



О профилактике киберпреступлений



В связи с динамичным и масштабным ростом числа киберугроз и киберпреступлений, причиняемым ими ущербом государственным структурам, юридическим и физическим лицам, такие противоправные деяния представляют серьезнейшую проблему для общества, а борьба с ними является актуальной и стратегически важной задачей для правоохранительных органов. Разветвленные элементы инфраструктуры сети Интернет, мобильных сетей связи (телекоммуникации) являются наиболее востребованными средствами совершения преступлений, как для хакеров, так и для различного рода мошенников, террористов, торговцев людьми, порнографией, наркотиками, а также в целях совершения сексуального насилия и развратных действий в отношении несовершеннолетних (малолетних).

Следственным управлением Следственного комитета Российской Федерации по Курганской области совместно с другими правоохранительными органами Курганской области проводится постоянная целенаправленная работа по противодействию киберпреступности, в том числе совершаемой в банковской сфере в отношении граждан, производящих платежи посредством использования сети Интернет.



Официальный сайт

Следственное управление Следственного комитета Российской Федерации по Курганской области

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



Официальный сайт

Следственное управление
Следственного комитета Российской Федерации
по Курганской области

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.

20 Сентября 2017

Адрес страницы: <https://kurgan.sledcom.ru/news/item/1165494>