Защитим себя от киберпреступности

Киберпреступность - это преступления, совершенные с помощью сети Интернет. За последние годы этот вид преступлений становиться весьма распространенным, так как с каждым годом по всему миру значительно повышается количество пользователей Интернета.

Основные виды компьютерных преступлений:

1. Запрещенный доступ к информации, хранящейся в компьютере.

Несанкционированный доступ часто осуществляется, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации, оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных.

2. Ввод в программное обеспечение «логических бомб», которые срабатывают при выполнении определённых условий и частично или полностью выводят из строя компьютерную систему.

3. Разработка и распространение компьютерных вирусов.

Компьютерные вирусы - «сотри все данные этой программы, перейди в следующую и сделай тоже самое» обладают свойствами переходить через коммуникационные сети из одной системы в другую, распространяясь как вирусное заболевание. Обнаруживается вирус не сразу: первое время компьютер «вынашивает инфекцию», поскольку для маскировки вирус нередко используется в комбинации с «логической бомбой» или «временной бомбой». Вирус наблюдает за всей обрабатываемой информацией и может перемещаться, используя пересылку этой информации.

Некоторые советы по предупреждению подобных киберпреступлений:

- Не загружайте файлы из непроверенных источников

- Не переходите по ссылкам, содержащимся в электронных письмах отправителей, которых вы не знаете

- Не сообщайте никому свои пароли и личные данные

Обеспечение защиты от киберпреступлений может занять довольно продолжительное время, но всегда того стоит. Соблюдение таких правил безопасной работы в Интернете, как воздержание от загрузок из неизвестных источников и посещения сайтов с низкой репутацией - это здравый смысл в рамках предотвращения киберпреступлений. Внимательное и бережное отношение к своим учетным и персональным данным может также существенно поспособствовать защите от злоумышленников.

Кроме того, постоянно появляются новые способы «бытовых» преступлений. Одно из разновидностей киберпреступлений - это мошенничество.

Например:

Пользователь получает по электронной почте сообщение (якобы от банка или организации, где он планирует что-то заказать и купить), в котором автор письма просит уточнить Ваши банковские реквизиты. Получатель письма легкомысленно отвечает, в результате чего с его счетов списываются денежные средства. Помимо таких преступлений существуют ещё предложения сделать вклад, за который Вы будете получать проценты. Часто организовываются какие-то подложные интернет-аукционы, в которых предлагается принять Вам участие, не бесплатно конечно. Также можно что-то купить, но так и не получить товара. И это, конечно же, далеко не все.

Чтобы защитить себя в таких случаях необходимо:

Не доверять слишком заманчивым предложениям и проверить автора письма, его Интернет-сайт и координаты, а именно:

- Номер телефона, который указан на сайте;

- Адрес организации;

- Нюансы оплаты;

- Гарантии выполнения обещаний.

Также, не доверяйте слишком заманчивым предложениям. Такие фразы, как «бесплатно», «почти даром», «подарок», «большие скидки». Мошенники всегда используют эти фразы и хорошо понимают человеческую сущность. Как правило, обещается большая зарплата за минимум труда, большие деньги за небольшое вложение, заем даже если у Вас плохая платежеспособность и так далее.

11 Февраля 2019

Адрес страницы: https://oren.sledcom.ru/news/item/1298683