УДК 004.42

БЕЗОПАСНОСТЬ ПЛАТЕЖЕЙ В ИНТЕРНЕТЕ

Пунтус А.П., студент гр. ПИб-172, IV курс.
Научный руководитель: Корниенко И.Л., старший преподаватель.
Кузбасский государственный технический университет
имени Т. Ф. Горбачева
г. Кемерово

В настоящее время электронные денежные переводы и онлайн-платежи самый популярный способ оплаты товаров и услуг. Кассы у большинства компаний перестают функционировать и люди переходят на платежи в интернете, как показывают многие примеры компаний и статистика, собранная по переходу на онлайн-платежи, то для большинства потребителей товаров и услуг оплата через интернет не вызывает никаких трудностей.

Самая большая проблема, назревшая после массового перехода на онлайн-платежи – мошенничество в интернете. Данная деятельность является противозаконной и уголовно наказуемой, так как количество таких преступлений в настоящее время растет с геометрической прогрессией, то приходится расширять отделы по борьбе с киберпреступностью для безопасности пользователей 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.

Люди должны быть осторожны при оплате товаров и услуг и соблюдать, некоторые меры предосторожности, как и в любой операции с деньгами. На сегодняшний момент существует ряд протоколов и правил, о которых вам как непосредственным участникам любой транзакции необходимо знать и помнить каждый раз, когда вы совершаете онлайн-платеж.

Основные советы и правила по онлайн-платежам:

1. Обязательно совершать оплату только посредством использования защищенных соединений, то есть адрес веб-сайта должен начинать с префикса HTTPS:// (рис.1). В данном случае интернет-магазин или платежная система заслуживает большего доверия со стороны пользователя.
2. Всегда набирать точный адрес ресурса, проверять название сайта, доменное имя, визуальное составляющее сайта может быть идентичным с оригинальным сайтом, обязательно стоит обращать на эти детали внимание.

3. Технология 3-D Secure - проверка держателя карты в реальном времени, которую включает банк-эмитент. Банк в качестве подтверждения высылает секретный код по СМС покупателю, после введения кода вы подтверждаете свою личность, и банк разрешает выполнить денежную операцию
4. При оплате банковской картой через интернет никогда не используется ПИН-код карты, если сайт запрашивает ПИН-код, то это уже веский повод усомниться в безопасности сайта.
5. Не желательно сохранять данные карты в кэше браузера, если вдруг вы сохранили данные, то лучше всего почистить кэш вашего браузера в настройках.
6. Никому не отправляйте фотографии с вашей картой и данными обратной стороны – CVV-код

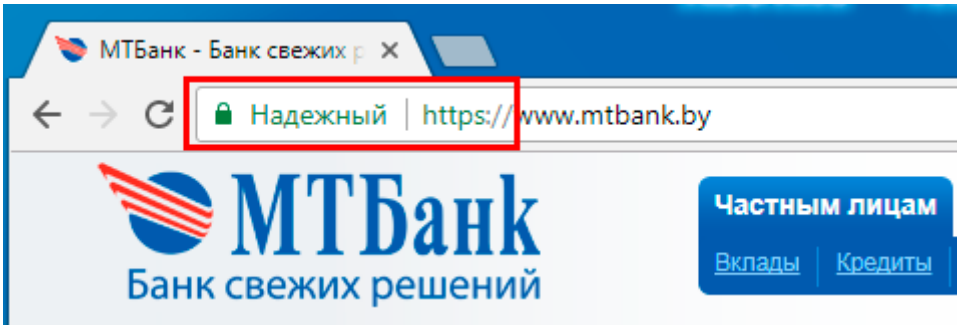

Рисунок 1 - Надежный сайт

Применяя данные правила, можно максимально обезопасить себя от угрозы завладения вашими средствами.

Если вы думаете, что с вашей карты все-таки незаконно списали денежные средства, то необходимо предпринять следующие действия:

1. Если у вас есть другой счет, то незамедлительно переведите оставшиеся денежные средства на этот счет, для этого можете воспользоваться онлайн-сервисами банка.
2. Заблокировать свою банковскую карту, позвонив на линию поддержки банка, либо заблокировав карту в онлайн-сервисе банка или прийти в отделение банка с паспортом.
3. Обратиться в службу поддержки компании, в которой у вас списали деньги, возможно это поможет, часто при подключении автоплатежа, пользователь забывает об этом и у него автоматически списывается сумма денег, после обращения в поддержку в течение трех рабочих дней деньги поступают обратно на карту.
4. Получить выписку из банка с совершенными транзакциями и обратиться в полицию, написав заявление, если вы уверены, что это сделали злоумышленники.

Участники электронной торговли должны быть уверены в том, что при передаче от отправителя к адресату содержание сообщения останется неизменным. Сообщения, отправляемые владельцами карточек коммерсантам, содержат информацию о заказах, персональные данные и платежные инструкции. Если в процессе передачи изменится хотя бы один из компонентов, то данная транзакция не будет обработана надлежащим образом. Поэтому во избежание ошибок протокол SET должен обеспечить средства, гарантирующие сохранность и неизменность отправляемых сообщений. Одним из таких средств является использование цифровых подписей.

Список литературы:

1. Интернет ресурс Билайн [Электронный ресурс] – Режим доступа: https://spb.beeline.ru/customers/pomosh/bezopasnost/ugrozy-v-internete/virus-trojan-winlock/, свободный (дата обращения 28.03.2021)
2. Интернет ресурс Forbes [Электронный ресурс] – Режим доступа: https://www.forbes.ru/finansy-i-investicii/346943-bezopasnost-v-internete-kak-zashchitit-svoi-platezhi, свободный (дата обращения 28.03.2021)