Способы защиты от мошеннических действий с использованием информационно-телекоммуникационных технологий.

19.06.2023

Федеральным законом от 23.04.2018 № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» усилена уголовная ответственность за хищение денежных средств с банковского счета или электронных денежных средств, в том числе с использованием электронных средств платежа, путем дополнения части 3 статьи 158 УК РФ пунктом «г» - кража, совершенная с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159.3 УК РФ).

Результаты статистических данных, свидетельствуют о возросшем числе подобных преступлений, которым, как показывает практика способствует недостаточная осведомленность граждан о необходимых мерах по предупреждению хищений денежных средств при использовании банковских карт.

Для предотвращения противоправных действий по снятию денежных средств с банковского счета необходимо исходить из следующего.

Сотрудники банка никогда по телефону или в электронном письме не запрашивают:

· персональные сведения (серия и номер паспорта, адрес регистрации, имя и фамилия владельца карты);

· реквизиты и срок действия карты;

· пароли или коды из СМС-сообщений для подтверждения финансовых операций или их отмены;

· логин, ПИН-код и CVV-код банковских карт.

Сотрудники банка также не предлагают:

· установить программы удаленного доступа (или сторонние приложения) на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки (например, удаление вирусов с устройства);

· перейти по ссылке из СМС-сообщения;

· включить переадресацию на телефоне клиента для совершения в дальнейшем звонка от его имени в банк;

· под их руководством перевести для сохранности денежных средств на «защищенный счет»;

· зайти в онлайн-кабинет по ссылке из СМС-сообщений или электронного письма.

Банк может инициировать общение с клиентом только для консультаций по продуктам и услугам кредитно-финансового учреждения, и звонки совершаются с номеров, указанных на оборотной стороне карты, на сайте банка или в оригинальных банковских документах, другие номера не имеют никакого отношения к банку.

Стоит учитывать, что держатель карты обязан самостоятельно обеспечить конфиденциальность реквизитов и в этой связи избегать:

· подключения к общедоступным сетям Wi-Fi;

· использование ПИН-кода или CVV-кода при заказе товаров и услуг через сеть «Интернет», а также по телефону (факсу);

· сообщений кодов третьим лицам (в противном случае любые операции, совершенные с использованием ПИН-кода или CVV-кода, считаются выполненными самим держателем карты и нем могут быть опротестованы);

Также при использовании банкоматов отдавайте предпочтение тем, которые установлены в защищенных местах (в госучреждениях, офисах банков, крупных торговых центрах).

При использовании мобильного телефона соблюдайте следующие правила:

· при установке приложений обращайте внимание на полномочия, которые они запрашивают, будьте особенно осторожны, если приложение просит права на чтение адресной книги, отправку СМС-сообщений и доступ к сети «Интернет»;

· отключите в настройках возможность использования голосового управления при заблокированном экране.

При оплате услуг картой в сети «Интернет» требуется всегда учитывать высокую вероятность перехода на поддельный сайт, созданный мошенниками для компрометации клиентских данных, включая платежные карточные

данные.

Обращаем особое внимание на необходимость использования только проверенных сайтов, внимательного чтения текстов СМС-сообщений с кодами подтверждений, проверки реквизитов операций.

При возникновении малейших подозрений насчет предпринимаемых попыток совершения мошеннических действий следует незамедлительно уведомлять об этом банк.

Соблюдение указанных мер по предупреждению мошеннических действий с использованием информационно-телекоммуникационных технологий помогут Вам обезопасить себя от противоправных действий.

Межрайонный прокурор Д.И. Ткачев

Адрес страницы: http://ubutovo.mos.ru/events/detail/11658284.html

---