-Код безопасности (CVV2 или CVC2) – комбинация цифр, указанная на оборотной стороне карты, а именно: три крайние правые цифры, указанные после четырех последних цифр номера карты. Проверочный код необходим только для совершения платежей в интернете. При онлайн-оплате он вводится вместе с номером карты, именем держателя карты и сроком окончания действия карты.

-Одноразовый пароль банка для подтверждения оплаты онлайн – комбинация цифр, отправляемых банком в смс-сообщении или push- уведомлении для подтверждения операций с денежными средствами.

Ни в коем случае не сообщайте ПИН-код, код безопасности или одноразовый пароль третьим лицам!

Никто, в том числе сотрудники банка, не вправе требовать от держателя карты сообщить ПИН-код или код безопасности.

Одним из самых распространенных видов интернет-мошенничества является так называемый «Фишинг». Мошенники совершают определенные действия, направленные на получение доступа к денежным средствам на банковской карте потенциальной жертвы, при помощи почтовых рассылок от лица банка, содержащих в себе ссылки на страницы, являющиеся точными копиями официальных сайтов, на которых предлагается ввести данные карты для возможности дальнейшего ее использования.

Еще одним крайне распространенным видом интернет-мошенничества являются фальшивые интернет-магазины. Мошенники берут с покупателя предоплату за товар и не выполняют своих обязательств.

Важно отметить, что популярность сайта в поисковике вовсе не гарантия вашей безопасности. В действительности мошенники активно продвигают свои сайты с использованием вебмаркетинга. И зачастую фальшифки стоят даже выше ссылок на оригинальный сайт и внешне он на первый взгляд ничем не отличается от оригинала. Платежные страницы на таких сайтах только маскируются под оплату товаров и услуг, на самом деле потенциальная жертва переводит деньги на карты мошенников или на номера мобильных телефонов, с которых впоследствии мошенники снимут деньги. Кроме того на поддельных сайтах мошенники собирают реквизиты карт, которые потом используют для несанкционированных операций. После совершения такой оплаты гражданин-покупатель даже может получить подтверждение по почте, но товаров и услуг доставлено и оказано не будет.

Признаки отличия поддельных сайтов от настоящих:

-Внимательно изучите адресную строку. Дизайн может полностью копировать оригинальный сайт, но в адресной строке точно будет что-то не так, хотя бы один символ.

-Сайт новый и о нем нет никакой информации в интернете.

-Тексты на сайте могут содержать ошибки и неработающие ссылки.

-Дизайн страницы ввода одноразового пароля может отличаться от привычного дизайна вашего банка.