

# Распространенные виды мошенничества

## 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 это 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



Такая 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 смс, 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 и коды СМС-подтверждений по телефону - никогда никому их не сообщайте! Внимательно относитесь к СМС и e-mail-сообщениям от имени банка, в которых содержится информация о блокировке вашей карты, никогда не перезванивайте по номерам, указанным в этих сообщениях, всю дополнительную информацию узнавайте у официальных представителей банка по телефонам, указанным на карте.*



# ОСТОРОЖНО: МОШЕННИКИ!

## НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

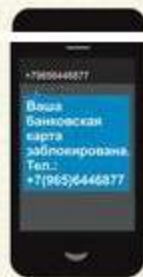
**ИНТЕРНЕТ-МОШЕННИКИ**

### ОБЪЯВЛЕНИЕ О ПОКУПКЕ

Мошенники-покупатели спрашивают реквизиты банковской карты и (или) sms-код якобы для перечисления денег за товар, после чего похищают деньги с банковского счета.



**ТЕЛЕФОННЫЕ МОШЕННИКИ**

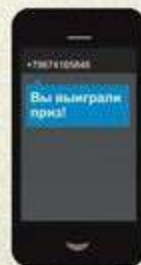


### БЛОКИРОВКА БАНКОВСКОЙ КАРТЫ

Сообщение о блокировании банковской карты с номером, по которому нужно позвонить. Цель – узнать личный код банковской карты.

### ПОЛУЧЕНИЕ ВЫИГРЫША (компенсации за потерянный вклад)

Мошенники сообщают о выигрыше приза, возможности получения компенсации за потерянный вклад в «финансовую пирамиду» и т.п. Жертве можно забрать его, заплатив налог или плату якобы «за сохранность денег».



# ИНТЕРНЕТ-МОШЕННИЧЕСТВА



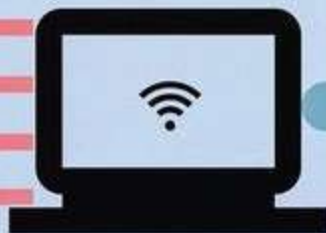
Хищения денег под видом продажи товара ненадлежащего качества, не соответствующего заявленному, с использованием интернет-площадок



При осуществлении входа на сайт уже известных Вам банков или организаций внимательно изучите открывшуюся страницу-она может оказаться двойником



Мошенники создают интернет-сайты "двойники" по продаже товаров, которые идентичны оригинальным



Не производите предоплату товара.



Продажа несуществующей в реальности продукции в лже-интернет магазинах



Деньги можно отдать только в том случае, если заказанный товар проверен и полностью устраивает



Хищение денег с банковских счетов физических лиц при использовании неправомерного доступа к банковским картам потерпевших



Ни под каким предлогом и ни при каких обстоятельствах не сообщайте незнакомым людям цифры, написанные на вашей банковской карте