ПРОФИЛАКТИКА КИБЕРПРЕСТУПЛЕНИЙ

Киберпреступления — это преступления, совершаемые с использованием современных информационно-коммуникационных технологий, т.е. с использованием компьютерной техники и/или Интернета в информационном (виртуальном) пространстве, в котором находятся сведения о лицах, предметах, фактах, событиях, явлениях, находящиеся в движении по локальным и глобальным компьютерным сетям, либо сведения, хранящиеся в памяти любого физического или виртуального устройства, или другого носителя, предназначенного для их хранения, обработки и передачи.

Киберпреступление может совершаться с помощью различных методов и инструментов, например, фишинг – получение доступа к конфиденциальным данным пользователя (логинам и паролям), с помощью вирусов, шпионских программ, программ-вымогателей и другой социальной инженерии — чаще всего с целью кражи личных данных или финансовых средств.

Преступления в данной сфере в настоящее время достигли беспрецедентного размаха, чему чрезвычайно поспособствовало 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 на две категорий: одноразовые, например, установка на компьютер вируса, похищающего личные данные; и систематические преступления, например, кибербуллинг (интернет-травля), т.е. намеренные оскорбления, угрозы и сообщение другим компрометирующих данных, вымогательство, распространение детской порнографии, размещение статей экстремистского толка 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 с целью совершения атак на крупные организации.

Признаки киберпреступления зависят от рода совершенного преступления. Вредоносное программное обеспечение, скрыто установленное на компьютер, может замедлять скорость его работы и служить причиной отображения большого количества сообщений об ошибках. Фишинговые атаки подразумевают получение пользователем электронных писем от неизвестных отправителей, пытающихся выманить у него пароли или личные данные. Программы, целью которых является перехват набранных на клавиатуре символов (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 программе, скрытно установленной злоумышленниками для выполнения действий с использованием ресурсов зараженного компьютера.

Противодействие с киберпреступлениями входит в обязанности полиции, федеральных органов и отделов по борьбе с киберпреступностью и коммерческих организаций по обеспечению информационной безопасности.

Рядовые пользователи также могут существенно поспособствовать пресечению роста киберпреступности, заблокировав основной метод распространения киберпреступлений: вредоносное программное обеспечение.

Избавившись от вирусов, шпионского программного обеспечения и программ-вымогателей с помощью современного и эффективного антивируса Вы не только защитите свой компьютер от вредоносной программы, но пресечете попытки злоумышленников получать выгоду, в том числе Ваши финансовые средства противозаконно — что является их основной мотивацией.

Советы по предупреждению киберпреступлений:

- используйте лицензионное программное обеспечение для защиты от заражения компьютера или мобильного устройства при установке различных программ;
- установите антивирусную программу не только на персональный компьютер, но и на смартфон, планшет и другую технику;
- не загружайте файлы из непроверенных источников;
- не переходите по ссылкам, содержащимся в спаме и других подозрительных электронных письмах отправителей, которых вы не знаете;
- не сообщайте никому свои пароли и личные данные;
- воздержитесь от покупок на малоизвестных и подозрительных интернет-сайтах и у лиц, осуществляющих продажу товаров или услуг в социальных сетях, особенно при необходимости внесения полной предоплаты за товар или услуги;
- используйте сложные пароли, состоящие из комбинаций цифр и букв или иных символов;
- воздержитесь от паролей – дат рождения, имен, фамилий, то есть тех, которые легко вычислить либо подобрать.

Обеспечение защиты от киберпреступлений может занять довольно продолжительное время и некоторых усилий по изучению различных правил поведения в киберпространстве, 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 поспособствовать защите от злоумышленников. Однако наиболее эффективным методом защиты по-прежнему остается использование современного и качественного антивирусного решения.

27 Сентября 2017

Адрес страницы: https://adygheya.sledcom.ru/news/item/1167434