Рекомендации безопасного поведения при использовании сети «Интернет» и сотовой связи. Киберпреступность

Следственным управлением Следственного комитета РФ по Приморскому краю совместно с УМВД России по Приморскому краю проводится постоянная целенаправленная работа по противодействию киберпреступности, совершаемой в банковской деятельности, в том числе в отношении граждан, производящих платежи посредством использования сети Интернет.

Реальность такова, что сегодня техническими возможностями компьютеров, их программным обеспечением, сетью Интернет, сотовой связью стремятся воспользоваться криминальные элементы, количество которых с каждым днем возрастает, а расширяющаяся глобализация информационных процессов и пространства, способствует созданию новых способов, средств и объектов преступных киберпосягательств. Злоумышленники все чаще стали использовать новые электронные способы и средства, например мобильные системы связи, возможности интернет-банкинга.

Важную роль в вопросе противодействия незаконной деятельности киберпреступников является предусмотрительность и соблюдение элементарных правил производства электронных платежей самими гражданами, некоторыми из них могут быть:

- К своей основной карте в вашем банке выпустите дополнительную, которой будете расплачиваться в интернете. Туда легко можно будет переводить небольшие суммы денег, и в случае компрометации данных достаточно просто заблокировать ее.

- Регулярно проверяйте состояние своих банковских счетов, чтобы убедиться в отсутствии «лишних» и странных операций.

- Храните номер карточки и ПИН–коды в тайне. Запомните и сотрите/заклейте CVC-код.

- Используйте виртуальные карты, которые сейчас предоставляют платежные системы.

- Поставьте лимит на сумму списаний или перевода в личном кабинете банка.

- Будьте осмотрительны в отношении писем со вложенными картинками, поскольку файлы могут содержать вирусы. Открывайте вложения только от известных вам отправителей. И всегда проверяйте вложения на наличие вирусов, если это возможно.

- Не переходите необдуманно по ссылкам, содержащимся в спам-рассылках. Удостоверьтесь в правильности ссылки, прежде чем переходить по ней из электронного письма.

- Не заполняйте полученные по электронной почте формы и анкеты. Личные данные безопасно вводить только на защищенных сайтах.

- Проверяйте запросы персональных данных из каких-либо деловых и финансовых структур. Лучше обратиться в эти структуры по контактам, указанным на официальном сайте, а не в электронном письме.

- Насторожитесь, если кроме вас в электронном сообщении указаны другие адресаты. Крайне маловероятно, чтобы при общении с клиентом по поводу личных учетных данных банк ставил кого-то в копию.

- Насторожитесь, если от вас требуют немедленных действий или представляется чрезвычайная ситуация. Это тоже может быть мошенничеством. Преступники вызывают у вас ощущение тревоги, чтобы заставить вас действовать быстро и неосмотрительно.

Помните!!! Бдительность и осмотрительность помогут защитить Вас от противоправных посягательств киберпреступников.

31 Августа 2017

Адрес страницы: https://primorsky.sledcom.ru/news/item/1159836