Фразы, которые чаще всего используют мошенники. Услышав их - смело бросайте трубку!

В другом городе была совершена сомнительная операция по карте либо зафиксирована попытка несанкционированного списания средств со счета.

Так мошенники начинают разговор. Вас вовлекают в диалог и под предлогом обезопасить сбережения мошенники узнают конфиденциальную информацию по банковской карте. Никогда и никому не сообщайте уникальные данные банковской карты.

Необходимо срочно перевести денежные средства на безопасный счет либо передайте наличность сотруднику банка

Мошенники сами предоставляют реквизиты якобы безопасного счета, зачастую просят жертву пройти к банкомату, снять сбережения и передать их третьим лицам. Никогда не совершайте банковские операции по телефонной просьбе посторонних лиц.

На Вас оформили кредит

Так мошенники узнают данные карты и оформляют уже настоящий кредит, похищают деньги или совершают покупки с Вашей карты. Зачастую, мошенники по телефону просят оформить кредит либо заложить квартиру, объясняя, что это позволит обезопасить сбережения и недвижимость. Никогда не берите кредиты по просьбе незнакомцев.

Продиктуйте код из смс

Сообщая данный код, Вы предоставляете мошеннику доступ к переводу денежных средств.

Установите безопасное приложение

Мошенники могут отправить ссылки для установки программы, но такие якобы «безопасные» программы и мобильные приложения предоставляют злоумышленникам доступ к счетам и персональной информации.

Возникли сомнения, что звонит сотрудник банка - прекратите разговор. Позвоните в свой банк самостоятельно!

Если Вы стали жертвой или свидетелем мошенничества незамедлительно сообщите в полицию (102,112).

Мошенничество в отношении пенсионеров

Чтобы Ваши престарелые родственники или знакомые не пострадали от рук мошенников, расскажите им следующие правила:

никогда не пускайте в квартиру подошедших на улице или позвонивших в дверь незнакомых людей, кем бы они не представлялись (работниками социальных, коммунальных служб, медицинскими работниками), если Вы предварительно не вызывали их.

если человек представился сотрудником социальной службы- попросите предъявить удостоверение или поднести его к глазку двери,
держите на видном месте телефоны полиции, социальных служб, пенсионного фонда. Не бойтесь звонить с уточнениями, действительно ли у них работает пришедший к Вам сотрудник и с какой целью он ходит по квартирам. Если телефон не отвечает (занят) – попросите посетить Вас в другое время,
позвоните родным и сообщите о «непрошенном госте»,
если человек настойчиво просится в квартиру – позовите соседей,
не отдавайте документы (паспорт, пенсионное, ветеранское удостоверение и др.),
не отдавайте деньги и ничего не подписывайте, не приобретайте продукты, мелкую бытовую технику, лекарства
Если же случилось, что Вас обманули – немедленно звоните в полицию. Постарайтесь запомнить внешность и особые приметы, это облегчит поиск мошенника и предотвратит последующие преступления.

Как обезопасить себя при поступлении СМС или звонка о блокировке карты?

СИТУАЦИЯ: Вам приходит сообщение о том, что банковская карта заблокирована. Для получения подробной информации указан определенный номер, после звонка, на который предлагают сообщить номер карты и ПИН-код для ее перерегистрации, либо дойти до ближайшего банкомата и следуя «подсказкам» оператора разблокировать карту.

КАК ОБЕЗОПАСИТЬ СЕБЯ:

Не торопитесь выполнять требования лица, представившегося сотрудником банка. Свяжитесь со службой поддержки клиентов банка самостоятельно.

Никогда и никому не сообщайте ПИН-код карты и пароли из СМС-сообщений от банка. Ни сотрудники банки, ни любой другой организации не вправе их требовать.

Относитесь к ПИН-коду и паролю из СМС как к ключам от сейфа с Вашими средствами.

Помните: сотрудники службы поддержки банка никогда не запрашивают личные данные по телефону, никогда не отправляют ссылки на скачивание каких-либо программ.

Как обезопасить себя от телефонных вирусов?

СИТУАЦИЯ: на телефон приходит сообщение со следующим текстом: "Вам пришло ММС-сообщение. Для получения пройдите по ссылке...". При переходе по указанному адресу на телефон скачивается вирус и происходит списание денежных средств со счета.

Создание сайтов-двойников-один из способов кражи паролей, номеров кредитных карт, банковских счетов. Внешне такие сайты не отличаются от оригинальных, разница как правило в одной букве адреса. Если не заметить

разницы и ввести свои логин и пароль на таком сайте, то эти данные окажутся в руках мошенника.

КАК ОБЕЗОПАСИТЬ СЕБЯ?

Обращайте внимание на правильность написания адреса сайта, а также на показатели безопасности сайта, такие какзначок закрытого замка в адресной строке браузера и наличие буквы "s" (обозначает "secure"-безопасный), "https://"в начале адреса сайта. Если эти элементы отсутствуют - на такой странице небезопасно вводить данные, особенно реквизиты банковских карт.

Используйте антивирусные программы

Не открывайте с телефона сомнительные ссылки из сообщений

Не скачивайте приложения с неизвестных сайтов, из неофициальных магазинов приложений, по ссылкам, которые содержатся в электронных рассылках, рекламе в социальных сетях

Не пользуйтесь "банковскими" приложениями, предустановленными на смартфоне, который вы только что купили

Не сканируйте Qr-коды из недостоверных источников

Помните: перейдя по сомнительной ссылке или установив "безопасное" приложение Вы открываете доступ к своим персональным и платежным данным.

Покупка в интернет-магазине мошенника.

Мошенники пользуются все возрастающей популярностью покупок в интернет-магазинах.

Создать "интернет-магазин" и наполнить его фотографиями товаров, которые якобы есть у продавца-дело нескольких минут. После того, как деньги будут перечислены (такие интернет-магазины обязательно требуют предоплату), сотрудники магазина перестают выходить на связь, а потом магазин бесследно исчезает.

КАК ОБЕЗОПАСИТЬ СЕБЯ?

Никогда не совершайте покупки в непроверенных интернет-магазинах, особенно если требуется внесение предоплаты

Уточните юридический адрес организации и проверьте через интернет существует ли она (например, через сервис 2gis.ru), позвоните, чтобы убедиться в том, что это действительно интернет-магазин

Изучите товар по фото, описанию и отзывам покупателей

Посмотрите, как вернуть деньги; если такой информации нет, уточните у продавца

Помните: от покупки можно отказаться в любое время до получения товара и в течение 7 дней после его получения без объяснения причин

Вы имеете право вернуть товар с нарушенной упаковкой, но в товарном виде и без повреждений

Обратитесь в суд, если продавец не возвращает деньги за возврат товара

В следующем выпуске нашего цикла разъяснений "Будьте осторожны - финансовое мошенничество" - "Финансовые пирамиды".