**Что такое дистанционное мошенничество?**

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.

Зачастую сайты - "фальшифки" стоят в поисковых системах выше ссылки на оригинальный сайт и внешне ничем не отличаются 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, жертва даже может получить подтверждение по почте, но товаров ни услугдоставлено и оказано не будет.

Как же отличить поддельные сайты от настоящих?

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

Второе – сайт новый и о нем нет никакой информации в интернете.

Третье – тексты на сайте могут содержать ошибки и неработающие ссылки.

Четвертое – дизайн страницы ввода одноразового пароля может отличаться от привычного дизайна вашего банка, а еще название магазина будет написано порски, а не латинскими буквами как обычно в легальных платежных системах.

Пятое – вместо названия магазина на аутентификационной странице символы Р2Р, PEREVODNAKARTU, или CARD2CARD, то есть информация о переводе средств с карты на карту.

Шестое – сумма на аутентификационной странице банка может быть изменена.

Седьмое – после введения корректных данных сайта для одноразового пароля жертве сообщают, что пароль неверный и просят ввести новый пароль на самом деле, чтобы провести новую операцию.

Заметив любой из этих признаков, звоните по телефону, который указан на вашей карте и пользуйтесь только проверенными интернет-площадками.

Прокуратура Тужинского района