Памятка

о мерах безопасности в сфере информационной безопасности

Киберпреступления – преступления, связанные с использованием компьютерной техники (преступления против информационной безопасности, хищения путем использования средств компьютерной техники, шантаж, вымогательство, изготовление и распространение порнографических материалов и т.д.).

Как обезопасить себя в интернете:

1. Придумайте сложные пароли доступа

Пароль, который состоит из букв разного регистра (строчные и заглавные), разных языков, цифр и пр., сложнее взломать. Не лишним будет также устанавливать разные пароли для разных аккаунтов.

2. Не заходите на неизвестные или малознакомые сайты.

3. Не открывайте письма, которые пришли с незнакомого или подозрительного e-mail. Сразу отправляйте такие письма в спам. Если так вышло, что письмо открыли, не переходите по ссылкам из него, не открывайте прикрепленные документы. Если же подозрительное письмо пришло от вашего знакомого - обязательно свяжитесь с ним для уточнения информации.

4. Перед скачиванием файлов, программ убедитесь, что они не вредоносны.

5. Регулярно обновляйте антивирусную программу.

6. Критически относитесь к предложениям совершить предоплату какого-либо товара (услуги) путем перечисления денег на виртуальный кошелек или на карту частного лица. Перед совершением покупки стоит проверить информацию о продавце, почитать отзывы на сайте. Если на сайте не указан как минимум адрес продавца и контактный телефон - это повод задуматься, можно ли доверять такому продавцу.

7. Никогда, никому и ни при каких обстоятельствах не сообщать реквизиты своих банковских счетов и банковских карт, в том числе лицам, представившимся сотрудниками банка или правоохранительных органов, при отсутствии возможности достоверно убедиться, что эти люди те, за кого себя выдают.

В случае поступления звонка «от сотрудника банка» необходимо уточнить его фамилию, номер телефона, после чего завершить разговор и самим позвонить в банк.

Необходимо принимать во внимание, что реальному сотруднику банка известна следующая информация: фамилия держателя карты, паспортные данные, какие карты оформлены, остаток на счете.

Не следует сообщать в телефонных разговорах (даже сотруднику банка), а также посредством общения в социальных сетях: полный номер карточки, срок ее действия, код CVC/CVV (находящиеся на обратной стороне карты), логин и пароль к интернет-банкингу, паспортные данные,

кодовое слово (цифровой код) из SMS-сообщений.

В случае если «сотрудник банка» в разговоре сообщает, что с карточкой происходят несанкционированные транзакции, необходимо отвечать, что вы придете в банк лично, – все подобные вопросы нужно решать в отделении банка, а не по телефону.

Обратите внимание!

Сотрудники банковских учреждений никогда не используют для связи с клиентом мессенджеры (Viber, Telegram, WhatsApp).

8. Не следует хранить банковские карты, их фотографии и реквизиты в местах, которые могут быть доступны посторонним лицам; это же относится к фотографиям и иным видам информации конфиденциального характера.

Стопроцентной защиты от злоумышленников на просторах Интернета нет. Однако, пользуясь вышеперечисленными рекомендациями, вмешательство извне в ваши данные можно свести к минимуму.

Если вы все-таки стали жертвой киберпреступника

В первую очередь смените пароли доступа к взломанной странице (аккаунту). Переустановите антивирусную программу. Если есть подозрение, что мошенники получили доступ к вашим банковским карточкам, немедленно свяжитесь с обслуживающим банком для их блокировки.

Как можно быстрее напишите заявление о совершенном в отношении вас правонарушении. Заявление можно подать в один из органов уголовного преследования - в орган дознания (например, милицию), следователю или прокурору (ч. 1 ст. 172, п. 22 ст. 6 УПК). Вместе с заявлением следует сообщить максимум имеющейся информации. Например:

1) сайт, на котором произошли мошеннические действия;

2) переписка с нарушителем;

3) номер счета или электронного кошелька, на который были перечислены деньги;

4) адрес электронной почты злоумышленника, номер телефона и др.