ПРАВИЛА
ФИНАНСОВОЙ БЕЗОПАСНОСТИ

1 Звоните в банк сами

Набирайте номер вручную. Телефон горячей линии указан на обратной стороне карты и на официальном сайте банка.

Перезванивая на номер, с которого пришел звонок или сообщение, вы рискуете снова попасть к мошенникам.

2 Сосредоточьтесь

Если банк выявит подозрительную транзакцию, он приостановит ее на срок до двух суток.

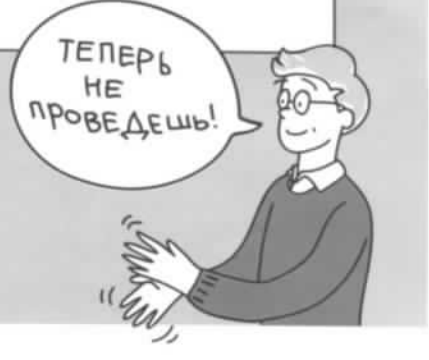
У вас есть 48 часов, чтобы спокойно принять решение: подтвердить или отменить операцию.

3 Не говорите никому секретные коды

Если вас убеждают продиктовать или ввести CVC/CVV-код на обратной стороне карты, пин-код или коды из СМС – это мошенники!

Называть кодовое слово можно, только если вы сами звоните на горячую линию банка.

Подробнее о том, как защититься от киберкраж и финансовых мошенников, читайте на сайте **fincult.info**



Банк России

Контактный центр Банка России:

8 800 300-30-00

(для бесплатных звонков из регионов России)

Интернет-приемная Банка России:

www.cbr.ru/reception

Банк России

ОСТОРОЖНО: ТЕЛЕФОННЫЕ МОШЕННИКИ!

5 ПРИЗНАКОВ ОБМАНА

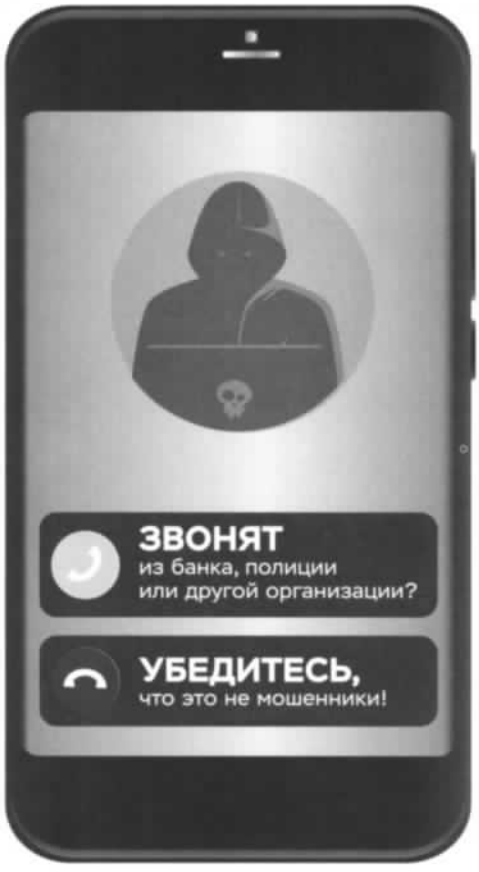
1 НА ВАС ВЫХОДЯТ САМИ

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

НИКОГДА НИКОМУ НЕ СООБЩАЙТЕ:

- 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

Как защитить свои финансы, читайте на fincult.info

Финансовая культура

Доведите до граждан простые правила защиты от телефонных мошенников (особенно пожилым):

1. Службе безопасности банка не требуется получать от клиента никакой дополнительной информации (у них она и так есть). Сотрудники банка в состоянии самостоятельно при остановить движение средств по карте, если транзакции им покажутся подозрительными.

2. Если вам по телефону представляются сотрудником банка или полицейским, всегда считайте, что общаетесь с мошенником (в 99,999% случаев это соответствует действительности).

3. Когда кто-то представляется вам сотрудником службы безопасности банка, смело кладите трубку и перезванивайте по номеру на банковской карте. Если вам действительно звонил представитель банка - вас соединят с ним.

4. Банк никогда не будет просить вас сделать что - то через банкомат. Настоящие сотрудники банка пригласят вас в свой ближайший офис. Если вас просят сходить к банкомату и совершить там какое-то действие – это……

5. Сотрудники полиции (и других силовых ведомств) никогда не привлекают граждан к оперативно-розыскным мероприятиям по телефону. Всегда организуется личная встреча.

6. Ни в коем случае никогда не переводите деньги, следуя рекомендациям по телефону. Не сообщайте собеседнику ни код из СМС, ни данные вашей карты. Попросить сообщить код может лишь сотрудник банка в офисе (в таком СМС будет указано, что код следует сообщить сотруднику банка).

7. Для оформления карт с повышенным кэшбэком, выгодных условиях вклада и прочих заманчивых предложений не требуются личные данные, реквизиты банковской карты и сообщение кода из СМС. Если под предлогом оформления выгодных банковских продуктов у Вас пытаются получить эти сведения – вы разговариваете с мошенниками.

8. Сотрудники полиции не когда не будут по телефону у Вас просить денежное вознаграждение, за урегулирования вопросов с правоохранительными органами (например, Ваш сын, внук попал в ДТП).

ГУ МВД России по Волгоградской области

*Для прослушивания голосовых аудиозаписей, наведите камеру мобильного телефона, нажмите на всплывающую ссылку