Как распознать мошенника?

1 ПРИЗНАК - НА ВАС ВЫХОДЯТ САМИ
Вам звонит незнакомец, присылает СМС-сообщение, электронное письмо или ссылку в мессенджере. Кем бы он ни представился — сотрудником банка, полиции, магазина, — насторожитесь.

2 ПРИЗНАК - С ВАМИ ГОВОРЯТ О ДЕНЬГАХ
Схемы обмана почти всегда связаны с финансами: вам предлагают перевести все деньги на «безопасный счет», оплатить «страховку для получения кредита» или «очень выгодно» инвестировать свои сбережения (на самом деле — в финансовую пирамиду).

3 ПРИЗНАК - ВАС ПРОСЯТ СООБЩИТЬ ДАННЫЕ
Настоящий сотрудник банка никогда не спросит секретные реквизиты карты, ПИН-коды и пароли.

4 ПРИЗНАК - ВАС ВЫВОДЯТ ИЗ РАВНОВЕСИЯ
Мошенники стремятся вызвать у вас сильные эмоции — напугать или обрадовать. Так они сбивают с толку и притупляют бдительность потенциальной жертвы.

4 ПРИЗНАК - НА ВАС ДАВЯТ
Мошенники всегда торопят, чтобы не дать вам времени обдумать ситуацию. Вас принуждают к чему-то, ставят условия: «сейчас или будет поздно». Ситуация, в которой вам не дают права выбора и заставляют немедленно действовать, подозрительна.

Что делать, если вы стали жертвой мошенника?

1. Если мошенники использовали вашу банковскую карту, заблокируйте ее в мобильном приложении или позвоните в банк по официальному номеру

2. Сообщите о мошенничестве в ваш банк

3. Просим обо всех случаях мошенничества сообщать: по телефону 02 (или 102) или по телефону доверия МВД по РС(Я): 45-22-22

Звонят с номера банка и просят предоставить конфиденциальные данные. Что делать?

Аферисты могут позвонить не только от имени финансовой компании, но и прокуратуры, налоговой службы, Банка России и других организаций.

Таким образом мошенники пытаются вывести человека из равновесия, застать врасплох. Но как только с вами начинают говорить про деньги, кладите трубку. Позвоните по официальному номеру своего банка и уточните, все ли в порядке с вашими счетом и картой. Не звоните на номер, с которого звонили мошенники!

Как защитить свои деньги от мошенников?

1. Всегда набирайте только официальный номер банка. Он указан на обратной стороне карты и на официальном сайте банка;

2. Не перезванивайте и не отправляйте СМС на незнакомые номера, не спешите переходить по ссылкам из сообщений;

3. Если вам звонят из банка, финансовой организации или госоргана, уточните ФИО и должность звонящего и скажите, что перезвоните ему сами. Положите трубку и перезвоните по официальному телефону организации или на горячую линию банка. Номер нужно набрать вручную;

4. Не стоит паниковать и спешить. Если банк выявит подозрительную транзакцию, он сразу приостановит ее на срок до двух суток. За это время вы можете либо подтвердить эту операцию банку, либо отменить ее. Это решение надо принять в течение 48 часов — этого времени достаточно, чтобы хорошо все обдумать и без спешки самостоятельно позвонить в банк. Если же вы ничего не сделаете, то через двое суток банк автоматически снимет блокировку и операция пройдет;

5. Ни под каким предлогом никому не сообщайте личные данные, реквизиты карты и секретную информацию: CVC/CVV-код на обратной стороне карты, коды из СМС и ПИН-коды. Называть кодовое слово можно, только если вы сами звоните на горячую линию банка.

АЭБ
АКБ «АЛМАЗЭРГИЭНБАНК» АО

Бесплатная горячая линия:
8-800-100-34-22
Call-центр
(4112) 34-22-22
www.albank.ru

АКБ «Алмазэргиэнбанк» АО, г. Якутск, пр. Ленина, 1.
Генеральная лицензия ЦБ РФ №2602 от 08.06.2015.
Материал носит информационный характер
и не является публичной офертой.

Как обезопасить себя от мошенничества

Списание денег со счета без ведома владельца, кража паролей и ПИН-кодов, легкий заработок в интернете и вклады под невероятные проценты, онлайн-казино — все это виды финансового мошенничества. Преступники будут спекулировать на ваших чувствах, обещать золотые горы, маскироваться под сотрудников банков или гос. организации, чтобы выманить деньги.

Как распознать мошенника и что делать, если вас все-таки удалось обмануть?

Как обезопасить гаджеты от мошенников

Мошенники выманивают конфиденциальные данные, с помощью социальной инженерии и фишинга.
Нередко они рассылают сообщения со ссылками на вредоносные программы или файлами, содержащими вирусы. С помощью них киберпреступники надеются получить доступ к гаджетам
и украсть с них секретные данные.

Как защитить устройство?

- Пользуйтесь антивирусами;
- Постоянно обновляйте систему;
- Скачивайте только проверенные приложения;
- Для защиты устройства включите автоматическую блокировку экрана;
- Регулярно делайте «бэкап» – резервное копирование ваших данных;
- Выбирайте сложные пароли;
- Установите программу, чтобs дистанционно отслеживать местоположение устройства;
- Не устанавливайте программы по просьбе незнакомцев;
- Изучайте настройки конфиденциальности.

Узнайте больше о финансовой безопасности на albank.ru

https://albank.ru/ru/more/info/security/

Финансовая кибербезопасность

Установите **антивирус** на телефон и компьютер

Используйте **защищенный вайфай**

Скачивайте мобильные приложения только **в официальных магазинах**

Установите **двухфакторную аутентификацию**, где возможно

Используйте защищенные папки на устройствах для персональной информации

Перед покупкой **проверяйте подлинность** Интернет магазина

Используйте **отдельную карту** для покупок онлайн

Подключите СМС-оповещения от банка обо всех операциях по карте

Используйте приложения для **определения незнакомых номеров**

Не передавайте платежные данные, пароли и коды **третьим лицам**

Не публикуйте персональные данные (например, **номер телефона**)

Используйте разные пароли для разных сервисов, периодически **обновляте их**

Как уберечь себя и своих близких от финансового мошенничества

Стать жертвой преступников может каждый, и неважно, использует он банковскую карту или предпочитает рассчитываться наличными. Мошенники умеют выманивать деньги онлайн, с помощью звонков и СМС, в социальных сетях и офисах.

Мошенничество с банковскими картами

Чтобы использовать вашу карту в своих целях, мошенникам нужно узнать ее номер, имя владельца, срок действия, номер CVC или CVV. Они могут установить скиммер на банкомат (специальное устройство, которое накладывают на приемник карты в банкомате) и видеокамеру над клавиатурой.

Мошеннические организации

Сейчас финансовые пирамиды начинают маскироваться под микрофинансовые организации, работающие по принципу сетевого маркетинга, инвестиционные и управляющие предприятия, онлайн-казино.

Кибермошенничество

Кибермошенники отправляют сообщение якобы от банка со ссылкой, просьбой перезвонить по номеру или с уведомлением о крупном выигрыше. Или звонят от имени банка и просят сообщить личные данные, ПИН-код от карты или номер СМС-подтверждения. Или пишут в социальных сетях от имени друзей или родственников, которые внезапно попали в беду и просят перевести энную сумму денег на неизвестный счет.

Мошенничество на финансовых рынках

Еще один тип мошенников — псевдопрофессиональные участники финансового рынка, которые активно рекламируют свои услуги по организации торговли на рынке Форекс.