Противодействие IT-мошенникам

IT-преступления, или киберпреступления - это противоправные действия, совершаемые с использованием информационных технологий. Они могут быть направлены против отдельных лиц, организаций или даже государств.

Основные виды мошенничества:

1. Взлом аккаунта

Если вы получаете сообщение с просьбой об одолжении денег или сборе средств для благотворительности, то убедитесь, что это реальный человек, спросите у него что-то, что знает только он, либо просто игнорируйте такие сообщения.

2. Кликбейт — захватывающий заголовок, который прерывается на самом интересном месте, и вас отсылают читать продолжение в источнике. В большинстве случаев кликбейт относительно безопасен — скорее всего вас просто перенаправит на страницу с рекламными баннерами. Однако такие новости могут быть опасными, потому что туда можно вложить ссылку с опасным контентом.

3. Выигрыши

Баннер, картинка или плашка от браузера, где заявляется, что ваш IP-адрес был выбран в качестве победителя.

4. Платные опросы

Если вы видите такие предложения, то обратите внимание на предлагаемую сумму, если вам предлагают заработать 25 тысяч рублей за опрос — это обман.

5. Спам

Такие письма почти гарантированно содержат в себе вирус. Вы получаете спам-письмо, переходите по ссылке и дальше идет цепная реакция — одна ссылка перенаправляет на другую (а таких перенаправлений может быть сколько угодно много) и рано или поздно вы получите вирус или требование ввести личные данные.

6. Документы и файлы

В документах могут содержаться макросы. Они потенциально очень опасны. Поэтому если вы не пользуетесь макросами, то вам лучше отключить их исполнение в настройках офисных программ.

Важно помнить, что IT-преступность – это серьезная проблема, которая требует внимания и принятия мер для защиты себя и своих данных.

КАК ОБЕЗОПАСИТЬ СЕБЯ ОТ МОШЕННИКОВ:

1. Установить на телефон (компьютер) лицензированное антивирусное программное обеспечение.

2. Не устанавливаете и не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников: скачанные с неизвестных сайтов, присланные по электронной почте (подозрительные файлы лучше сразу удалять).

3. Используйте пароли, не связанные с Вашими персональными данными.

4. Не сообщайте данные карты, пароли и другую персональную информацию.

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

6. По всем возникающим вопросам обращаться в банк, выдавший карту.

7. Не выполнять никаких срочных запросов к действию, в том числе по установке каких бы то ни было приложений.

8. Не перезванивать по номерам, и не переходить ни по каким ссылкам, которые приходят на e-mail или по SMS.