Памятка
об основных способах совершения сотовых мошенничеств с банковскими картами и мерах их предупреждения

Одна из схем сотового мошенничества выглядит следующим образом. Злоумышленники звонят и представляются специалистами социальных служб или сотрудниками банков. Они обещают различные льготы, социальные выплаты и компенсации. Предлагают оформить кредит с минимальной ставкой или снизить проценты по действующему кредиту. Своими обещаниями они вызывают доверие и усыпляют бдительность. Во время разговора мошенники предлагают «проверить», какая льгота положена и какую сумму можно получить. Для этого абоненту нужно сообщить паспортные данные и информацию по банковской карте, на которую якобы переведут деньги. Дополнительно уточняют, к какому номеру телефона привязана карта.

Через некоторое время у владельца карты пропадает со счета крупная сумма или все деньги. Злоумышленники воспользовались информацией и оплатили дорогостоящую покупку с карты жертвы.

По-прежнему звонят мошенники, которые выдают себя за работников банков. Сначала владелец карты получает сообщение, что с карты списаны деньги. Сообщение не вызывает сомнения, потому что номер злоумышленников напоминает номер банка. Через несколько секунд злоумышленник звонит и выдает себя за работника службы безопасности банка. Мнимый сотрудник говорит, что прямо сейчас кто-то пытается снять деньги с вашей карты, нужно действовать быстро и сработать на опережение. После такого напора злоумышленник просит назвать одноразовый пароль из смс или кодовое слово — они якобы нужны, чтобы отменить операцию. Как только человек сообщает код, мошенник тут же списывает деньги. Отличительная черта мошенников — говорят уверенно, часто повторяют слово «безопасность» и торопят с ответом.

Заметно участились случаи рассылки смс-сообщений, содержащих информацию о том, что банковская карта абонента заблокирована в силу ряда причин. Иногда подобные сообщения содержат призыв перевести деньги для разблокировки карты, иногда абонента просят позвонить или отправить смс на короткий номер. После чего происходит списание средств.

Имеют место случаи когда мошенник прикидывается сотрудником банка. А чтобы человек не распознал обман, запугивает его — говорит, что по карте произошла подозрительная операция и списались деньги. Затем злоумышленник интересуется, проводился ли платеж в ближайшее время. Чтобы отменить несанкционированное списание, «представитель банка» предлагает открыть резервный счет и перевести на него деньги. Клиента просят пройти «верификацию»: назвать номер банковской карты и срок ее действия после чего неправомерно завладевают его денежными средствами.

Часто мошенники, представляются сотрудниками полиции, прокуратуры, следственного комитета, другими сотрудниками правоохранительных органов, Центробанка, просят перевести денежные средства под каким-либо предлогом.

Чтобы не оказаться жертвой мошенников необходимо знать следующее:

– сотрудники любого банка никогда не просят сообщить данные банковской карты (номер карты, срок её действия, секретный код на оборотной стороне карты), так как у них однозначно имеются эти данные;

– не при каких обстоятельствах никому не сообщать данные банковской карты, а так же секретный код на оборотной стороне карты;

– хранить пин-код отдельно от карты, ни в коем случае не писать пин-код на самой банковской карте;

– не сообщать пин-код третьим лицам;

– лучше избегать телефонных разговоров с подозрительными людьми, которые представляются сотрудниками банка, не бояться прервать разговор, положить трубку;

– внимательно читать СМС сообщения приходящие от банка;

– никогда и никому не сообщать пароли, и секретные коды, которые приходят в СМС сообщении от банка;

– помнить, что только мошенники спрашивают секретные пароли, которые приходят к в СМС сообщении от банка;

– сотрудники банка никогда никого не попросят пройти к банкомату;

– если вас попросили пройти с банковской картой к банкомату, то это очевидно мошенники;

- при любых подозрениях, что в отношении вас возможно совершаются мошеннические действия, сообщить в полицию по телефону 02, или 020 с мобильного телефона, а так же по телефонам дежурной части УМВД России по г. Кургану 45-64-48, 49-57-97.

Банк России

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

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

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 значика 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

Банк России

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

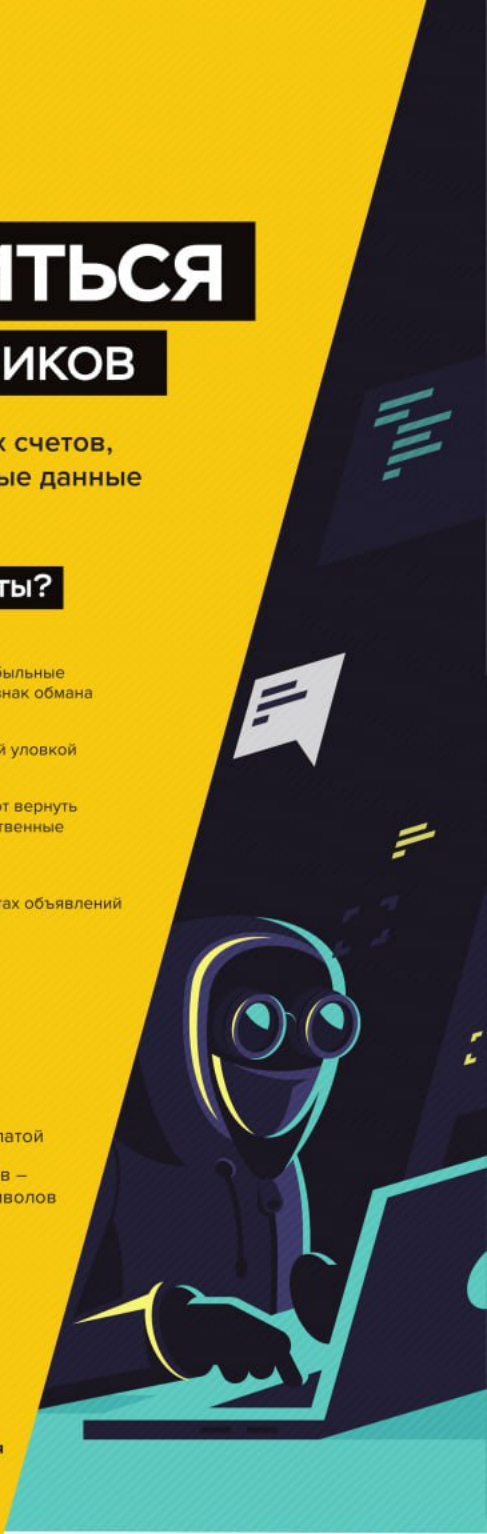
ЗАМАНИВАЮТ НА РАСПРОДАЖИ
Огромные скидки и низкие цены могут оказаться мошеннической уловкой

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

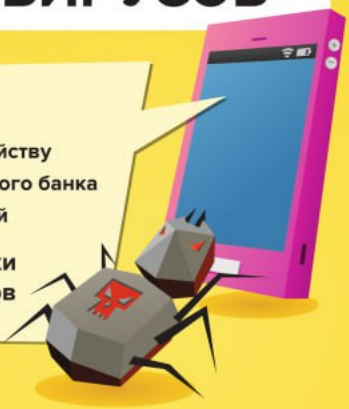


Подробнее о правилах кибергигиены читайте на fincult.info

Финансовая культура

Банк России

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