Преступления в Интернете

Не всякое общественно опасное деяние объявляется уголовно наказуемым. Некоторые из них государство предпочитает не криминализировать, поскольку тогда оно не сможет эти преступления раскрывать, расследовать и осуществлять правосудие - настолько их будет много. То есть бессмысленно бороться уголовно-правовыми методами с массовыми явлениями, для которых не хватит производительности существующих правоохранительных и судебных органов. Однако в отношении некоторых общественно опасных деяний такая логика не принимается во внимание законодателями. В результате в Уголовном кодексе РФ немало составов, расследований по которым не проводится, даже если есть заявление от потерпевшего. Или ещё хуже: расследования проводятся лишь по избранным случаям из массы аналогичных. В качестве примера можно привести распространение порнографии (ст. 242 УК) или нарушение тайны связи (ст. 138 УК).

К большому сожалению, значительная часть компьютерных преступлений относится именно к таким деяниям - криминализированным, но не обеспеченным ресурсами для раскрытия и расследования. Причём ресурсов не просто не хватает, не просто меньше, чем требуется. Их много меньше, чем нужно для полноценного уголовного преследования соответствующих преступлений. То есть их не хватило бы даже на малую часть, даже при идеально функционирующих правоохранительных органах.

В этой ситуации для работников правоохранительных органов не остаётся иного выхода, кроме как самостоятельно расставлять приоритеты, сообразуясь со степенью общественной опасности преступления и иными обстоятельствами.

Что такое «компьютерное преступление»?

Уголовный кодекс РФ содержит три состава, называемые преступлениями в сфере компьютерной информации, - статьи 272, 273 и 274. Термин же «компьютерные преступления» несколько шире, чем «преступления в сфере компьютерной информации». Он также охватывает те преступления, где компьютерная техника, программы, компьютерная информация и цифровые каналы связи являются орудиями совершения преступления или объектом посягательства. К таким преступлениям относятся:

- мошенничество с применением банковских карт (кардинг);
- мошенничество с выманива нием персональных данных (фишинг);
- незаконное пользование услу гами связи и иной обман в обла сти услуг связи (фрод, кража тра фика);
- промышленный и иной шпио наж, когда объектом являются ин формационные системы и т.д.

Именно раскрытие этих преступлений входит в компетенцию Управления «К».

Компьютерное преступление (киберпреступление) - уголовное правонарушение, для совершения или расследования которого существенным условием является наличие специальных знаний в области информационных технологий.

Компьютер и компьютерная информация могут играть три роли в преступлениях, которые относятся к компьютерным:

- объект посягательства;
- орудие совершения;
- доказательство или источник доказательств.

Во всех трёх случаях требуются специальные знания и специальные методы для обнаружения, сбора, фиксации и исследования доказательств.

Разница между компьютерными преступлениями и преступлениями, совершенными с использованием сети Интернет, состоит в разной уголовно-правовой квалификации. Например, если речь идет о вымогательстве, шантаже, разжигании межнациональной розни, все эти статьи представлены в Уголовном кодексе и не являются сферой деятельности Управления «К», даже если они и совершены с использованием Интернета. Экстремистские лозунги могут быть написаны и на заборе, угрожающие жизни и здоровью письма могут быть отправлены обычной почтой, квалификация преступления от того, что при этом использовалась Сеть, не меняется.

О преступлениях, связанных с педофилами

Анализ контента сети Интернет свидетельствует об активизации противоправной деятельности лиц, склоняющих малолетних детей к развратным действиям.

По имеющимся данным, в России в 2010 году число фактов педофилии выросло в зависимости от конкретного состава преступления на 150-6000/0. Тах, На 1-50% (ао 577 преступлений) увеличилось

число фактов изнасилования детей, а насильственных действий сексуального характера - на 250%. На 623% (до 3 6а2) Bbrpocro qnc-ло случаев принуждения к совершению насильственных действий сексуального характера. При этом отмечается рост гомосексуальной педофилии.

Общедоступность сетевых ресурсов, предполагающих межличностное приватное общение, видеотрансляции с использованием веб-камер в режиме реального времени позволяют растлителям малолетних беспрепятственно создавать аккаунты для склонения детей сначала к демонстрации половых органов и имитации половых актов, а затем и к реальным развратным действиям в отношении них.

Лица, склоняющие детей к развратным действиям, используя сеть Интернет, не во всех случаях публикуют и распространяют полученные в результате материалы порнографического характера с участием несовершеннолетних, в связи с чем в их действиях отсутствует состав преступления, предусмотренного статьей 242-1 УК РФ.

Действия, соответствующие вышеприведённому общему определению растления малолетних, могут быть квалифицированы как попадающие под определение статей 134 и 135 УК РФ. Они рассматриваются как посягательство на половую неприкосновенность и нормальное психосексуальное развитие несовершеннолетнего, т.к. до определённого момента ребёнок не может в силу недостаточного социального опыта осознанно и ответственно оценивать действия, связанные с сексуальной сферой. Вследствие этого согласие ребёнка на совершение сексуальных действий со взрослым психологически недостоверно и не имеет юридической силы. Кроме того, считается, что раннее вовлечение в сексуальные действия может стать причиной появления у ребёнка искажённых представлений о сексуальности, то есть нанести ему объективный вред.

Компьютерное преступление (киберпреступление) - уголовное правонарушение, для совершения или расследования которого существенным условием является наличие специальных знаний в области информационных технологий

Куда обращаться пострадавшим?

В случае если вы обнаружили в сети Интернет сайты с детской порнографией (где детям визуально меньше 12 лет, иначе потом будут проблемы с экспертизой), вам надо скопировать эту ссылку и направить ее по горячей линии сайта «Дружественный Рунет» http:// www.friendlyrunet.ru/. Orry4a uaтериал сам попадет по подследственности. Это можно сделать и анонимно.

Если вы через сеть Интернет получили угрозу жизни и здоровью либо в отношении вас совершено иное преступление общеуголовного характера, надо обращаться в общественную приемную правоохранительного портала, расположенного rro aApecy http://Ll2.ru/. Туда же можно обращаться в случаях обнаружения криминального контента в Сети (продажа оружия, наркотиков, предложения киллерских услуг, подготовка террористических актов, информация о педофилах и т.п.). Они сами определят службу, куда необходимо переслать ваш материал. Если вы хотите получить официальный ответ на ваше заявление, об этом нужно сообщить в тексте, указав свои личные данные.

Можно, конечно, обращаться с заявлением в любое территориальное отделение полиции. Но надо помнить, что для многих сотрудников данных подразделений Интернет является еще не обследованной территорией, а также отсутствуют специалисты, способные оперативно помочь тем же операм на местах разобраться в технических составляющих преступлений, совершенных с использованием Сети.

Действительно, были случаи, когда в отделение полиции пришел гражданин и сообщил, что у него были похищены редкие доспехи, очень большой ценности, в игре такой-то в сети Интернет. Дежурный не понял, что доспехи виртуальные, и направил материал на рассмотрение в отдел, занимающийся расследованием хищения антиквариата. Там разобрались, о чем идет речь. (Примечание: в некоторых зарубежных странах прошли первые судебные процессы, касающиеся хищения виртуальных предметов и персонажей. В России же интересы игроков не подлежат судебной защите, согласно ст. 1062 ГК. Исключения редки: для некоторых из видов упомянутого типа мошенничества могут использоваться вредоносные программы).

В случае если вы еще не определились, нужно или нет писать официальное заявление, является ли преступлением то, что с вами произошло в Интернете, можно обратиться на неофициальные форумы сотрудников полиции с вопросами. Там вы можете получить разъяснения, открыв отдельную тему и объяснив ситуацию в формате форума. Одним из таких форумов является «Клуб сотрудников полиции» http://police-club.ru/, rAe Mo?nHo получить консультацию как непосредственно в теме, так и по личной почте форума. В теме следует указать как можно больше сведений о произошедшем событии. Например, если вам угрожают, то какими именно действиями, посредством чего (по «аське», электронной почте или иное). Изложить свои версии: кто это мог бы быть. Унижение чести и достоинства физического лица, порча деловой репутации юридического лица, оскорбление - всё это, как правило, делается не из корыстных, а из личных побуждений. Такое движущее чувство, как обида, обычно развивается постепенно. И если ж подозреваемому пришло в голову разместить клевету или оскорбления именно в Интернете, то логично предположить, что там же, в Интернете, его «светлое» чувство обиды росло и развивалось. Поэтому в подобных случаях лучше дать подробное описание событий, предшествовавших факту, о котором вы хотите поведать. Дополнительно сообщаем, что перепосты видеофайлов и текстов, официально судом признанных экстремистскими (ст.282 УК РФ) или террористическими [ст.280 УК РФ], приравниваются к распространению данных материалов. Если не хотите подставить форум, не делайте этого, т.к. ответственность понесет Администратор.

Как научить ребенка быть осторожным в Сети и не стать жертвой Интернет - мошенников?

Кибермошенничество - один из видов киберпреступления, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и другое).

Предупреждение кибермошенничества

Проинформируйте ребенка о самых распространенных методах мошенничества и научите его советоваться со взрослыми перед тем, как воспользоваться теми или иными услугами в Интернете.

Прежде чем совершить покупку в интернет-магазине, удостоверьтесь в его надежности, и, если ваш ребенок уже совершает онлайн-покупки самостоятельно, объясните ему простые правила безопасности:

- ознакомьтесь с отзывами покупателей;
- проверьте реквизиты и название юридического лица - владельца магазина;
- уточните, как долго существует магазин. Посмо треть можно в поисковике или по дате регистрации домена fcepazc WhoIs http://wvvw.whois_service.ru/);
- поинтересуйтесь, выдает ли магазин кассовый чек;
- сравните цены в различных интернет-магазинах;
- позвоните в справочную магазина;
- обратите внимание на правила интернет-магазина;
- выясните, сколько точно вам придется заплатить, включая доставку.

Объясните ребенку, что нельзя отправлять слишком много информации о себе при совершении интернет-покупок: данные счетов, пароли, домашние адреса и номера телефонов. Помните, что никогда администратор или модератор сайта не потребует полные данные вашего счета, пароли и пин-коды.

Если кто-то запрашивает подобные данные, будьте бдительны - скорее всего, это мошенники.

Куда и как обращаться в случаях интернет-мошенничества? Бесплатный сыр - в мышеловке!

На просторах Интернета все чаще встречаются разговоры о мошеннических схемах в отношении покупателей. Главное - соблюдение основного правила: если кто-то обещает вам деньги или другую выгоду, но при этом утверждает, что вам делать ничего не нужно, только лишь внести какую-либо сумму предоплаты, то это уже 100-процентная афера.

Как вернуть свои деньги и наказать мошенника?

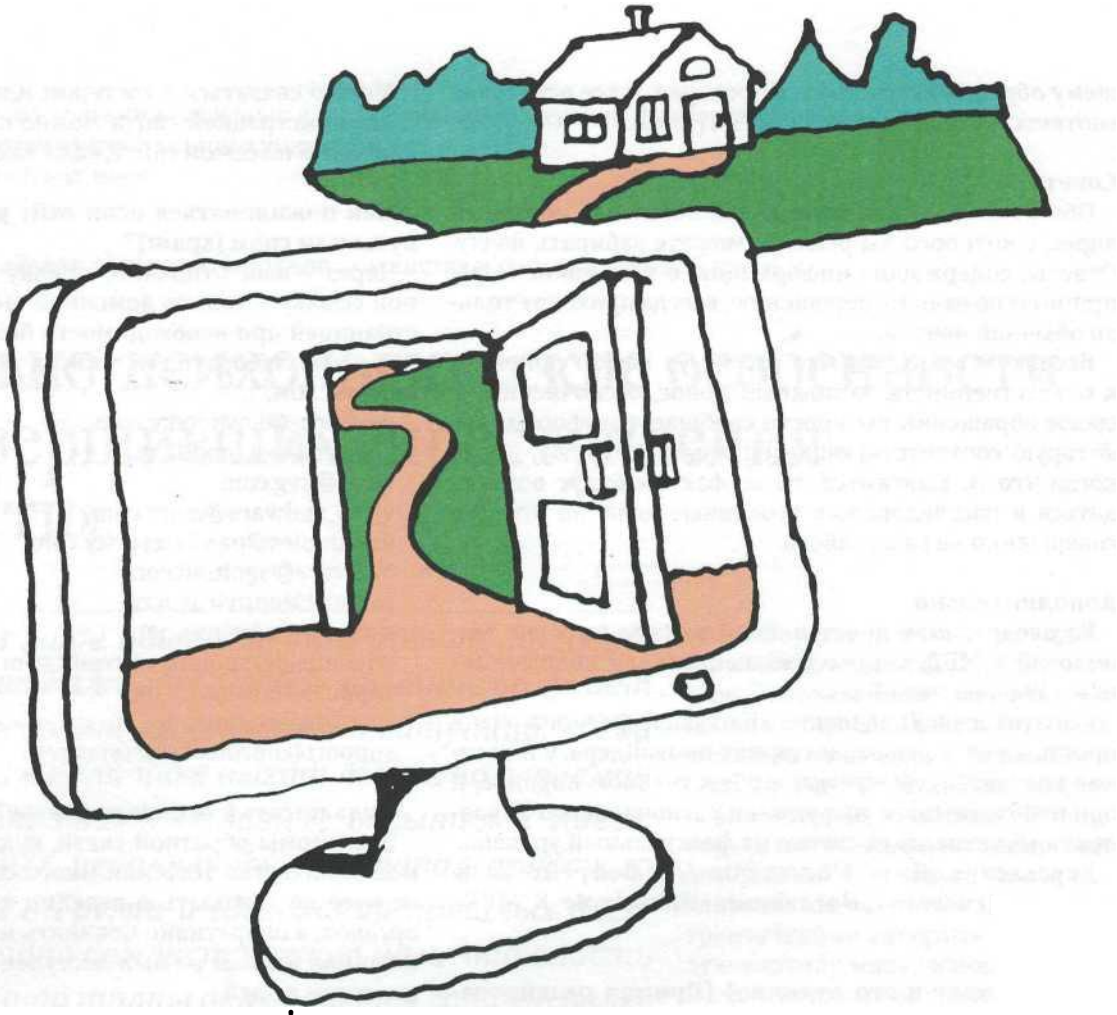
Если вы уже отдали деньги, еще не все потеряно, есть шанс вернуть свое кровное или хотя бы наказать обидчика. Наказать тоже польза, чтобы другие не попались на уловку.

Несколько важных аспектов наказания интернет-мошенников. Можно сразу переходить к действиям или прочитать, узнать правила и не попадаться на «удочку».

Например, если вас просят сделать перевод через платежную систему QIWI, это должно вас насторожить. Причина тому - через эту систему вы никак не вернете деньги.

Гарантии от мошенников, или Сайты-однодневки

На многих сайтах-визитках можно встретить раздел «гарантии», но в большинстве случаев он нужен только для того, чтобы потенциальные покупатели легче расставались с финансовыми средствами. На этой странице все красиво оформлено и расписано о мифических гарантиях. Например, многие вывешивают сканированные копии левых сертификатов чего-либо, свидетельства об аттестации участников, и это может быть картинка с небольшими photoshop-изменениями.



Основная проблема - маленькие суммы!

Понятно, что из-за потери небольших сумм никто не будет обращаться суд. Не всегда понятно, кто должен быть ответчиком, отсутствует договор и платежные документы. Даже если решение суда будет в пользу истца, то его почти не реально исполнить, то есть взыскать с ответчика причитающуюся сумму. Более того, эта ситуация негативно сказывается на бизнесе тех, кто ведет дела честно и выполняет все взятые на себя обязательства.

Способы противодействия мошенникам

Самый эффективный способ - юридическая помощь профессионалов. Единственной реальной гарантией для покупателя является обращение в правоохранительные органы. Прятки с пробегами и наглые заявления мошенников не отменяют Уголовный кодекс Российской Федерации.

Действия большинства мошенников подпадают под следующие статьи Уголовного кодекса РФ:

- статья 159 «Мошенничество»;
- статья 171 «Незаконное предпринимательство»;
- статья 182 «Заведомо ложная реклама»;
- статья 199 «Уклонение от уплаты налогов»;
- статья 200 «Обман потребителей»;
- статья 146 «Нарушение авторских и смежных прав».

Многие совершенно ошибочно считают, что обращение в правоохранительные органы по вопросам мошенничества в Интернете - это сложное, обременительное и наверняка безнадежное мероприятие. Это не так! По времени - это примерно 15-20 минут, а эффект весьма впечатляющий.

Обращаться можно по электронной почте! Это значительно упрощает дело. В своем обращении вам достаточно сообщить известные вам факты или указать на подозрительные моменты в коммерческой деятельности. Все факты и подозрения, указанные в обращениях граждан, обязательно проверяются. Для большинства интернет-мошенников уже сама проверка становится венцом карьеры.

Куда обращаться?

1. Обычное заявление в МВД Российской Федерации (раньше можно было анонимно, но по законодательству МДВ не может пустить вход все инструменты от лова мошенников по анонимному запросу).
2. Напрямую на горячую линию МВД.
3. В Генеральную Прокуратуру Российской Федерации. Если нарушения касаются не только интернет-мошенничества, но также стали известны факты мошенничества или нарушения закона должностными лицами.
4. Можно также писать в Федеральную службу безопасности Российской Федерации.

Заблуждения

Беспокоиться о том, что ваши сведения являются неполными или малозначительными, не стоит. По ва-

шему обращению состоится проверка, и все остальное соответствующие органы выяснят сами.

Совет

Обязательно указывайте такой обратный почтовый адрес, с которого вы реально можете забирать почту. Ответы, содержащие информацию о том, какие меры приняты по вашему обращению, всегда приходят только обычной почтой.

Беспокойства о том, что вас могут как-то привлечь к ответственности за ложный донос, беспочвенны. В своем обращении вы просто сообщаете информацию, которую соответствующие органы проверяют, а уже когда что-то выяснится, то по фактам будут возбуждаться и расследоваться уголовные дела, но это уже совершенно не ваша забота.

Дополнительно

Расследованием преступлений в сфере высоких технологий в МВД занимается специальное подразделение - Управление «К».

Обратиться в Управление «К» вашего региона очень просто - через любого интернет-провайдера, у них такие контакты существуют в обязательном порядке, и при необходимости сотрудники регионального Управления «К» передадут сигнал на федеральный уровень.

Управление «К» по Москве http://limited.petrovka38.ru/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii

МВД работает и это отлично! (Пример реагирования МВД)

На телефон поступило сообщение, что моя пластиковая карта заблокирована и указан телефон, куда перезвонить. Телефон своего банка я знаю отчетливо. На всякий случай проверил работу карты через интернет-банк. Все работало.

Но СМС продолжали приходить.

Можно написать через онлайн-форму в МВД Российской Федерации. Указал свои данные и e-mail, а также своими словами описал ситуацию: кто-то вымогает деньги путем шантажа, телефон такой-то.

На следующий день GMC поступать перестали.

Через три недели я получил официальный ответ по электронной почте, а еще через месяц пришло официальное письмо с подтверждением - официальным ответом МВД на интернет-мошенничество.

Сомнения в том, что МВД не работает в данном направлении, - беспочвенны.

С первого сентября 2013 года заявление можно написать из личного кабинета Госуслуг, где заполняются автоматически все поля по всей форме.

Способы найти автора сайта

Используя сервисы WH0IS, например:
lwhois.ru
nic.ru
whois.pp.ru
wwhois.ru
2ip.ru

Можно связаться с хостером или владельцем сайта. С администрацией сайта можно связаться, используя контакты на самом *сайте,* если таковые имеются.

Как пожаловаться если сайт распространяет вирусы или спам (spam)?

Через e-mail отправьте ссылку (сделайте неактивной ссылку - только доменное имя или с конкретной страницей при необходимости без протокола) в антивирусные лаборатории, описав причину отправки на английском:
newvirus@kaspersky.com
support@esetnod32.ru
virus@avg.com
virus_malware@avira.com
urlsamples@pandasecurity.com
malware@agnitum.com
support@antivirusin.ru
samples@adminus.net
windefend@submit.microsoft.com
support@emsisoft.com
root@malwares.com
support@nprotect.rsystems.com

Куда писать о мошенничестве?

Это формы обратной связи, куда можно написать о мошенничестве того или иного сайта. Тем самым вы можете не дожидаться реакции правоохранительных органов, а оперативно повлиять на то, чтобы сайт мошенника больше не был доступен максимальному количеству людей.

Yandex AntiSpam - российская поисковая система;
Google - глобальная поисковая система;
Baidu - китайская поисковая система;
Scumware;
Siteadvisor;
Badwarebusters;
Cybertopcops;
Trendmicro;
Cybercrime Tracker;
Web Inspector;
Касперский - антивирус;
Avira - aHTVBVpyc;
DrWeb - aHTr.BHpyc;
Avast - aHTHBHpyc;
Stopbadware;
Abuse;
МВД - поддерживается государством;
Роскомнадзор - поддерживается государством;

Составлено по материалам ежемесячного журнала «НарокоНет», №2, февраль 2016.