Сегодня мы поговорим о понятии киберпреступность, а так же рассмотрим виды киберпреступлений и методы защиты от них.

Киберпреступностью является любая преступная активность, где объектом в качестве цели и/или инструмента является компьютер или сетевое устройство.

В некоторых киберпреступлениях осуществляются прямые атаки на компьютеры или другие устройства с целью вывода из строя. В других - компьютеры используются в своих целях киберпреступниками для распространения вредоносных программных кодов, получения незаконной информации, или для получения криптовалюты.

Разделить киберпреступления на отдельные категории не так просто, поскольку существует множество пресечений, однако в целом можно выделить следующие виды киберпреступлений:

Финансово-ориентированные киберпреступления.

Немудрено, что многие киберпреступники используют интернет с целью получения коммерческой выгоды, осуществляя следующие типы атак:

- фишинг

Кибермошенники любят собирать низко висящие фрукты, когда предоставляется возможность заразить компьютеры ничего не подозревающих жертв. 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

Еще один популярный метод финансово-ориентированного киберкриминала – вымогательство. 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 или другой криптовалюты). Так как государственные денежные знаки можно отследить, а 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. Некоторые типы мошенничества, связанного с финансами, чрезвычайно сложно обнаружить.

Киберпреступления, связанные со вторжением в личную жизнь

Существует несколько типов подобных киберпреступлений, целью которых является кража личной конфиденциальной информации. Хотя зачастую злоумышленниками движет более глубокая мотивация (например, денежная или связанная с изменение политических настроений), основное внимание сосредоточено на обходе законов и поиске брешей в технологиях, которые защищают персональные конфиденциальные сведения.

- кража персональных данных

Кража личной информации обычно происходит с целью последующей подмены личности человека или группы людей. Хотя некоторые злоумышленники крадут паспорта или другие удостоверения личности для

физической подмены личности, в основном кража персональных данных происходит исключительно в интернете.

Например, некто, желающий получить банковский заем, может украсть персональную информацию человека с хорошей кредитной историей.

- шпионаж

Целью шпионажа, начиная от взломов индивидуальных компьютеров или устройств и заканчивая нелегальной массовой слежкой, является тайное отслеживание нашей личной жизни. Здесь может быть как физический шпионаж (например, при помощи веб- или CCTV-камер для наблюдения за отдельными персонами или группой людей), так и массовый мониторинг различного рода коммуникаций (чтение почты, текстовых сообщений мессенджеров, смс и так далее).

Нарушение авторского права

Нарушение авторских прав – одна из наиболее распространенных форм киберпреступлений. В первую очередь в эту категорию попадает выкладка в общий доступ музыки, фотографий, фильмов, книг и т. д. без согласия авторов.

Спам

Спам – чрезвычайно распространенный и многовариантный тип киберпреступлений. Сюда входит массовая рассылка по электронной почте, смс, мессенджерам и другим каналам коммуникации. Любую рассылку без согласия получателей можно отнести к спаму.

Социальные и политически мотивированные киберпреступления

Некоторые типы киберпреступлений направлены на изменения настроений в политической среде или нанесение намеренного вреда или снижения влияния отдельных личностей или группы людей.

Преступления на почве ненависти и домогательства

Преступления на почте ненависти по отношению к личности или группе людей обычно совершаются на основе гендерной, расовой, религиозной, национальной принадлежности сексуальной ориентации и других признаков. Примеры: домогательства и рассылка оскорбительных сообщений и вброс ложных новостей, касающихся определенной группы лиц.

Анонимность и легкодоступность интернета серьезно затрудняют борьбу с преступлениями на почве ненависти.

Терроризм

Группировки экстремистской направленности и воинственные народы все чаще используют киберпространство для запугивания, распространения пропаганды и иногда нанесения вреда IT-инфраструктурам. Увеличения количества бизнесов, служб и устройств, доступных через интернет, несомненно будет и провоцировать новые случаи кибертерроризма.

Кибербуллинг

Использование компьютеров и подключенных устройств для домогательств, унижения и запугивания личностей подпадает под категорию кибербуллинга. Граница между кибербуллингом и некоторыми формами преступлений на почве ненависти зачастую размыта. Некоторые формы кибербуллинга

(например, вброс обнаженных фотографий) могут подпадать под незаконные действия (например, эксплуатация детей).

Киберпреступления, связанные с недозволенными действиями

Изнанка интернета, именуемая также «dark web» (или глубоким интернетом), используется для совершения разного рода противоправных действий.

Противозаконная порнография

Распространение порнографии через интернет во многих странах трактуется как киберпреступление, в других – происходит лишь запрет содержимого экстремистской направленности. Распространение изображений с детской порнографией запрещено в большинстве стран.

Груминг

Сетевой груминг связан с сексуальными домогательствами до несовершеннолетних. В процессе могут использоваться различные методы общения: смс, социальные сети, электронная почта, чаты (например, в онлайн играх) и форумы. Во многих странах груминг подпадает под категорию киберпреступлений.

Распространение наркотиков и оружия

Различные IT-решения, используемые для распространения легитимных товаров и служб, могут также использоваться злоумышленниками. Например, рынки даркнета, существующие во всемирной паутине, помогают контрабандистам продавать оружие и наркотики и в тоже время оставаться вне поля зрения правоохранительных органов.

Как же киберприступники совершают свои преступления?

Существует четыре наиболее распространенных способа, которыми пользуются киберпреступники.

Первый, которого боятся многие люди – использование вредоносных программ. Вероятно, вы понимаете, что существует множество методов эксплуатации систем, и насколько важно использоваться различными мерами безопасности, например, устанавливать длинные пароли и делать регулярные обновления. Этот тип атак базируется на злоупотреблении компьютерами и сетями.

Второй способ – DDOS атаки, когда злоумышленник пользуется коммуникационным сетевым протоколом для создания огромного количества запросов к серверу или службе. В этом типе атак главная цель – вывести из строя объект воздействия.

Третий способ – комбинация социальной инженерии и вредоносного кода. Наиболее известная форма подобного рода атак – фишинг, когда жертву принуждают к определенным действиям (нажатию на ссылку в электронном письме, посещению сайта и т. д.), что впоследствии приводит к заражению системы при помощи первого метода.

Четвертый способ – незаконная деятельность: домогательства, распространение незаконного контента, груминг и т. д. В этом случае злоумышленники скрывают свои следы посредством анонимных профайлов, шифрованных сообщений и других подобных технологий.

Как вы могли убедиться, киберпреступления включают в себя широкий диапазон незаконных деяний, начиная от мошенничества и кражи персональной информации и заканчивая преступлениями на почве ненависти

и распространение наркотиков. Между этими видами существуем множество пересечений, и сложно провести точную границу. Например, фишинговая атака может быть направлена на кражу персональной информации. В то же время, подделка личности впоследствии может использоваться для получения денег, контрабандистами наркотиков или даже террористами. Важно понимать, что киберпреступления не всегда ассоциируются с изощренными схемами и не всегда затрагивают «глубокий интернет». Наилучший метод защиты от кибератак – быть в курсе современных угроз о которых мы рассказываем на нашем портале.