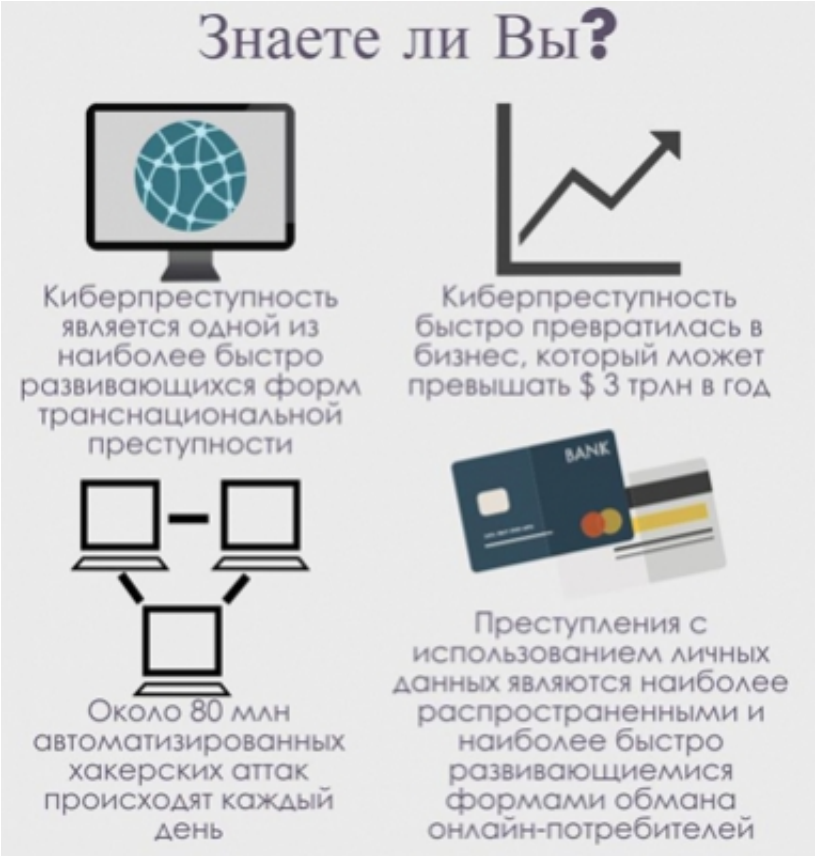
ПРОФИЛАКТИКА КИБЕРПРЕСТУПЛЕНИЙ !



Киберпреступление — это общее название для всех типов криминальной активности, совершаемой с использованием вычислительных машин и/или Интернета. Киберпреступление может совершаться с помощью различных методов и инструментов, например, фишинг, вирусы, шпионское ПО, программы-вымогатели и социальная инженерия — чаще всего с целью кражи личных данных или финансовых средств.

Киберпреступность на сегодняшний день достигла беспрецедентного размаха, чему чрезвычайно поспособствовала всеобщая дигитализация и повсеместное подключение к Интернету с помощью ноутбуков, смартфонов и планшетов, и по праву считается одной из самых прибыльных статей криминального бизнеса в целом. Существует бесконечное количество видов киберпреступлений, которые можно разделить до двух категорий: одноразовые, например, установка на компьютер вируса, похищающего личные данные; и систематические преступления, например, кибербуллинг, вымогательство, распространение

детской порнографии или организация террористических атак.

Киберпреступление, как и любое иное преступление, является плодом труда одного или нескольких злоумышленников, в данном случае с обширными знаниями в области Интернета и цифровых технологий, используемыми для достижения корыстных целей. Киберпреступники используют целый арсенал узкоспециальных знаний и навыков в целях получения несанкционированного доступа к банковским счетам, совершения краж личности, вымогательства финансовых средств, мошенничества, преследования и запугивания или использования зараженного компьютера в разветвленной сети ботнетов с целью совершения DDoS-атак на крупные организации.

Признаки киберпреступления зависят от рода совершенного преступления. Вредоносное ПО, скрыто установленное на компьютер, может замедлять скорость его работы и служить причиной отображения большого количества сообщений об ошибках. Фишинговые атаки подразумевают получение пользователем эл. писем от неизвестных отправителей, пытающихся выманить у него пароли или личные данные. Кейлоггеры тоже обладают характерными признаками, к которым относятся появление странных иконок, дублирование введенных пользователем сообщений и т. п. С другой стороны, пользователь почти не имеет шансов распознать принадлежность своего компьютера к ботнету.

Решение киберпреступлений входит в компетенцию правоохранительных органов и коммерческих организаций по обеспечению информационной безопасности. Рядовые пользователи также могут существенно поспособствовать пресечению роста киберпреступности, заблокировав основной метод распространения киберпреступлений: вредоносное ПО. Избавившись от вирусов, шпионского ПО и программ-вымогателей с помощью современного и эффективного антивируса вы не только защитите компьютер от вредоносного ПО, но пресечете попытки киберпреступников получать деньги противозаконно — что является их основной мотивацией.

Некоторые советы по предупреждению киберпреступлений:

- не загружайте файлы из непроверенных источников;
- не переходите по ссылкам, содержащимся в эл. 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. Однако наиболее эффективным методом защиты по-прежнему остается использование современного и качественного антивирусного

решения.

20 Сентября 2017

Адрес страницы: https://orel.sledcom.ru/news/item/1165703