**«Защита банковских карт при дистанционном способе продажи товаров»**

В последнее время мы все чаще стали совершать покупки в интернет-магазинах, производить другие всевозможные расчеты в сети Интернет, и банковская карта является одним из наиболее удобных и доступных способов осуществить такой платеж. Вводя данные своей банковской карты, каждый покупатель подвергается потенциальной опасности.

Одним из самых распространенных способов обмана является «фишинг» (в переводе, «рыбалка»). Его суть заключается в том, что мошенники создают 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.

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, просят 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.

Еще один способ использования чужой банковской карты – заражение электронных устройств 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.

Обезопасить себя полностью невозможно. Но соблюдать элементарные правила при использовании банковской карты в интернете необходимо:

1.    Подключите интернет-банк и СМС-оповещение, это позволит вам отслеживать операции в режиме реального времени.

2.    Не сообщайте никогда и никому платежные реквизиты своей банковской карты, не пересылайте реквизиты электронной почтой. Помните, при оформлении интернет-платежа у вас не должны запрашивать пин-код.

3.    Не используйте подозрительные сайты.

4.    Необходимо установить и периодически обновлять антивирус. Также рекомендуется регулярно обновлять операционную систему.

5.    Используйте 3-D Secure — авторизацию платежа по СМС (проверка личности держателя карты в реальном времени), при этом обращайте внимание на назначение платежа, которое приходит в СМС от банка вместе с проверочным кодом.

6.    Постарайтесь не использовать для покупок чужие компьютеры, не будучи уверенными в их безопасности, минимизируйте пользование wi-fi сетями общего доступа.

7.    Откройте отдельную карту для интернет-платежей и не храните на ней значительных денежных средств.

8.    Установите лимит расходования средств по своей карте, это особенно необходимо, если на карте хранится значительная сумма средств.

Если Вы получили смс-оповещение о том, что по вашей карте проведен платеж, которого Вы явно не совершали, немедленно позвоните в банк и заблокируйте карту, потом напишите заявление на мошенническую или ошибочную транзакцию.

Будьте осторожны при оплате банковской картой онлайн! Удачных покупок!

Для получения консультации по вопросам защиты прав потребителей можно обратиться по телефонам:

**Единого Консультационного Центра Роспотребнадзора** 8 800 555 49 43 (круглосуточно, звонок бесплатный);

**Консультационного центра для потребителей (в рабочее время):**

* 8 (3012) 37-90-29, 8 (9025) 62 34 17, E-mail: zpp\_cgebur@mail.ru;

**Консультационного пункта для потребителей (в рабочее время):**

* 8 (30145) 43726, 8 (9025) 62-31-99 (в рабочее время), электронная почта selenga\_cge@mail.ru или по адресу: Республика Бурятия, г. Гусиноозерск, ул. Школьная, д. 26