

#ВБЕЗОПАСНОСТИ



Просят оплатить услуги через камеру мобильного телефона?

Прежде чем направить камеру на неизвестный QR-код, подумайте, насколько эта съемка безопасна для вашего кошелька

Узнать больше:



МВД.РФ

#ВБЕЗОПАСНОСТИ



Звонок от оператора сотовой связи? Закончился договор или действие сим-карты?

Просто положите трубку
или перезвоните
оператору связи сами

Узнать больше:



МВД.РФ

#ВБЕЗОПАСНОСТИ



Звонки из службы безопасности — классика телефонного мошенничества

Прервите разговор
и сами позвоните
в свой банк

Узнать больше:



МВД.РФ

КАК БЫСТРО РАСПОЗНАТЬ МОШЕННИКА?

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



КАК ЗАЩИТИТЬ СВОИ ФИНАНСЫ



Узнай больше на
fincult.info

НЕ ГОВОРИ

НИКОГДА И НИКОМУ

- 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



ЗВОНЯТ

из банка, полиции
или другой организации?



УБЕДИТЕСЬ,

что звонят не
телефонные мошенники!



Банк России



Финансовая
культура



УМВД России по Смоленской области ПРЕДУПРЕЖДАЕТ



ОСТОРОЖНО - МОШЕННИКИ! НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!



ОБЪЯВЛЕНИЕ О ПРОДАЖЕ / ПОКУПКЕ

Мошенники просят перечислить деньги за товар, который впоследствии жертва не получает.

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



СООБЩЕНИЯ ОТ ДРУЗЕЙ/РОДСТВЕННИКОВ

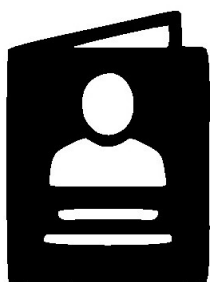
Мошенники пользуются чужой страничкой в социальной сети в Интернете, и под видом Вашего знакомого просят перечислить деньги или сообщить данные Вашей карты, якобы для перечисления Вам денег, под различными предложениями. Могут позвонить от лица близкого человека или от представителя власти. Выманивают деньги под предлогом несчастного случая с близким.

ВЗЛОМ АККАУНТА НА ПОРТАЛЕ «ГОСУСЛУГИ»

Сообщение/звонок от неизвестного о взломе аккаунта на портале «Госуслуги» с номером, по которому нужно позвонить. Цель - запугать Вас, для выполнения дальнейших указаний мошенников.

**БУДЬТЕ
БДИТЕЛЬНЫ**

ФИШИНГ (англ. phishing от fishing — «рыбная ловля, выуживание») — вид интернет-мошенничества, при котором злоумышленники выманивают конфиденциальные данные пользователей — логины, пароли, реквизиты банковской карты. Используют поддельные сайты, письма или сообщения, похожие настоящие. Задача — заставить человека перейти по ссылке, ввести данные и тем самым передать их мошенникам.



**Не сообщайте
неизвестным лицам
персональные
данные**

