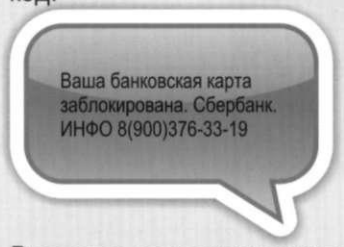
## Схемы телефонного мошенничества


**Обман по телефону:** требование выкупа или взятки за освобождение якобы из отделения полиции знакомого или родственника.

**SMS-просьба о помощи:** требование перевести определенную сумму на указанный номер, используется обращение «мама», «сынок», «друг» и т.д.

**Выигрыш в лотерее, которую якобы проводит оператор связи:**

для получения приза Вас просят перевести определенную сумму на указанный номер телефона или счета и сообщить специальный код.


**SMS «Ваша карта временно заблокирована, перезвоните по номеру»:**

Вам ответит мошенник и попытается узнать реквизиты банковской карты.

**Если Вы сомневаетесь, что звонивший - действительно Ваш друг или родственник, постарайтесь перезвонить на его мобильный телефон.**

## Мошенничество в сети ИНТЕРНЕТ

**Онлайн покупки:** мошенники просят предоплату за несуществующий товар или услугу.

**Дублирование сайтов (фишинг):** мошенники создают свой сайт (группу в социальной сети) или копию сайта по продаже авиабилетов. При этом в реквизитах оплаты указывают свои банковские счета.

**Лже-благотворительность:** интернет пестрит объявлениями о людях, нуждающихся в помощи, однако не спешите перечислять деньги, не проверив необходимую информацию;

**Работа в ИНТЕРНЕТЕ:** работодатели, которые предлагают Вам легкую работу за огромные деньги, не только не заплатят Вам ни копейки, но и обманным путем завладеют вашими деньгами;

**Спам (нежелательное сообщение):** открывая такое сообщение, вы впускаете в свою систему компьютерный вирус-троян, который собирает информацию, а затем высылает её спамерам, которые могут использовать полученное в своих целях.

**Устанавливайте на свои ПК и мобильные устройства только лицензионное ПО.**

## Мошенники в социальных сетях


**Взлом аккаунта друга:** люди могут даже не подозревать, что им пишет посторонний человек.

Таким образом, войдя в доверие, мошенники попытаются украсть ваши деньги;.

**Схемы проведения аукционов в системе on-line:** мошенники в соцсетях предлагают своим жертвам выслать деньги в оплату товара, а затем доставляют изделие намного менее ценное, чем то, которое было заявлено.

**Группы «Отдам даром»:** Опасность может таится в том, что мошенники попросят оплатить пересылку или «защиту от обмана». В результате Вы можете лишиться денежных средств.

**Не распространяйте в социальных сетях слишком подробную информацию о себе, это может отлично сыграть на руку мошенникам.**

**Межведомственная Комиссия по профилактике правонарушений в Моргаушском районе**

**ОМВД России по Моргаушскому району** **Прокуратура Моргаушского района**

# !!! ПРЕДУПРЕЖДАЕТ !!!

## Сайты-двойники

Мошенники создают сайт-двойник официального сайта, на котором совершаются онлайн-покупки. Потерпевший оплачивает услугу, переводя средства на счет преступника. Часто так происходит при заказе страхового полиса на сайте страховой компании. Не убедившись в подлинности источника, посетители заказывают страховку ОСАГО.

## Рассылка SMS

В этом случае на телефон приходит объемный файл с текстом якобы от Вашего знакомого, типа: «Вспомни, как у нас всё было». Вы открываете файл, и ваш телефон заражается вредоносной программой. В итоге с привязанного к сим-карте банковского счета списываются деньги. Подобные смс/ммс могут поступить и от того, чьи контакты действительно есть в вашей записной книжке.

## Рассылка на e-mail

Поступившие на электронную почту письма со ссылками на различные сайты также могут содержать вирусную программу. Перейдя по ссылке, вы запускаете вредоносное программное обеспечение, с помощью которого преступники получают доступ к вашим банковским счетам.

## Переписка в соцсетях

Злоумышленники взламывают страницу в социальной сети и от имени лица, на которое она зарегистрирована, рассылают сообщения его друзьям с просьбой занять деньги. Откликаясь на просьбу товарища, многие люди лишаются таким образом своих денег.

## Кража с потерянного телефона

Также списание денежных средств со счета гражданина может произойти в результате утери им сотового телефона, в котором не была отключена «привязка» телефонного номера к банковским счетам. Ведь любой нашедший телефон человек получает к ним доступ и имеет возможность перевести деньги

## КАК ПРЕДОСТЕРЕЧЬ СЕБЯ?

- В целях получения необходимых услуг пользуйтесь только официальными сайтами. Для оплаты используйте дополнительную карту (не основную)» на которую будет заблаговременно переведена нужная для оплаты приобретаемого товара или услуги сумма.
- При смене сим-карты отключайте так называемые «привязки» номеров телефонов к банковским счетам. При утере телефона с подключенной услугой «Мобильный банк» - сразу же заблокируйте сим-карту либо отмените действие данной услуги.
- Не доверяйте поступившим на телефон или электронную почту емс, в которых требуется переход по различным ссылкам.
Лучше перепроверьте информацию.
- Не перечисляйте деньги друзьям, которые просят об этом в соцсети - возможно, их страница взломана мошенниками. Сначала убедитесь, что товарищи действительно нуждаются в вашей помощи.


## ВАЖНО!

*Сотрудники банка никогда не запрашивают пароли, коды СМС-подтверждений, дату вашего рождения, паспортные данные, состояние счета, номер карты и др. по телефону.*

*Внимательно относитесь к СМС, e-mail-сообщениям и телефонным звонкам от имени банка.*

*Никогда не звоните по номерам, указанным в этих сообщениях и не сообщайте свои персональные данные по телефону.*

*Всю дополнительную информацию узнавайте у официальных представителей банка по телефонам, указанными на карте.*