Компьютеризация, начавшаяся в конце 80-х годов XX столетия, значительно расширила сферу применения электронно-вычислительных машин. Компьютер стал необходимым атрибутом повседневной жизни.

Современные информационные технологии дали импульс не только прогрессу общества, но и способствовали возникновению и развитию некоторых негативных процессов. Одним из них стало появление одной из новых форм преступности в сфере информационных технологий - ИТ-преступность, или IT-crime.

Что же такое преступности в сфере информационных технологий ?

Преступления в сфере информационных технологий включают как распространение вредоносных вирусов, взлом паролей, кражу номеров банковских карт и других банковских реквизитов (фишинг), так и распространение противоправной информации (клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду и т.п.) через Интернет, а также вредоносное вмешательство через компьютерные сети в работу различных систем

Кроме того, одним из наиболее опасных и распространенных преступлений, совершаемых с использованием Интернета, является мошенничество, как, например интернет-аукционы, в которых сами продавцы делают ставки, чтобы поднять цену выставленного на аукцион товара.

Получили распространение и аферы, связанные с продажей доменных имен: производится массовая рассылка электронных сообщений, в которых, например, сообщают о попытках неизвестных лиц зарегистрировать доменные имена, похожие на адреса принадлежавших адресатам сайтов и владельцам сайтов предлагается зарегистрировать ненужное им доменное имя, чтобы опередить этих лиц.

Какая ответственность предусмотрена по закону за такие преступления?

В соответствии с действующим уголовным законодательством Российской Федерации под преступлениями в сфере компьютерной информации понимаются совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства

Данная группа посягательств являются институтом особенной части уголовного законодательства, ответственность за их совершение предусмотрена гл. 28 УК РФ. В качестве самостоятельного института впервые выделен УК РФ 1996 года. и относится к субинституту «Преступления против общественной безопасности и общественного порядка». Видовым объектом рассматриваемых преступлений являются общественные отношения, связанные с безопасностью информации и систем обработки информации с помощью ЭВМ.

По УК РФ преступлениями в сфере компьютерной информации являются: неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) и нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).

За данные преступления предусматривается ответственность, начиная от штрафов до 200 тысяч рублей и заканчивая 7 годами лишения свободы, в зависимости от тяжести причиненного вреда.

Хотелось бы отметить, что преступления в сфере информационных технологий могут квалифицироваться не только по специальным составам, но и по общеуголовным статьям, к примеру ст. 159 УК РФ (мошенничество) т.д.

В России борьбой с преступлениями в сфере информационных технологий занимается Управление «К» МВД РФ и отделы «К» региональных управлений внутренних дел, входящие в состав Бюро специальных технических мероприятий МВД РФ.

Как происходит борьба с так называемой «Киберпреступностью» ?

Впервые о проблемах борьбы с компьютерной преступностью в России официально было заявлено в 1992 году - с момента создания постоянно действующего межведомственного семинара "Криминалистика и компьютерная преступность", организованного в рамках координационного бюро по криминалистике при Научно-исследовательском институте проблем укрепления законности и правопорядка Генеральной прокуратуры Российской Федерации и Экспертно-криминалистического центра МВД России.

Недавно, к примеру, разоблачена и обезврежена группа мошенников, занимавшаяся электронным вымогательством. Виртуальные преступники, используя глобальную сеть Интернет и вредоносные программные продукты, создавали контролируемые сети (так называемые бот-неты) и осуществляли массированные атаки на компьютеры своих жертв, полностью блокируя их работу, с последующим требованием денег за прекращение атаки.

Для перечисления денег преступники предлагали электронные кошельки в различных платежных системах, преимущественно Webmoney, затем деньги обналичивались в различных городах России и странах СНГ. В результате проведенных оперативно-розыскных мероприятий в телекоммуникационной среде преступники были выявлены. Ими оказались жители Москвы, Новосибирска и Иркутской области, которые дистанционно управляли созданной ими сетью. Установлено, что преступниками было атаковано более 50 информационных ресурсов различных организаций.

Раскрытием таких преступлений, занимается специализированное подразделение МВД, а что делать простым людям, как самим уберечься?

Разберем несколько видов наиболее всего распространенных вариантов мошенничества.

1. Продажа несуществующего товара.

В Сети есть очень много различных магазинов, и купить можно все что угодно. Но некоторые магазины размещают товар, как правило, по низкой цене, посетитель видит привлекательные условия, оплачивает деньги, но товар до него не доходит. Он пишет в поддержку, звонит на телефон, но никто ему не отвечает. Сайт, скорее всего, через некоторое время удалят с интернета, кошелек на который вы отправили деньги, также будет удален.

В общем чтобы не попасться на мошеннические интернет магазины, нужно пользоваться проверенными ресурсами. Но там могут быть еще недобросовестнее продавцы, которые продают некачественный товар, всегда читайте о них отзывы.

Если интернет-магазин вам неизвестный, то проверьте о нем информацию, когда был зарегистрирован домен, если неделю назад, то это плохо. Какая там посещаемость, если 10 посетителей в сутки, то это также плохо. Кроме этого почитайте отзывы о сайте на форумах, если есть покупатели, которым не отправили товар, или отправили плохой товар, то естественно ненужно там ничего покупать.

2. Мошенничество в сети интернет на СМС.

Предположим вам нужно скачать какую-нибудь хорошую платную программу или информационный продукт с интернета, вы заходите в поисковую систему, находите эту программу и большую зеленую кнопку «Скачать». Вы довольны, что сейчас у вас будет отличная программа бесплатно, нажимаете на кнопку, а вам говорят, что для того, чтобы снять ограничения на скачивание нужно ввести свой номер телефона и нажать «Продолжить». Вы нажимаете, а перед вами появляется информация, что на ваш номер отправили бесплатное смс с каким-нибудь вопросом, например, сколько вам лет. Так вот, самое интересное то, что вам нужно отправить смс в ответ, для того, чтобы ответить на этот вопрос и якобы подтвердить, сколько вам лет. Но когда вы отправляете смс в ответ, то с вашего счета списывают деньги, причем немалые.

Или может быть еще другая ситуация, вы уже скачали файл, хотите разархивировать архив, но перед вами выскакивает табличка, что архив защищен паролем и чтобы ввести пароль, нужно отправить смс на какой-нибудь номер.

Запомните, если вас просят куда-нибудь отправить смс, то это на 99 % обман и с вашего счета могут списать, все что там есть. Смс подтверждение действительно может быть, но оно выглядит по-другому. Вам на телефон приходит смс с цифрами, вы вводите их, нажимаете продолжить и все.

3. Мошенничество на сайтах знакомств.

Сейчас появилось очень много различных сайтов знакомств и многие там знакомятся, ведут переписки, встречаются и даже строят серьезные отношения. Но проблема в том, что на этих сайтах зарегистрированы мошенники. Например, человеку пришла идея быстро заработать денег. Он регистрируется на каком-нибудь сайте знакомств, загружает красивые фото девушек, или просто копирует какую-нибудь женскую анкету и начинает переписываться с парнями. Естественно другие парни не знают, что за такими красивыми женскими фото сидит обычный компьютерный программист. И тут через некоторое время ему приходит предложение об оказании интим услуг. Он соглашается, но говорит, что работает только по предоплате. Деньги отправляются, а анкета - удаляется. Вот такие схемы мошенничества есть в интернете на сайтах знакомств.

4. Вы выиграли в лотерею.

Вам на почту или на телефон может прийти письмо о том, что вы выиграли в лотерею, победили в конкурсе или что-то еще, и чтобы вам прислали подарок, вы должны отправить несколько долларов за перевод. Вы отправляете деньги, но подарка естественно не получаете.

Если вы и участвовали в каком-нибудь конкурсе, то подарок отправляют, как правило, за счет компании.

5. Попрошайки в Сети.

Всем нам, наверное, много раз приходили в социальных сетях сообщения, что нужны срочно деньги на операцию, умирает ребенок или что-то в этом роде. Да, не спорю, есть люди, которым действительно нужна помощь, но в большинстве случаев такое объявление создает мошенник и пишет там номер своей банковской карточки. Вы, думаете, что помогаете ребенку вылечить рак, а на самом деле кормите мошенника.

В общем, если у вас и возникло желание пожертвовать деньги, то это конечно нужно сделать, но не через социальные сети и даже не через волонтеров, а лучше отправлять деньги напрямую на карточку больному.

Прокуратура Киевского района г. Симферополя