ЗАЩИТА
БАНКОВСКОЙ КАРТЫ

НЕ СООБЩАЙТЕ НИКОМУ

- Информацию, размещенную на вашей банковской платежной карте (на обеих сторонах): номер, дату, код.
- Цифровые или буквенные коды.
- Паспортные данные.

ЕСЛИ ВАМ ПОСТУПИЛ СОМНИТЕЛЬНЫЙ ЗВОНОК

- Немедленно завершите разговор.
- Обратитесь в контакт-центр банка, выпустившего карту.
- Следуйте рекомендациям сотрудника банка.

РЦФГ
Региональный центр финансовой грамотности

8 (343) 221-96-23

Екатеринбург
ул. 8 марта, 62

РЦФГ Региональный центр финансовой грамотности
МВД

ИНФОРМИРУЮТ

ЗАЩИТА БАНКОВСКОЙ КАРТЫ

РЕГИОНАЛЬНЫЙ ЦЕНТР ФИНАНСОВОЙ ГРАМОТНОСТИ И МВД ИНФОРМИРУЮТ

ФИНАНСОВАЯ БЕЗОПАСНОСТЬ

СОВЕТЫ ПО ГРАМОТНОМУ ИСПОЛЬЗОВАНИЮ БАНКОВСКИХ КАРТ

Никогда **не храните PIN-код** рядом с банковской картой.

Не сообщайте никому PIN-код и CVV2-код карты (цифры с обратной стороны карты), а также срок ее действия и персональные данные владельца. Ни один банк не будет спрашивать у вас эти реквизиты. Для зачисления средств на ваш счет достаточно лишь 16-значного номера, указанного на лицевой стороне карты.

Не входите в интернет-банк с **чужих компьютеров** или из публичных незащищенных сетей Wi-Fi.

Не используйте карты с основным своим финансовым капиталом для оплаты покупок в Интернете. Создайте для этих целей виртуальную карту или электронный кошелек (QIWI, Яндекс Деньги и т.д.)

Не переходите по подозрительным ссылкам и не оплачивайте покупки через сомнительные сайты, где не указаны полные реквизиты компании. Проверить, существует ли такая фирма можно на сайте egrul.nalog.ru (введите в поле поиска ОГРН или ИНН компании).

Если вы пользуетесь СМС-банкингом и при этом потеряли/сменили SIM-карту, сообщите об этом банку.

БУДЬТЕ БДИТЕЛЬНЫ!

Мошенники могут имитировать телефонные номера банков. Банки не рассылают сообщений о блокировке карт, а в телефонном разговоре не выспрашивают конфиденциальные сведения и коды, связанные с картами клиентов.

НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ МЕТОДЫ РАБОТЫ ЗЛОУМЫШЛЕННИКОВ

1. Выманивание реквизитов банковских карт с использованием взломанных аккаунтов в социальных сетях.

2. ЛЖЕПОКУПАТЕЛЬ. Под видом покупателя злоумышленник связывается с продавцом, предлагает внести залог перед покупкой товара, а для получения денежного перевода предоставляет ему ссылку на мошенический сайт.

3. ВИШИНГ. Представляясь по телефону сотрудником банка, злоумышленник пытается узнать у держателя карты ее реквизиты, номер паспорта, личный идентификационный номер, логины, пароли, СМС-коды.