Киберхулиганы

Киберхулиганство имеет место, когда ребенок или подросток использует новые технологические ресурсы и решения (интернет, мобильный телефон, игры в режиме онлайн и др.), чтобы приставать, обижать, ставить в неловкое положение, угрожать или издеваться над другим ребенком. В эту категорию попадают следующие действия: отправка назойливых или раздражающих текстовых сообщений, написание сообщений со злым умыслом в блогах или социальных сетях, отправка фотографий или видеозаписей по электронной почте или с мобильного телефона, пересылка вредоносных кодов и вирусов, или выдача себя за кого-то другого в общении по интернет.

Киберхулиганство - это такой вид online - поведения, когда человек использует интернет для отправки «плохих», «агрессивных »писем и сообщений другим пользователям. Кроме этого, для кибер-хулиганства люди могут использовать мобильные телефоны: отправлять сообщения и звонить.

Есть масса различных способов испортить жизнь жертве. Вот самые популярные из них:

- отправка грубых или угрожающих сообщений, электронных писем, изображений, видеороликов и прочих материалов;
- публикация компрометирующих сообщений или фотографий на различных сайтах;
- общение с жертвой от имени другого человека с целью доставить душевные страдания;
- «клонирование» учетных записей жертвы для того, чтобы испортить ей репутацию на определенном ресурсе;
- взлом и получение контроля за учетными записями жертвы.

Как уберечься:

Не реагируй и не отвечай. Расскажи взрослому, если кто-то присылает тебе сообщения с агрессивным содержанием. Сохрани все «плохие» sms и сообщения электронной почты, чтобы показать взрослым. Расскажи взрослым – папе, маме и другим родственникам. Расскажи, они смогут помочь. Помни, что всегда можно обратиться на горячую линию.

Фишинг

Фи́шинг— вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того, как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Фишинг — это способ интернет-мошенничества, когда всеми возможными правдами и неправдами у вас пытаются узнать различные персональные данные (пароли, логины, номера банковских карт и счетов). Смысл заключается в том, чтобы побудить вас перейти по фишинговый ссылке на фишинговую страницу, где под различными предлогами выудить персональную информацию.

Основная защита от фишинга – это внимательность пользователя. В этом случае не помешает быть излишне подозрительным! Несколько советов, которые помогут Вам обезопасить себя от фишинга:

Проверяйте источник, от которого вам приходит письмо или сообщение.

Прежде чем переходить на страницу проверьте, нет ли ее в списке подозрительных, набирайте в адресной строке самостоятельно название.

Проверьте правильность написания домена сайта. К примеру, вместо vkontakte.ru может быть использовано vkontake.ru или vkonlakte.ru.

Проверьте цифровой сертификат сайта (замочек в статусной строке).

Также стоит обратить внимание на наличие орфографических ошибок в тексте сообщения, ни одна уважающая компания не позволит себе этого.

Пользуйтесь антивирусами, но знайте, что это не самая лучшая защита от фишинговых сайтов, так как они не загружают Вам вирусы, а Вы сами добровольно передаёте свои данные. Покупайте полные версии антивирусных продуктов, у некоторых из них ест защита от фишинговых сайтов благодаря собранной базе.

Ну и самое главное, будьте бдительны и внимательны!

Кража личных данных

Кража личных данных – любой вид мошенничества, в результате которого происходит хищение личной информации, к примеру, паролей, имен пользователей, банковских данных, номеров кредитных карточек и т.д. Кража данных доступа к счету пользователей является наиболее распространенным видом мошенничества в Интернете. Злоумышленники чаще всего используют фишинг атаки для кражи персональной информации.
Исследователи выделяют несколько групп собственности, которая наиболее часто подвергается кражам с компьютеров пользователей: параметры доступа к финансовым системам, к интернет-пейджерам и сайтам, к адресам электронной почты, пароли к онлайн-играм. Для осуществления кражи чаще всего используются вредоносные программы или методы социального инжиниринга.
Защитите свою информацию:

Для того чтобы не стать жертвой мошенников, необходимо обеспечить защиту личной информации. Если злоумышленнику не удастся получить такие данные, как номер социального страхования или банковского счета, он не сможет совершить мошеннические действия против вас.

Никогда не сообщайте свои имя, номер телефона, адрес проживания или учебы, пароли или номера кредитных карт, любимые места отдыха или проведения досуга. Используйте фильтры электронной почты для блокирования спама и нежелательных сообщений. Не регистрируйся на сайтах под своей реальной фамилией. Не общайся в чатах с незнакомыми людьми. Составляйте такие пароли, чтобы никто не мог догадаться, даже люди, имеющие доступ к вашей личной информации. Можно использовать памятные даты, но разбавленные буквами или составленные в запутанном порядке. Не храните пароли на компьютере. Все электронное можно взломать. Храните пароли либо на компакт-диске, либо на флешке в оффлайн-режиме, либо банально - на бумаге.

Вирусы

Компьютерный вирус был назван по аналогии с биологическими вирусами за сходный механизм распространения.

Компьютерный вирус — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в другие программы. Целью вируса является нарушение работы программно-аппаратных комплексов: удаление файлов, приведение в негодность структур размещения данных, блокирование работы пользователей или же приведение в негодность аппаратных комплексов компьютера и т. п. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами. Кроме того, вирусы, как правило, занимают место на накопителях информации и потребляют некоторые другие ресурсы системы.

Вирусы распространяются, используя флешки, через электронную почту, через системы обмена мгновенными сообщениями, Веб-страницы , Интернет и локальные сети.

Для защиты от вирусов установите на свой компьютер хорошую антивирусную программу, а также программу антишпион.

В настоящий момент существует множество антивирусных программ, используемых для предотвращения попадания вирусов в ПК. Однако нет гарантии, что они смогут справиться с новейшими разработками. Поэтому следует придерживаться некоторых мер предосторожности, в частности:

Не запускать незнакомые программы из сомнительных источников.

Стараться блокировать возможность несанкционированного изменения системных файлов.

Пользоваться только доверенными дистрибутивами.

Постоянно делать резервные копии важных данных, желательно на носители, которые не стираются (например, BD-R) и иметь образ системы со всеми настройками для быстрого развёртывания.

Выполнять регулярные обновления часто используемых программ, особенно тех, которые обеспечивают безопасность системы.