**

Для разблокировки перезвоните сотруднику безопасности Банка – Петру Иванову 8-910-\*\*\*-\*\*-\*\*



Получив любое тревожное сообщение или звонок из банка, не поддерживайте переписку или разговор. Немедленно позвоните в банк сами – вручную наберите номер, указанный на обороте банковской карты или на официальном сайте.

Звонок сотрудника банка – когда неизвестный представляется сотрудником службы безопасности какого-либо банка и сообщает, что с Вашего банковского счета происходят операции по несанкционированному списанию денежных средств, и в целях безопасности счета предлагает перевести сбережения на «резервный» или «безопасный» счет. Распространены случаи сообщения информации об оформлении на Вас кредита и необходимости пройти в приложении онлайн-Банка по определённой ссылке для его аннулирования (выполнить иные инструкции).

Звонок сотрудника правоохранительных органов – когда неизвестный представляется сотрудником полиции, следователем и т.д. и сообщает, что проводится спецоперация по поимке мошенников и для этого необходимо перевести деньги на «специальный» счет. При этом требует не звонить в банк, так как сотрудники банка заодно с мошенниками.

Ваш родственник, либо близкий человек попал в беду (например, машиной сбил человека или обвиняется в совершении преступления), и задержан сотрудниками полиции, и неизвестный сообщает, что для освобождения необходимо перевести на счет денежные средства либо для примирения с пострадавшим либо в качестве взятки сотрудникам полиции. Возможны варианты, при которых в разговоре может принять участие якобы сотрудник полиции, который будет подтверждать сказанное.

**ВАЖНО:** Это звонят мошенники (несмотря на то, что определившийся на телефоне номер может соответствовать номеру телефона банка или правоохранительных органов, зачастую – Московского региона (499, 495... и т.д.), так как при помощи специальных устройств мошенники меняют номера на абсолютно любой номер – так называемые подменные номера), сотрудники банков никогда не звонят своим клиентам, и тем более, никогда не требуют переводить с личного счета деньги. Представители правоохранительных органов могут звонить только для вызова в помещения правоохранительных органов с целью получения объяснений, истребования документов по находящимся в производстве уголовным делам и материалам проверок.

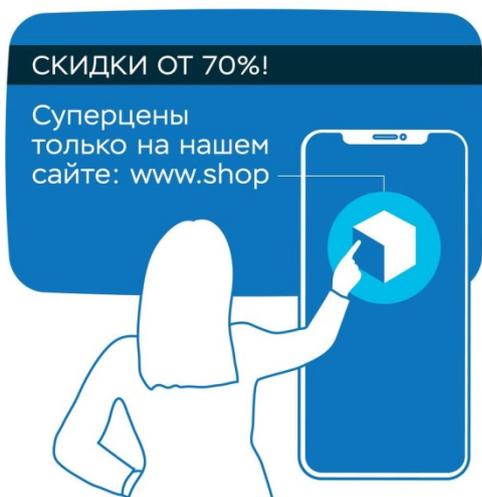
При поступлении такого звонка необходимо прервать разговор и перезвонить тому, о ком идет речь, либо в указанный государственный орган или кредитную организацию для перепроверки информации.

## 2. Обман при покупке (продаже) товара на интернет сайтах.

Предоплата за несуществующий товар – подается объявление на востребованный товар с привлекательной ценой (ниже рыночной) с приложением ненастоящих фотографий. В ходе общения «продавец» уклоняется от встречи ввиду житейских причин (нет времени, занятость на работе, удаленность расположения) и предлагает оплатить товар безналичным платежом с гарантированной последующей доставкой через курьера, но после получения денег, продавец-мошенник перестает выходить на связь.

Оплата муляжа по почте наложенным платежом – злоумышленник пытаются вначале заполучить предоплату на доверии, если не получается, то предлагают получить заказ на. Покупатель спрашивает номер карты и код из СМС – по Вашему объявлению о продаже товара в интернете Вам позвонил покупатель и попросил сообщить реквизиты банковской карты (предварительно выяснив номер телефона к которому привязана карта) и смс-код, чтобы перевести деньги, якобы это нужно для банковского перевода. На самом деле это мошенник, который пытается войти в личный кабинет онлайн-банка и списать все деньги с Вашего счета.

**ВАЖНО:** Оплачивайте товар только после его получения и проверки и не отправляйте деньги в качестве залога (задатка). Для перевода денежных средств достаточно номера телефона и другой дополнительной информации не требуется.



«Выгодные предложения» могут оказаться уловкой. С их помощью мошенники завлекают пользователей в свои фальшивые интернет-магазины. Это фишинг – попытка выманить реквизиты вашей банковской карты, чтобы украсть с нее деньги. Всегда проверяйте адрес сайта и не вводите данные на сомнительных страницах.



Вирусные и фишинговые рассылки обычно касаются самых популярных тем. Даже если вы сдавали анализ и ждете результат, не спешите следовать инструкциям незнакомого отправителя. Сначала проверьте адрес лаборатории на ее официальном сайте.

### 3. Телефонные вирусы.

Очень часто используется форма мошенничества с использованием телефонных вирусов. На телефон абонента приходит сообщение следующего вида: «Вам пришло MMS-сообщение. Для получения перейдите по ссылке...». При переходе по указанному адресу на телефон скачивается вирус и происходит списание денежных средств с вашего счета.

Другой вид мошенничества выглядит так. При заказе какой-либо услуги через якобы мобильного оператора или при скачивании мобильного контента абоненту приходит предупреждение вида: «Вы собираетесь отправить сообщение на короткий номер ..., для подтверждения операции, отправьте сообщение с цифрой 1, для отмены с цифрой 0». При отправке подтверждения, со счета абонента списываются денежные средства. Мошенники используют специальные программы, которые позволяют автоматически генерировать

**ВАЖНО:** Не следует звонить по номеру, с которого отправлен SMS – вполне возможно, что в этом случае с Вашего телефона будет автоматически снята крупная сумма и переходить по сомнительным ссылкам.



Не переходите по ссылке – сначала позвоните в банк по официальному номеру и уточните, настоящая ли это рассылка. Аферисты рассчитывают, что вы не станете проверять информацию и выполните их инструкции. А в итоге – скачаете вирус или введете свои секретные банковские данные на поддельной странице.



Преступники часто рассылают письма от имени популярных сервисов. Адрес отправителя может отличаться от настоящего всего парой символов. Ссылки в этих сообщениях ведут на фишинговые сайты или содержат вирусы, крадущие платежные данные с устройств. Не переходите по ним – сразу удаляйте подозрительные письма.

### 4. Ошибочный перевод средств.

Абоненту поступает SMS-сообщение о поступлении средств на его счет, переведенных с помощью услуги «Мобильный перевод». Сразу после этого поступает звонок и мужчина (или женщина) сообщает, что ошибочно перевел деньги на его счет, при этом просит вернуть их обратно тем же «Мобильным переводом». В действительности деньги не поступают на телефон, а человек переводит свои собственные средства. Если позвонить по указанному номеру, он может быть вне зоны доступа. Кроме того, существуют такие номера, при осуществлении вызова на которые с телефона снимаются все средства.

**ВАЖНО:** Если Вас просят перевести якобы ошибочно переведенную сумму, напомните, что для этого используется чек. Отговорка, что «чек потерян», скорее всего, свидетельствует о том, что с Вами общается мошенник.



Только мошенники запрашивают пароли «для отмены операции». Никому и никогда не сообщайте данные для входа в свой онлайн-банк и коды из банковских уведомлений. Также нужно держать в секрете полные реквизиты карты, включая срок действия и три цифры с оборота. В любой непонятной ситуации сами звоните в банк по официальному номеру.

## Мошенничества с банковскими картами

Банковская карта – это инструмент для совершения платежей и доступа к наличным средствам на счёте, не требующий для этого присутствия в банке. Но простота использования банковских карт оставляет множество лазеек для мошенников.

При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраной: в государственных учреждениях, банках, крупных торговых центрах и т.д.

Совершая операции с пластиковой картой, следите, чтобы рядом не было посторонних людей.

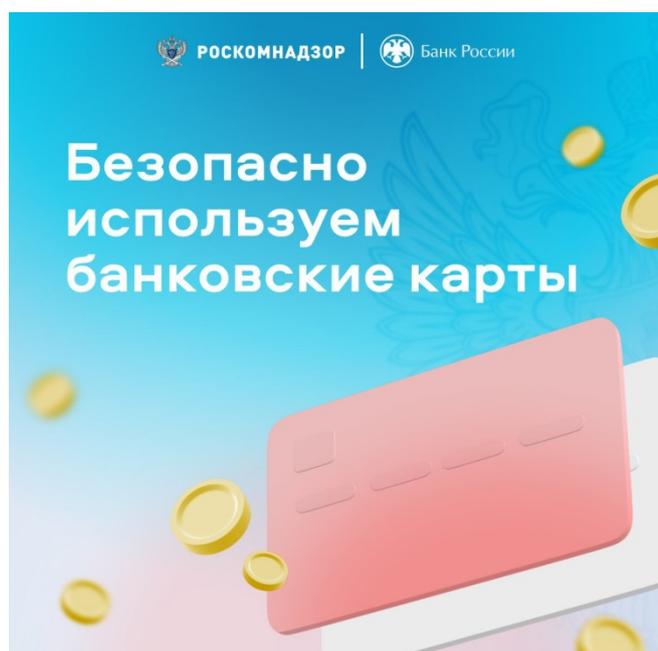
Набирая ПИН-код, прикрывайте клавиатуру рукой. Реквизиты и любая прочая

Обращайте внимание на картоприемник и клавиатуру банкомата. Если они оборудованы какими-либо дополнительными устройствами, то от использования данного банкомата

В случае некорректной работы банкомата – если он долгое время находится в режиме ожидания или самопроизвольно перезагружается – откажитесь от его использования. Велика вероятность того, что он перепрограммирован злоумышленниками.

### Как обезопасить себя от мошенников:

1. Проверяйте информацию, полученную в ходе телефонного разговора и интернет переписки с неизвестными (они могут представляться сотрудниками правоохранительных органов, представителями кредитных организаций).
2. Установить на телефон (компьютер) современное лицензированное антивирусное программное обеспечение.
3. Не устанавливайте и не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников: скачанные с неизвестных сайтов, присланные по электронной почте (подозрительные файлы лучше сразу удалять).
4. Используйте пароли не связанные с Вашими персональными данными.
5. Ни при каких обстоятельствах не сообщайте реквизиты своих банковских счетов (карт), пароли и другую персональную информацию.
6. Поставьте лимит на сумму списаний или перевода в личном кабинете банка.
7. По всем возникающим вопросам обращаться в банк, выдавший карту.
8. Не выполнять никаких срочных запросов к действию, в том числе по установке каких бы то ни было приложений.
9. Не переходить ни по каким ссылкам, которые приходят на e-mail или по SMS.
10. Обращать на все сообщения от банка (например, если они содержат грамматические ошибки).
11. Не перезванивать по номерам которые приходят на e-mail или по SMS.
12. Перепроверяйте подлинность интернет-сайтов, на которых осуществляете заказ товара.



## Не используйте зарплатную карту для онлайн-покупок

Для онлайн-шопинга заведите **отдельную дебетовую карту** и пополняйте ее ровно на ту сумму, которая **нужна для оплаты**.



РОСКОМНАДЗОР | Банк России

## Не храните банковские карты, как и документы, в машине

На эти ценные вещи **автомобильные воры** обращают внимание в **первую очередь**.



РОСКОМНАДЗОР | Банк России

## Не привязывайте банковские карты к сайтам и сервисам

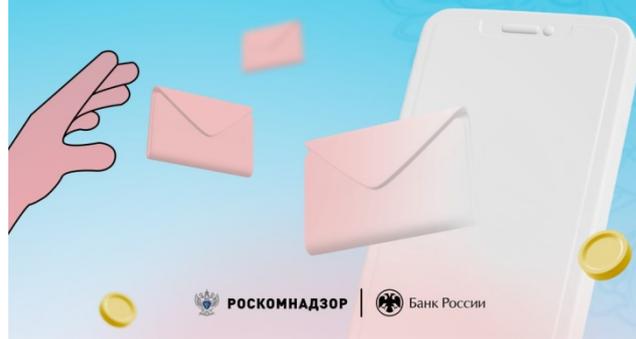
Если **сайт взломают** или произойдет утечка данных, то платежные реквизиты **окажутся в руках мошенников**.



РОСКОМНАДЗОР | Банк России

## Не пересылаете в мессенджерах и соцсетях фото банковских карт и документов

Если личные и финансовые данные окажутся в руках **киберпреступников**, они могут воспользоваться **конфиденциальной информацией** в преступных целях.



РОСКОМНАДЗОР | Банк России

## Не храните пин-код вместе с банковской картой и не записывайте его на «пластик»

Если у вас несколько банковских карт, для каждой **установите свой пин-код**. **Не устанавливайте простые числовые комбинации** вроде 1234, 0000, 1111. Злоумышленники могут легко их разгадать.



РОСКОМНАДЗОР | Банк России

## Как себя обезопасить

**Подключите sms- или пуш-уведомления.** Так вы оперативно узнаете об операциях, которые не совершали, и сможете быстро **заблокировать банковскую карту**.

Пуш-уведомления обычно **бесплатны и доступны** для смартфона с приложением банка. Владельцам кнопочных телефонов подойдут sms-уведомления



РОСКОМНАДЗОР | Банк России

## Как себя обезопасить

Для безопасности на смартфоне лучше **отключить отображение уведомлений при заблокированном экране устройства**. Тогда при утере или краже мобильного мошенники не увидят содержимое оповещений от банка.



РОСКОМНАДЗОР | Банк России