

# НЕ ПОПАСТЬ НА УДОЧКУ МОШЕННИКОВ

## ЛИШИТЬСЯ ЧЕСТНО ЗАРАБОТАННЫХ СРЕДСТВ СЕГОДНЯ ОЧЕНЬ ПРОСТО

### БУДЬТЕ ВНИМАТЕЛЬНЫ ПРИ РАБОТЕ С КАРТОЙ ОФФЛАЙН

- При утере или подозрении на действия мошенников, немедленно заблокируйте карту
- Никому не сообщайте пин-код и другие данные карты
- Прикрывайте номер, пин и CVV-код карты во время ввода в терминале или банкомате
- Если банкомат вызывает у вас подозрение, воспользуйтесь другим терминалом
- В случае подозрительного звонка прекратите разговор и обратитесь в ближайшее отделение банка

### НЕ ПОЗВОЛЬТЕ ПСЕВДО-БЛАГОТВОРИТЕЛЯМ СЫГРАТЬ НА ВАШЕЙ ДОБРОТЕ

- Сборы средств на улицах и в транспорте в 99% случаев - мошенничество
- Сборы денег на лечение якобы тяжелобольных детей, нуждающихся в дорогостоящих операциях
- Проверьте наличие у благотворительного фонда сайта с контактами и отчётами о расходах за последний год
- Мошенники часто привлекают к сбору средств подростков
- Обманщики никогда не пригласят провести мастер-классы или посидеть с большими детьми



### ЧАСТЫЕ СПОСОБЫ ОБМАНА ПО ТЕЛЕФОНУ:

– Вам звонят и представляются сотрудником Банка (чаще всего «сотрудником финансовой службы безопасности»), сообщают о выявлении подозрительных операций по счету и якобы «для сохранности Ваших денег» просят назвать полные данные карты, CVV- или CVC-код, код из СМС или пароли интернет-банка.

**ЗАПОМНИТЕ!** Работник Банка НИКОГДА не попросит назвать ему секретные данные карты или интернет-банка!

- Вам приходит SMS о выигрыше в конкурсе, где вы не участвовали, а для получения приза требуется денежный взнос
- Звонящий представляется сотрудником прокуратуры/полиции/суда/мобильных операторов и т.д.
- Вам звонят и сообщают, что ваш близкий якобы попал в беду, просят перевести деньги и не звонить пострадавшему
- Вам сообщают, что ваша карта якобы заблокирована, и нужно срочно назвать все её данные

### МЕРЫ БЕЗОПАСНОСТИ В СЕТИ

– Совершайте покупки только на проверенных онлайн-площадках

- Не стоит устанавливать сторонние приложения для хранения паролей
- Не оставляйте свои персональные данные на сомнительных сайтах
- Заведите дополнительную банковскую карту с ограниченным лимитом
- Подключите SMS-уведомления о движении средств на счёту
- Не совершайте никаких операций по инструкциям незнакомых Вам людей
- Следите за актуальностью базы антивируса вашего компьютера
- Не скачивайте программы для смартфона по просьбе лжесотрудников банка (с помощью приложений удаленного доступа к устройству мошенники могут получить пароли к личному кабинету и совершить операции по Вашему банковскому счету)
- Соблюдайте меры безопасности при использовании услуги «Мобильный банк». Если не в полной мере владеете информацией об услуге бесконтактного оформления кредита, то лучше отключите ее и при необходимости обратитесь в отделение банка
- При смене абонентского номера Вам необходимо обратиться в отделение банка и отключить услугу «Мобильный банк» от старого привязанного номера к карте и подключить услугу на новый номер телефона



**Мошенничество – п. «Г» часть 3 статьи 158 УК РФ, статья 159 УК РФ**

Вплоть до лишения свободы на **10 лет** со штрафом до **1 000 000 рублей**

**Если вы столкнулись с действиями мошенников, звоните:**

**02** (с мобильного – **102**) либо в ближайший районный отдел полиции