Правила информационной безопасности

В современном мире противодействие киберпреступности является одной из наиболее актуальных и сложных криминологических проблем. Высокая латентность, рост числа киберпреступников, совершенствование информационных технологий, создающие новые возможности совершения этих преступлений, необходимость иных подходов противодействия преступлениям, совершаемым в виртуальном пространстве, создают угрозы для глобальных информационных сетей и общества в целом.

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.

Преступления в данной сфере в настоящее время достигли беспрецедентного размаха, чему чрезвычайно поспособствовало повсеместное подключение к Интернету с помощью ноутбуков, смартфонов и планшетов. Пожалуй, главной причиной роста компьютерной преступности становятся ее криминогенные факторы, возникшие в ходе совершенствования сети Интернет. С помощью сети «Интернет» киберпреступники могут совершать преступление анонимно, скрывать свою истинную личность. Ее трансграничный характер не ограничивает преступников территориальным пространством и позволяет уходить от уголовной ответственности.

Наиболее часто киберпреступления являются финансово-ориентированными и осуществляются посредством следующие типов атак.

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. В подобных схемах излюбленным средством злоумышленников является электронная почта. Суть метода заключается в принуждении получателя письма к переходу по ссылке от имени легитимной организации (банка, налоговой службы, популярного интернет магазина и т. д.). В подобных случаях целью, зачастую, является овладение банковскими данными.

Кибервымогательство. Как правило, вначале у пользователя или компании, после загрузки вредоносного кода шифруются файлы, а затем поступает предложение о восстановлении в обмен на денежное вознаграждение (обычно в виде биткоинов, так как криптовалюту отследить сложно).

Финансовое мошенничество. Большинство изощренных схем финансового мошенничества связано со взломом компьютерных систем операторов розничной торговли с целью получения банковских данных о покупателях (так называемые целевые атаки) или последующими манипуляциями полученной информацией. 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.

Советы по предупреждению киберпреступлений:

- используйте лицензионное программное обеспечение для защиты от заражения компьютера или мобильного устройства при установке различных программ;

- не загружайте файлы из непроверенных источников;

- не переходите по ссылкам, содержащимся в спаме и других подозрительных электронных письмах отправителей, которых вы не знаете;

- 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.

- не сообщайте никому свои пароли и личные данные, 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.

Внимательное и бережное отношение к своим учетным и персональным данным поможет в защите от злоумышленников.

26 Ноября 2021

Адрес страницы: https://lipetsk.sledcom.ru/news/item/1633296