О совершении хищений имущества посредством сети Интернет

С каждым годом все больше людей приобщаются к использованию сети Интернет, расширяются возможности приобретения товаров и услуг посредством безналичных расчетов в различных онлайн-магазинах, разрешения различных вопросов, требующих финансовых затрат.

Развитие информационных технологий также сказывается на преступности – наблюдается увеличение совершенных преступных деяний в данной сфере.

Для того чтобы обезопасить себя и своих близких от утраты денежных средств необходимо соблюдать следующие правила:

1) Не сообщать кому-либо код CVV. Данная информация содержится на оборотной стороне любой банковской платежной карты. Состоит из трех цифр и является кодом проверки подлинности карты. Именно эти три цифры открывают доступ к использованию карты при осуществлении покупок.

2) Не хранить ПИН-код вместе с банковской платежной картой. В случае утраты кошелька, в котором хранится карта и записка с ПИН-кодом к ней, либо карта с написанным на ней ПИН-кодом, Вы автоматически предоставляете доступ к своему счету нашедшему со всеми вытекающими последствиями.

3) Не передавать кому-либо личные данные (паспортные), логин, пароль доступа к системе «Интернет-банкинг».

4) Не сообщать кому-либо данные, полученные в СМС-оповещениях от Вашего банка, сеансовые пароли (3D secure code), коды авторизации. Большинство банков предлагают клиентам дополнительные меры безопасности при осуществлении расчетов в сети Интернет. Их раскрытие позволит совершить хищение Ваших средств.

5) Не переходить по ссылкам на интернет-ресурсы, которые получены от неизвестных Вам лиц в интернет-мессенджерах (например Viber, Telegram, Instagram). Данные ссылки нередко направляют пользователей на фишинговые сайты, либо вовсе загружают сторонние вирусные программы, которые получают все данные, имеющиеся на телефоне либо компьютере.

Фишинговый сайт – сайт, в котором имеется возможность ввода реквизитов банковской платежной карты в целях совершения покупок или приобретения услуг. Нередко в таких сайтах используются наименования, способные ввести человека в заблуждение относительно его подлинности (например «название организации.xyz»), либо сообщения о том, что пользователь выиграл лотерею (джекпот) и ему необходимо его сейчас же забрать.

6) Не скачивать приложения, направленные по интернет-почте, интернет-мессенджеру от неизвестных Вам лиц. Данные приложения загружают сторонние вирусные программы, которые получают все данные, имеющиеся на телефоне либо компьютере.

7) Не вступать в переговоры с неизвестными лицами посредством интернет-мессенджеров о Ваших банковских платежных картах. Нередко гражданам напрямую звонят в интернет-мессенджер (например Viber) так называемые «сотрудники банков, правоохранительных органов» и сообщают о попадании Ваших родственников в происшествие, о наличии опасности и взлома их данных к карте, требуют продиктовать данные с карточки, осуществить определенные действия на телефоне. Незамедлительно прервите разговор и не реагируйте на все последующие действия преступников.

8) Проявляйте бдительность при покупке товаров и приобретении услуг по «бросовым» ценам. Очень часто данный метод используется мошенниками при хищении денежных средств у граждан, особенно в совокупности с фишинговыми сайтами.

Помните, только Вы в состоянии обеспечить безопасность своих денежных средств когда используете сеть Интернет!

Заместитель прокурора

Минского района Е.А.Дорожко