Банк России

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ

КАК ЗАЩИТИТЬСЯ ОТ ОНЛАЙН-МОШЕННИКОВ

Чтобы добраться до ваших банковских счетов, мошенникам нужны ваши персональные данные и реквизиты карт

Какие схемы используют аферисты?

ОБЕЩАЮТ ЗОЛОТЫЕ ГОРЫ
Опросы за вознаграждение, социальные выплаты или сверхприбыльные инвестиционные проекты. Гарантия быстрого обогащения – признак обмана

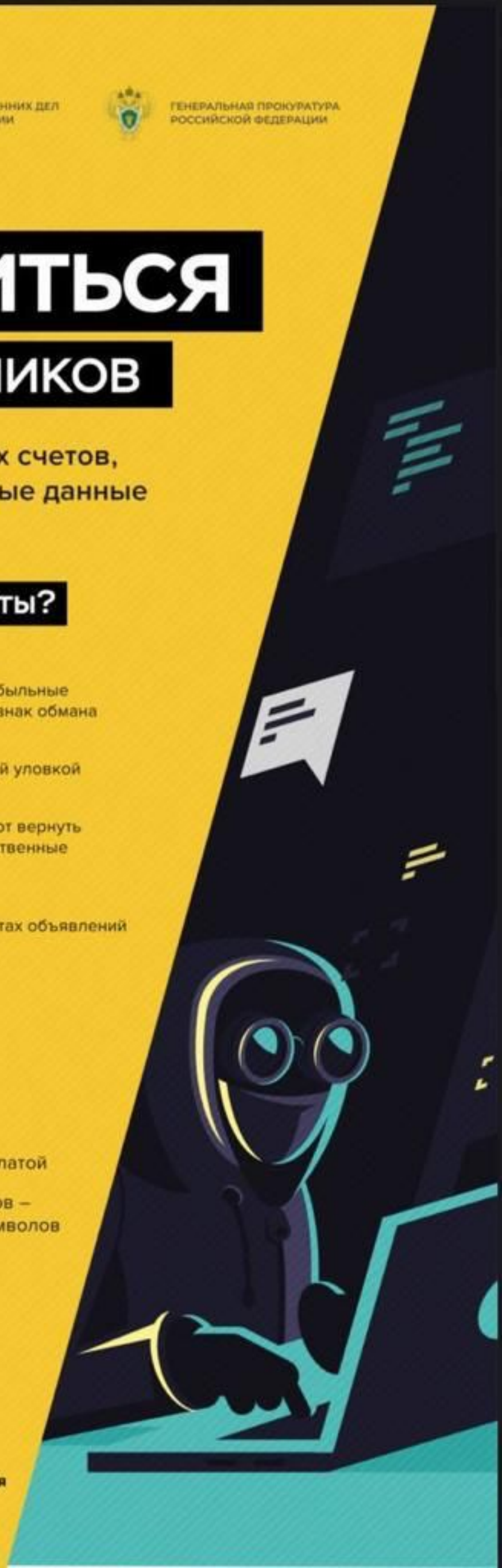
ЗАМАНИВАЮТ НА РАСПРОДАЖИ
Огромные скидки и низкие цены могут оказаться мошеннической уловкой

СПЕКУЛИРУЮТ НА ГРОМКИХ СОБЫТИЯХ
Например, объявляют сбор денег на разработку вакцин, обещают вернуть деньги за отмененные рейсы или предлагают получить государственные дотации

МАСКИРУЮТСЯ
Разыгрывают роль продавцов и покупателей на популярных сайтах объявлений

Как обезопасить свои деньги в интернете?

1. Установите антивирус и регулярно обновляйте его
2. Заведите отдельную дебетовую карту для платежей в интернете и кладите на нее нужную сумму перед оплатой
3. Всегда проверяйте адреса электронной почты и сайтов – они могут отличаться от официальных лишь парой символов
4. Не переходите по ссылкам от незнакомцев – сразу удаляйте сомнительные сообщения
5. Никому не сообщайте свои персональные данные



Подробнее о правилах кибергигиены читайте на fincult.info

Финансовая культура

Банк России

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ

КАК ЗАЩИТИТЬ СВОИ ГАДЖЕТЫ ОТ ВИРУСОВ

ВИРУСЫ:

- открывают удаленный доступ к вашему устройству
- крадут логины и пароли от онлайн- и мобильного банка
- перехватывают секретные коды из сообщений

Заполучив эти данные, киберпреступники могут похитить все деньги с ваших счетов

КАК ПОНЯТЬ, ЧТО УСТРОЙСТВО ЗАРАЖЕНО?

- Зависает, перезагружается или отключается
- Само завершает работу приложений
- Показывает всплывающие окна
- Теряет объем памяти

ЧТО ДЕЛАТЬ, ЕСЛИ НА УСТРОЙСТВЕ ВИРУС?

- **Позвоните в банк** и попросите заблокировать доступ к онлайн- и мобильному банку и все карты, которые использовали на устройстве
- **Обратитесь в сервисный центр**, чтобы вылечить гаджет
- **Перевыпустите карты, смените логин и пароль** от онлайн-банка и заново установите банковское приложение

КАК ЗАЩИТИТЬ УСТРОЙСТВО ОТ ВИРУСОВ?

- **Используйте антивирус** и регулярно его обновляйте
- **Не переходите по ссылкам** от незнакомцев, не устанавливайте программы по их просьбе и не используйте чужие флешки
- Скачивайте приложения **только из проверенных источников**
- **Обновляйте** операционную систему устройства
- **Избегайте** общедоступных Wi-Fi-сетей

Подробнее о защите гаджетов читайте на fincult.info

Финансовая культура

Банк России

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ

ЧТО ДЕЛАТЬ, ЕСЛИ С КАРТЫ УКРАЛИ ДЕНЬГИ?

1 ЗАБЛОКИРОВАТЬ КАРТУ

- по номеру телефона банка на банковской карте или на официальном сайте
- через мобильное приложение
- через личный кабинет на официальном сайте банка
- в отделении банка

2 НАПИСАТЬ ЗАЯВЛЕНИЕ О НЕСОГЛАСИИ С ОПЕРАЦИЕЙ

Заявление должно быть написано:

- в течение суток после сообщения о списании денег
- на месте в отделении банка

3 ОБРАТИТЬСЯ В ПОЛИЦИЮ

Чем больше людей подадут заявления, тем выше вероятность, что преступников поймают

КАК ОБЕЗОПАСИТЬ ДЕНЬГИ НА СЧЕТАХ?

НИКОМУ НЕ СООБЩАЙТЕ:

- срок действия карты и трехзначный код на ее оборотной стороне (CVV/CVC)
- пароли и коды из уведомлений
- логин и пароль от онлайн-банка

НЕ ПУБЛИКУЙТЕ

персональные данные в открытом доступе

УСТАНОВИТЕ

антивирусы на все устройства

КОДОВОЕ СЛОВО

называйте только сотруднику банка, когда сами звоните на горячую линию

Банк не компенсирует потери, если вы нарушили правила безопасного использования карты

Подробнее о правилах безопасности читайте на fincult.info

Финансовая культура

Банк России

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ

ОСТОРОЖНО: ТЕЛЕФОННЫЕ МОШЕННИКИ!

5 ПРИЗНАКОВ ОБМАНА

1 НА ВАС ВЫХОДЯТ САМИ

Аферисты могут представиться службой безопасности банка, налоговой, прокуратурой

Любой неожиданный звонок, СМС или письмо — повод насторожиться

2 РАДУЮТ ВНЕЗАПНОЙ ВЫГОДОЙ ИЛИ ПУГАЮТ

Сильные эмоции притупляют бдительность

3 НА ВАС ДАВЯТ

Аферисты всегда торопят, чтобы у вас не было времени все обдумать

4 ГОВОРЯТ О ДЕНЬГАХ

Предлагают спасти сбережения, получить компенсацию или вложиться в инвестиционный проект

5 ПРОСЯТ СООБЩИТЬ ДАННЫЕ

Злоумышленников интересуют реквизиты карты, пароли и коды из банковских уведомлений

ВАЖНО!

Сотрудники банков и полиции НИКОГДА не спрашивают реквизиты карты, пароли из СМС, персональные данные и не просят совершать переводы с вашей карты

НИКОГДА НИКОМУ НЕ СООБЩАЙТЕ:

- коды из СМС
- трехзначный код на оборотной стороне карты (CVV/CVC)
- PIN-код
- пароли/логины к банковскому приложению и онлайн-банку
- кодовое слово
- персональные данные

Как защитить свои финансы, читайте на fincult.info

Финансовая культура

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, рекламы, объявлений о лотереях, распродажах, компенсациях 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 значка 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 кибергигиены читайте на fincult.info

Финансовая культура

Что делать в случае незапланированного списания денег с карты

03.10.2023 \ АРБ ШПАРГАЛКА

Незапланированное списание денег с банковской карты может быть следствием небрежного хранения секретных данных ее держателем, технических ошибок в банковской инфраструктуре, а также противоправных действий. Об этом 3 октября «Известиям» сообщил юрист Евгений Антонов.

«В силу закона и договора с потребителем банк, выступая оператором по переводу денежных средств, обязан информировать клиента о совершении каждой операции с использованием банковской карты путем направления клиенту соответствующего уведомления. Если же банк не информирует клиента об операции, а списание средств произошло без его согласия, банк обязан возместить клиенту сумму операции», — сказал он.

При получении информации о расходовании денег с банковской карты, которое потребитель не совершал, а также при утрате банковской карты нужно незамедлительно сообщить об этом банку и не отказываться от блокировки карты до выяснения всех обстоятельств списания средств, подчеркнул юрист. В случае утраты доступа к телефону, на который приходят сообщения от банка, потребуется заблокировать сим-карту через оператора связи.

«При надлежащем уведомлении банка в срок не позднее следующего дня после утраты карты либо получения информации о несогласованной операции банк возмещает суммы таких транзакций, даже если они произошли до информирования банка клиентом. В то же время банки обладают и самостоятельным правом приостанавливать обслуживание банковских карт и обязанностью выявлять операции, признаки которых отнесены Центральным банком России к осуществляемым без согласия клиента. В любом случае приостановления банковского обслуживания держатель карты должен быть проинформирован об этом с указанием причины», — сказал Антонов.

По словам эксперта, финансовая организация освобождается от ответственности, если докажет, что клиент сам нарушил порядок использования электронного средства платежа, что повлекло совершение операции без согласия клиента. Таким нарушением может быть передача третьим лицам пароля личного кабинета клиента, ПИН-кода или CVC-кода карты и других данных, позволяющих производить операции по счету.

Списание денежных средств может быть и результатом преступной деятельности: подтверждение операций по карте незаконно привязали к чужому номеру телефона, оператор связи выпустил дубликат сим-карты, на которую поступают банковские коды без согласия владельца, произошло хищение банковской карты или телефонного аппарата, осуществлен взлом личного кабинета на сайте банка, отметил специалист. При этом добровольное сообщение мошенникам секретных кодов, паролей и других средств доступа к операциям может быть расценено как нарушение договора с банком, при котором добиться возврата средств не получится.

«Для проведения доследственной проверки потерпевший должен подать заявление о возбуждении уголовного дела в полицию. При выявлении признаков преступления будет возбуждено уголовное дело, а к виновным лицам, обвиняемым по делу, может быть также предъявлен гражданский иск в уголовном процессе, который и будет содержать денежные требования, направленные на возмещение ущерба, причиненного преступлением», — сообщил собеседник «Известий».

Антонов рекомендовал во избежание потери денежных средств, хранящихся на карточном счете, держать в тайне ПИН-код банковской карты и CVC-код, расположенный на оборотной стороне карты, никому не передавать ни карту, ни мобильный телефон, нанести свою подпись в поле на оборотной стороне карты, не сообщать звонящим по телефону лицам, которые представляются сотрудниками банка, а также говорящим роботам никакой персональной и секретной информации — в таких случаях лучше лично перезвонить в банк по официально опубликованному номеру (входящие звонки переводить в исходящие).

«Опасность для потребителя представляет и совершение покупок с использованием банковской карты на интернет-сайтах, вызывающих подозрение, скачивание банковских приложений из неофициальных источников. Действенными мерами защиты также могут быть применение сложных паролей и установление двухфакторной аутентификации для доступа в электронную почту, держать большую часть денежных средств на отдельном банковском счете

и переводить на карту частями по мере необходимости, установить для банковской карты лимит суточного снятия денежных средств, стереть CVC-код на оборотной стороне карты, сообщать в банк номера телефонов, с которых звонят мошенники», — сказал он.
Многие банки на своих интернет-сайтах размещают правила безопасности и обобщают опыт борьбы с хищениями, это дополнительная инструкция по технике безопасности потребителя финансовых услуг, заключил юрист.

Какую компенсацию могут получить клиенты банка от мошеннических списаний

06.10.2023 \ АРБ ШПАРГАЛКА

МОСКВА, 6 окт — ПРАЙМ. С октября страховка банковских карт покрывает риски от мошеннических списаний денежных средств. По новым правилам клиент банка сможет получить крупную компенсацию, рассказал агентству "Прайм" адвокат, преподаватель Финансового университета при Правительстве РФ Кирилл Данилов.
Минимальный размер страховой выплаты по банковским картам начал действовать с 1 октября 2023 года.
"Новые требования ЦБ направлены на то, чтобы страховщики не затягивали срок выплаты возмещения. Кроме того, установлен минимум возмещения, на который может претендовать клиент", — указывает юрист.
Согласно нововведениям, страховщик должен выплатить средства в срок, не превышающий 30 дней со дня получения заявления и необходимых документов от потерпевшего.
Если сумма, которую мошенники украли с карты, меньше или равна 100 тысячам рублей, то страховая полностью возместит ущерб. Если украдена большая сумма, то размер выплаты составит не меньше 100 тысяч рублей.
В то же время потеря или повреждение электронного средства платежа под страховой случай не подпадает.
Страховка также не покроет события, при наступлении которых оператор по переводу денежных средств обязан по закону возместить своему клиенту сумму операции. "Речь идет о случаях совершения операций без уведомления и получения согласия клиента", — поясняет Данилов.
Все эти требования приняты в пользу клиентов. "Но необходимо помнить, что заключение таких страховых договоров является добровольным и не может быть навязано. Заключение договора с банком также не обязывает гражданина подписывать договор страхования", — подытожил адвокат.