

Как не стать жертвой киберпреступника.

ЗАЩИТА БАНКОВСКОЙ КАРТЫ

Наиболее распространенные методы работы злоумышленников



выманивание реквизитов
банковских платежных
карт с
использованием
взломанных аккаунтов
знакомых в
социальных сетях



ЛЖЕПОКУПАТЕЛЬ -

под видом покупателя
злоумышленник связывается с продавцом,
предлагает внести залог перед покупкой товара, а для
получения денежного перевода предоставляет ему
ссылку на мошеннический сайт, визуально похожий на
официальный сайт банка



ВИШИНГ - представляясь по телефону
сотрудником банка, злоумышленник пытается
узнать у держателя карты конфиденциальную
информацию (ее реквизиты, а также номер паспорта,
личный идентификационный номер, логины, пароли,
СМС-коды)



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



Для защиты **денежных**
средств клиентов у банка
есть вся необходимая
информация



Работники банка по телефону
не должны спрашивать ни
реквизиты карты, ни
паспортные данные



Не давайте никому свой
мобильный телефон и
предупредите об этом ваших
близких, особенно детей и
лиц пожилого возраста

Изготовлено в рамках муниципальной программы «Профилактика правонарушений, преступлений и общественной безопасности в Усольском районе» на 2020-2025 годы.