БЕЗОПАСНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ

Рассуждать о безопасности и конфиденциальности в социальных сетях всего мира можно часами, но следует помнить одну довольно популярную и весьма уместную истину, которая гласит: спасение утопающих – дело рук самих утопающих! Еще не изобрели такие технологии, которые бы могли побороть силу элементарной человеческой лени, беспечности и разгильдяйства.

Тяжело найти такого человека, который бы осознано рискнул оставить свой паспорт, кошелек или дорогой мобильный телефон на лавочке в парке, троллейбусной остановке и отойти купить себе мороженое. Однако большая часть пользователей сети Интернет использует пароли такого плана: 123456 или genya1 для доступа к десяткам сайтам и личной электронной почте.  
Именно на этих пользователей рассчитана работа хакеров, и, поверьте, никакой даже лицензионный антивирус с последними обновлениями не сможет заблокировать столь безалаберное поведение. Защиту информации в Мировой Сети и не только необходимо начинать не с использования последних технических новинок, а с совершенствования самого себя.

Даже соблюдение простых правил позволит многократно уменьшить угрозы и риски потери компьютерной информации и убережет от мошенничества. Вот несколько совершенно элементарных правил.  
Никогда не стоит работать на компьютере, используя права администратора. Создать учетную запись довольно просто. Учетная запись обладает такими же пользовательскими правами, как и основная оболочка. Если же вам потребуется установить какую-либо программу, просто переключитесь на «Администратор».  
Каждый новый пользователь за одним компьютером должен иметь собственную учетную запись со своим уникальным паролем.

Необходимо использовать только лицензионные программы, а не скачанные с интернета или купленные на стихийном рынке. Особенно это относится к антивирусному программному обеспечению и операционной системе.  
В настройках антивируса и операционной системы должна быть включена функция автообновления и не выключайте ее никогда.

Не нужно использовать одинаковый пароль на различных сайтах, а если пароль очень простой и короткий, то есть меньше 10 символов, регулярно меняйте его. Особенно осторожно необходимо относиться к электронной почте, к сообщениям в социальных сетях и средствам массовой связи (это Skype, ICQ).  
Сайт "Одноклассники.ру", популярность которого давно снижается среди прогрессивной интернет-аудитории, запомнится пользователям несколькими вещами. Во-первых, это все же первая массовая социальная сеть в России и, как следствие, – всеобщая радостная ажиотация.

Во-вторых, жутко неудобный интерфейс и агрессивное стремление монетизировать все, что только можно.

С тех пор мошеннических схем в социальных сетях в России появились десятки, но сегодня они прежде всего направлены против пользователей самого популярного ресурса – "ВКонтакте". Вредоносные ссылки распространяют в основном через личные сообщения и через ленту новостей. Так повышается степень доверия потенциальных жертв.

С помощью украденных аккаунтов мошенники рассылают спам – это несколько миллионов писем в день. Причем в России до сих пор не было заведено ни одного дела против спаммеров. Но кроме не особо эффективной рассылки есть и другие способы монетизации. Украденные аккаунты могут использоваться злоумышленниками для подписки пользователей на различные тематические группы рекламного содержания, для голосований и, естественно, для дальнейшего распространения ссылок на мошеннические сайты.

«Украденные аккаунты, особенно с высокими рейтингами, успешно продаются на хакерских форумах, - говорит ведущий вирусный аналитик Денис Масленников. Цена зависит от рейтинга, количества друзей и пр. Средняя стоимость 1 тысячи аккаунтов варьируется от 1000 до 2000 рублей».  
Через социальные сети злоумышленники также распространяют вредоносные приложения или же специально создают приложения для соцсетей. Летом, например, в сети «ВКонтакте» хакеры начали распространять новый троян под условным названием «Маячок». Он заражал пользователей через рассылку, рекламирующую программу для просмотра гостей страницы. Далее «Маячок» от имени «Ростелекома» блокировал пользователям доступ в интернет. Под предлогом того, что канал перегружен, троян предлагал перейти на резервный канал – для этого нужно оставить свой номер мобильного. На указанный номер приходит смс, ответив на который пользователь теряет 30 руб.

Угнанные аккаунты – основной инструмент мошенников, поэтому фишинговых ловушек придумано уже довольно много, а преступные схемы становятся все более сложными. Например, большой популярностью пользуется реклама сервисов типа "Мои гости". Через взломанные аккаунты мошенники предлагают пользователям фишинговые сайты с названиями доменов, похожими на vkontakte.

Пользователи «ВКонтакте» также частенько получают сообщения от своих друзей с просьбой проголосовать за них на одном из сайтов, для этого опять же нужно пройти авторизацию. Такие предложения, как и во всех остальных случаях, поступают, как правило, от друзей, особенно от девушек. По ссылке открывается интернет - ресурс, действительно предлагающий «проголосовать» за выбранного кандидата, щелкнув мышью по его фотографии или кнопке Like. Но чтобы это сделать, нужно войти на сайт. Там нет стандартной формы авторизации, но жертва туда попадает через специальную системы «интеграции» с социальными сетями Twitter, Facebook и «ВКонтакте».

Чтобы не стать жертвой мошенников, нужно внимательно оценивать каждое сообщение со ссылками. Если на компьютере нет антивируса, но возникли какие-то подозрения, то необходимо сразу пользоваться лечебными утилитами, которые предлагают антивирусные компании.