НЕ ДАЙ СЕБЯ ОБМАНУТЬ!

ЗВОНОК ОТ МОШЕННИКА-«БРОКЕРА»

КАК РАСПОЗНАТЬ?

ПОЛИЦИЯ КУЗБАССА РЕКОМЕНДУЕТ

1. ***ОБЕЩАЕТ БЫСТРОЕ ОБОГАЩЕНИЕ*** за счет торговли на финансовых рынках, вложения в ценные бумаги;
2. ***ПРОСИТ УСТАНОВИТЬ*** на телефон или компьютер специальную ***ПРОГРАММУ***, зарегистрироваться на сайте и внести предоплату;
3. ***ПЫТАЕТСЯ*** убедить ***ОФОРМИТЬ*** крупные ***ЗАЙМЫ*** и пополнить брокерский счет на крупную сумму, обещая высокий доход;
4. ***ОТСУТСТВУЕТ*** реальная ***ВОЗМОЖНОСТЬ ВЫВОДА ДЕНЕГ.***

ЧТО ДЕЛАТЬ?

- **НЕ ОТВЕЧАЙТЕ НА ЗВОНКИ** с неизвестных вам номеров;
- **НЕ ВЕРЬТЕ** любой информации о быстром обогащении;
- **НЕ ЗАНИМАЙТЕ ДЕНЬГИ** и **НЕ ОФОРМЛЯЙТЕ КРЕДИТЫ** под диктовку
- **НЕ ПЕРЕВОДИТЕ** свои деньги на чужие счета;
- **ПРЕРВИТЕ РАЗГОВОР** и сообщите о произошедшем в полицию по телефону **«02»** (с мобильного – **«102»**)!

НЕ ДАЙ СЕБЯ ОБМАНУТЬ!

МОШЕННИКИ НА САЙТАХ ОБЪЯВЛЕНИЙ

КАК РАСПОЗНАТЬ?

ПОЛИЦИЯ КУЗБАССА РЕКОМЕНДУЕТ

1. **НИЗКАЯ СТОИМОСТЬ** товара;
2. **ТРЕБОВАНИЕ БЕЗНАЛИЧНОГО РАСЧЕТА;**
3. Предложение **ПОДКЛЮЧИТЬ «МОБИЛЬНЫЙ БАНК»;**
4. Предложение **ВОСПОЛЬЗОВАТЬСЯ СЕРВИСОМ «БЕЗОПАСНАЯ СДЕЛКА»;**
5. Покупатель готов **СОВЕРШИТЬ ПОКУПКУ, НЕ ВЗГЛЯНУВ НА НЕЕ;**
6. Покупатель просит **НАЗВАТЬ РЕКВИЗИТЫ БАНКОВСКОЙ КАРТЫ** и **ПАРОЛИ ИЗ СМС;**
7. Продавец **ТРЕБУЕТ ПРЕДОПЛАТУ.**

ЗАПОМНИТЕ:

Главная цель мошенника – **ПОДКЛЮЧИТЬСЯ К ВАШЕМУ «МОБИЛЬНОМУ БАНКУ»;**

Для совершения денежного перевода необходим **ТОЛЬКО НОМЕР БАНКОВСКОЙ КАРТЫ;**

ПРЕДЛОЖЕНИЕ ПРОЙТИ К БАНКОМАТУ для получения либо подтверждения перевода Верный признак того, что **ВАС ПЫТАЮТСЯ ОБМАНУТЬ!**

НЕ ОТКРЫВАЙТЕ ИНТЕРНЕТ-ССЫЛКИ от собеседника, они могут быть вредоносны!

БУДЬТЕ ВНИМАТЕЛЬНЫ при купле-продаже через **СЕРВИС «БЕЗОПАСНАЯ СДЕЛКА». Злоумышленник может прислать Вам ССЫЛКУ-ДУБЛЕР, которая ИМИТИРУЕТ** формуляр онлайн-страницы сервиса. В этом случае Ваши деньги будут перечислены не на виртуальный счет, а напрямую на карту мошенника.

ПРЕРВИТЕ РАЗГОВОР и сообщите о произошедшем в полицию по телефону **«02»** (с мобильного – **«102»**)!

НЕ ДАЙ СЕБЯ ОБМАНУТЬ!

ЗВОНОК ОТ МОШЕННИКА-«БАНКИРА»

КАК РАСПОЗНАТЬ?

1. **СООБЩАЕТ О БЛОКИРОВКЕ ВАШЕЙ КАРТЫ**, попытке хищения денежных средств или оформления кредита от Вашего имени;
2. **ПРЕДЛАГАЕТ ЗАБЛОКИРОВАТЬ** несанкционированную **ОПЕРАЦИЮ,**
3. **ОТПРАВЛЯЕТ ВАС В БАНК ОФОРМИТЬ** «зеркальный» **КРЕДИТ** либо перевести денежные средства на «безопасный» счет;
4. **ПЕРЕДАЕТ ТРУБКУ ПСЕВДОСОТРУДНИКУ** правоохранительных органов, который просит принять участие в «операции» по поимке мошенников из числа сотрудников банка;
5. **ПРОСИТ НАЗВАТЬ РЕКВИЗИТЫ БАНКОВСКОЙ КАРТЫ,** защитный код с ее обратной стороны и поступившие на телефон пароли;
6. **УБЕЖДАЕТ УСТАНОВИТЬ ПРОГРАММУ** удаленного доступа на телефон или компьютер;

ПОЛИЦИЯ КУЗБАССА РЕКОМЕНДУЕТ

ЗАПОМНИТЕ:

- **НЕ ОТВЕЧАЙТЕ НА ЗВОНКИ** с неизвестных вам номеров;
- **НЕ ВЕРЬТЕ ИНФОРМАЦИИ ОТ НЕЗНАКОМЦА,** даже если звонок поступил с официального телефона горячей линии банка или правоохранительного ведомства;
- **НЕ УСТАНАВЛИВАЙТЕ** на телефон или компьютер **ПРОГРАММЫ УДАЛЕННОГО ДОСТУПА;**
- **ПОМНИТЕ:** код от вашей карты и пароли подтверждения операций **НЕ ИМЕЕТ ПРАВО ЗАПРАШИВАТЬ ДАЖЕ СОТРУДНИК БАНКА;**
- **ПРЕРВИТЕ РАЗГОВОР** и сообщите о произошедшем в полицию по телефону **«02»** (с мобильного – **«102»**)!

НЕ ДАЙ СЕБЯ ОБМАНУТЬ!

«КОМПЕНСАЦИЯ» ОТ МОШЕННИКОВ

КАК РАСПОЗНАТЬ?

ПОЛИЦИЯ КУЗБАССА РЕКОМЕНДУЕТ

1. Поступление **ТЕЛЕФОННОГО ЗВОНКА С НОМЕРОВ,** начинающихся, преимущественно, с цифр **«8-495...», «8-499...», «8-812...»;**

2. Собеседник **ПРЕДСТАВЛЯЕТСЯ РАБОТНИКОМ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ,** сообщает, **БУДТО ВАМ ПОЛОЖЕНА КОМПЕНСАЦИЯ** от «МММ» либо за ранее приобретенные медицинские препараты или БАДы;

3. Собеседник **ПЫТАЕТСЯ УБЕДИТЬ ВАС, ЧТО** для получения денег **НЕОБХОДИМО ОПЛАТИТЬ** НДС, страховку, доставку или другие услуги.

ЗАПОМНИТЕ:

ЗАПОМНИТЕ: КОМПЕНСАЦИЯ от «МММ» либо за ранее приобретенные медицинские препараты или БАДы – это стандартная УЛОВКА МОШЕННИКОВ!

НЕ ПРИОБРЕТАЙТЕ медицинские препараты или добавки **ЧЕРЕЗ ИНТЕРНЕТ** и **НЕ ЗАКАЗЫВАЙТЕ ИХ ПО ТЕЛЕФОНУ.** Любой курс терапии назначается только лечащим врачом!

НЕ ПЕРЕВОДИТЕ ДЕНЬГИ по просьбе незнакомцев, кем бы они ни представлялись!

ПРЕРВИТЕ РАЗГОВОР и сообщите о произошедшем в полицию по телефону **«02»** (с мобильного – **«102»**)!

НЕ ДАЙ СЕБЯ ОБМАНУТЬ!

ЗВОНОК ОТ МОШЕННИКА-«РОДСТВЕННИКА»

КАК РАСПОЗНАТЬ?

ПОЛИЦИЯ КУЗБАССА РЕКОМЕНДУЕТ

1. **ЗВОНИТ** на телефон, **НАЗЫВАЕТ ВАС МАМОЙ ИЛИ ПАПОЙ (БАБУШКОЙ ИЛИ ДЕДУШКОЙ),** сообщает, будто совершил ДТП или преступление, в результате которого пострадал человек;

2. Передает телефон **ЯКОБЫ СОТРУДНИКУ** правоохранительных органов, который **БУДЕТ УБЕЖДАТЬ, ЧТО** для избавления родственника от уголовного преследования **НЕОБХОДИМЫ ДЕНЬГИ;**

3. **ПЫТАЕТСЯ УДЕРЖАТЬ ВАС** на связи любыми способами, **ЧТОБЫ НЕ** дать возможности **ПОЛОЖИТЬ ТРУБКУ.**

ЗАПОМНИТЕ:

ЗАДАЙТЕ собеседнику **ВОПРОС,** ответ на **КОТОРЫЙ МОЖЕТ ЗНАТЬ ТОЛЬКО БЛИЗКИЙ** Вам человек;

Прервите разговор и **ПЕРЕЗВОНИТЕ РОДНЫМ,** чтобы убедиться, что с ними все в порядке;

Если собеседник представляется работником правоохранительных органов, попросите его **НАЗВАТЬ ФАМИЛИЮ, ИМЯ, ОТЧЕСТВО, А ТАКЖЕ ДОЛЖНОСТЬ И МЕСТО СЛУЖБЫ,** позвоните в соответствующее ведомство и узнайте, действительно ли в нем работает такой сотрудник;

ПОМНИТЕ: ПЕРЕДАЧА ДЕНЕЖНЫХ СРЕДСТВ ДОЛЖНОСТНЫМ ЛИЦАМ за незаконные действия или бездействие **УГОЛОВНО НАКАЗУЕМА!**

ПРЕРВИТЕ РАЗГОВОР и сообщите о произошедшем в полицию по телефону **«02»** (с мобильного – **«102»**)!

НЕ ДАЙ СЕБЯ ОБМАНУТЬ!

ХИЩЕНИЕ ДЕНЕГ С УТРАЧЕННОЙ БАНКОВСКОЙ КАРТЫ ИЛИ СМАРТФОНА

В случае утраты или хищения Ваших БАНКОВСКОЙ КАРТЫ ИЛИ СМАРТФОНА следует В МАКСИМАЛЬНО КОРОТКОЕ ВРЕМЯ ПРИНЯТЬ МЕРЫ, чтобы злоумышленники не воспользовались ими для получения ДОСТУПА К ВАШИМ ДЕНЕЖНЫМ СРЕДСТВАМ.

ЧТО ДЕЛАТЬ?

ПОЛИЦИЯ КУЗБАССА РЕКОМЕНДУЕТ

ЗАБЛОКИРУЙТЕ БАНКОВСКУЮ КАРТУ, позвонив в службу поддержки банка (номер указан на оборотной стороне карты и на сайте банка), или сделайте это самостоятельно в мобильном приложении банка;

После блокировки карты **НАПИШИТЕ В ОФИСЕ БАНКА ЗАЯВЛЕНИЕ** о ее утрате или хищении, это снимет с Вас ответственность в случае использования платежного средства в противоправных целях;

В случае утраты смартфона **КАК МОЖНО БЫСТРЕЕ ИЗМЕНИТЕ ЛОГИНЫ И ПАРОЛИ** мобильного банка и всех своих аккаунтов в социальных сетях, чтобы ваши персональные данные не были скомпрометированы;

О фактах неправомерного снятия денег с Вашего счета или хищении телефона **СООБЩИТЕ В ПОЛИЦИЮ**, позвонив на **«02»** (с мобильного – **«102»**)!

ПОМНИТЕ:

1. **СМС О СНЯТИИ ДЕНЕГ ИЛИ ПОПЫТКЕ ВХОДА В МОБИЛЬНЫЙ БАНК** – признак того, что ваша банковская карта или телефон находятся в руках злоумышленника;
2. **НАДЕЖНЫЙ ПАРОЛЬ и РАЗБЛОКИРОВКА ПО ОТПЕЧАТКУ ПАЛЬЦА** – эффективные способы защиты от неправомерного доступа в Ваш мобильный банк;
3. **НЕ ХРАНИТЕ ЗАПИСАННЫЕ НА БУМАГУ ПАРОЛИ** доступа к своим счетам вместе с банковскими картами;
4. Не храните на телефоне **ФОТОГРАФИИ ПАСПОРТА И ДРУГИХ ЛИЧНЫХ ДОКУМЕНТОВ;**
5. **УСТАНОВИТЕ КОД ДОСТУПА К МОБИЛЬНОМУ БАНКУ,** отличный от пароля к телефону;
6. **УСТАНОВИТЕ ЛИМИТЫ НА ПЕРЕВОДЫ** денежных средств с ваших банковских счетов.

НЕ ДАЙ СЕБЯ ОБМАНУТЬ!

СООБЩЕНИЕ ОТ МОШЕННИКА-«ВЗЛОМЩИКА»

КАК РАСПОЗНАТЬ?

ПОЛИЦИЯ КУЗБАССА РЕКОМЕНДУЕТ

1. В социальной сети от пользователи из списка Ваших друзей поступает **СООБЩЕНИЕ С ПРОСЬБОЙ ОДОЛЖИТЬ ДЕНЬГИ** либо предложением **ПРИНЯТЬ УЧАСТИЕ В РОЗЫГРЫШЕ** (акции банка) и получить гарантированный приз;

2. Собеседник **ПРОСИТ НАЗВАТЬ РЕКВИЗИТЫ** банковской **КАРТЫ И ПАРОЛИ** из СМС-сообщений якобы для зачисления денег.

ПОМНИТЕ:

- **ОТЛИЧИТЬ настоящую страницу пользователя в соцсети от ее дубликата, созданного мошенниками, внешне практически НЕВОЗМОЖНО!**
- **Реквизиты банковской карты являются КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ ее владельца, как и уведомления банка с паролями, необходимыми для подтверждения денежной операции!**

ЧТО ДЕЛАТЬ?

- **ПРЕРВИТЕ ПЕРЕПИСКУ;**
- **ПОЗВОНИТЕ ЧЕЛОВЕКУ,** от имени которого поступило сообщение, и уточните достоверность информации;
- **ЗАЩИТИТЕ ОТ ВЗЛОМА СВОИ АККАУНТЫ** в социальных сетях **ПРИ ПОМОЩИ НАДЕЖНОГО ПАРОЛЯ,** регулярно меняйте его и держите втайне от окружающих;
- **ПРЕРВИТЕ РАЗГОВОР** и сообщите о произошедшем в полицию по телефону **«02»** (с мобильного – **«102»**)!

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

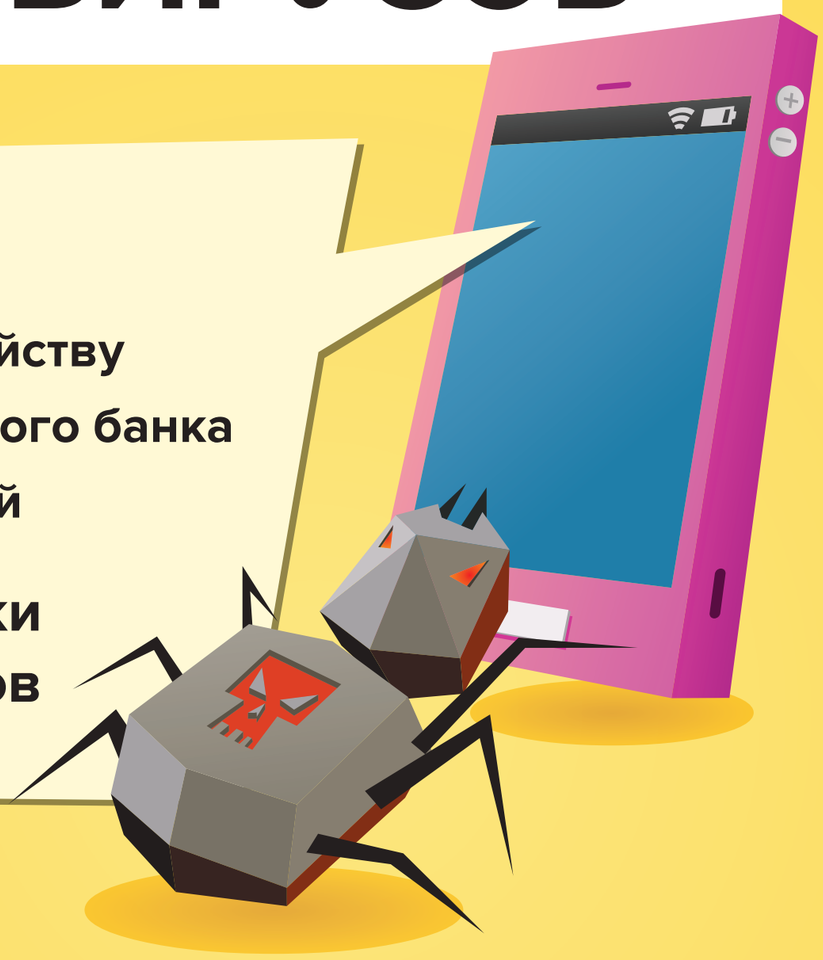
Финансовая культура

Банк России

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ

КАК 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

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 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

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

КОДОВОЕ СЛОВО
называйте только сотруднику банка, когда сами звоните на горячую линию

НЕ ПУБЛИКУЙТЕ
персональные данные в открытом доступе

УСТАНОВИТЕ
антивирусы на все устройства

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

Подробнее о правилах безопасности читайте на fincult.info

Финансовая культура