Сотрудники полиции призывают граждан к соблюдению мер безопасности при проведении платежей через интернет

Как избежать встречи с мошенниками во всемирной паутине? Специалисты помогут разобраться в способах безопасных покупок в сети интернет.

В безопасности интернет-операций заинтересованы не только держатели карт, но и банки, интернет-магазины и платежные системы, которые разрабатывают все новые, более совершенные и одновременно дорогостоящие средства безопасности онлайн-платежей и защиты от мошенников. Все участники транзакции рискуют своими деньгами, а магазины, банки и системы — еще и своей репутацией.

Какие существуют современные меры безопасности интернет-платежей, кто и за что отвечает непосредственно во время транзакции и как избежать мошенников во всемирной паутине?

В каждом процессе платежа принимает участие несколько сторон. Одна сторона — это держатель карты, физическое лицо, совершающее операцию. Другой стороной является интернет-магазин или любая другая торговая площадка, которая предлагает товары или услугу. Между ними стоит банк, который выдает карту, на счету у которого находятся деньги и который производит данную финансовую операцию. Последними, но не менее важными участниками операции выступают международные платежные системы и сервис-провайдеры – они осуществляют процессинг операции.

Когда вы совершаете покупку в интернет-магазине и нажимаете кнопку «Оплатить», вы переходите на страницу платежной формы для заполнения необходимых данных. Далее платежная система (сервис-провайдер) передает все ваши данные в банк, который обслуживает этот интернет-магазин. Банк проверяет информацию о вас, о карте, наличии свободных средств на ней, иногда запрашивая авторизацию покупателя по технологии 3-D Secure. После этого он разрешает (или не разрешает) провести операцию, передает данные платежной системе, платежная система — в магазин, а покупателю приходит уведомление, что операция совершена.

А кто отвечает за безопасность?

За безопасность интернет-операции отвечают все, кто принимает в ней участие. Ответственные банки, интернет-магазины, платежные системы постоянно совершенствуются, изобретая все новые способы обезопасить себя и своего клиента от возможной угрозы.

На сегодняшний день существуют протоколы и правила, которые позволяют безопасно передавать зашифрованную информацию от пользователя к серверу; стандарты защиты информации, разработанные международными платежными системами, защищающие данные банковских карт; стандарты проверки личности держателя карты в реальном времени, которую проводит банк при помощи SMS и т.д.

То есть другие участники операции принимают повышенные меры безопасности, но и сам пользователь не должен их нарушать, обходить или невнимательно к ним относиться. Иначе все попытки вас обезопасить будут абсолютно бесполезны.

Ответственно подходить к совершению платежей через интернет, выработать у себя минимальные навыки для обеспечения онлайн-безопасности — это главные элементы современной финансовой грамотности, соблюдать которую следует всем интернет-пользователям.

Оплата банковской картой через интернет связана с серьезным риском потери денег, обманывать вас могут по-разному, например:

1. Один из самых распространенных способов обмана - «фишинг» (по-русски, рыбалка). Суть фишинга заключается в том, чтобы создать сайт интернет-магазина с дешёвыми и необходимыми товарами, на который пользователь «клюёт», то есть покупает товары. При оплате покупатель вводит данные карты и теряет все деньги.

2. Второй способ обмана связан с тем, что при регистрации заказа покупатель оставляет контакты. Далее мошенники связываются с ним и под различными предлогами, представившись сотрудником банка или сотового оператора, просит предоставить конфиденциальную информацию: пароль, пин-код или код CVV2/CVC2 банковской

карты. Используя полученные данные, мошенники быстро выводят с карты деньги, оплачивая покупки или переводя средства на чужие счета.

3. Еще один способ использования чужой банковской карты - заражение компьютеров вирусными программами. Эти программы нацелены на хищение информации карты пользователя при её введении (номер, срок действия и т.д.). Программа сохраняет и пересылает эту информацию мошенникам. А далее можно прощаться с деньгами.

Пресс-служба МВД по Республике Крым