**ОПАСНОСТЬ СОЦИАЛЬНЫХ СЕТЕЙ**

С каждым днем социальные сети все больше захватывают внимание пользователей Интернет. Этот вирусоподобный сегмент сети уже больше не нуждается в рекламировании своих положительных сторон. Увлеченные социоманы с большим удовольствием распространяют вести о той или иной полюбившейся социальной площадке, заманивая в свои ряды лиц, хоть сколько-нибудь заинтересовавшихся социальными сетями в Интернет. Но как и следует того ожидать, рано или поздно, любое массовое скопление народа привлекает к себе любителей наживы и обмана доверчивых пользователей. Какова же реальная опасность и масштабы вреда, которые несут в себе социальные сети.

**Мобильные мошенники не спят**

Просиживая подолгу в Интернете и невольно читая, попадающуюся на глаза баненную и контекстную рекламу начинаешь задумываться, что за небольшие деньги можно купить любую информацию о нахождении или мобильной переписке человека лишь только по номеру его мобильного. А также всевозможные другие личные данные, строго охраняемые законами Российской Федерации. Мошеннические сайты предлагают всего лишь отправить SMS сообщение на указанный ими номер и все ваши потаенные желания о закрытых знаниях будут удовлетворены. При этом отправитель и не подозревает, что сумма, списанная с его счета за информационную услугу, может намного превысить указанную на сайте, а факт и качество исполнения заказанной услуги весьма сомнителен.

В ту же паутину пользователь может попасть, отправив SMS для получения результатов какого-нибудь теста или кода доступа к скачиванию игры, книги или фильма. Стоимость SMS накручивается благодаря немалым и многочисленным комиссиям от посредников, что стоят на пути от сайта высылающего заказанную информацию до вашего мобильного телефона.

Переходя на веб-страницу с предложением выслать SMS на короткий номер, убедитесь в надежности этого источника. Сведения об указанном номере и веб-сайте можно найти через поисковые сервисы вроде Google или Yandex. Многие операторы сотовой связи предлагают услугу определения точной суммы, которая будет снята за отправленное SMS сообщение. Подробности об этом узнавайте в сервис-центре своего оператора.

Нередко мошенники очень умело организовывают вид подложной страницы под один из сервисов социальных сетей. Таким образом, у пользователей не возникает сомнений к мошенническому ресурсу. Зачастую такие рекламные предложения могут появляться в доверенных социальных группах или от имени взломанных аккаунтов.

Если Вы по неосторожности все же попали в такую ловушку, можно порекомендовать немедленно обратиться как к оператору номера, на который ушли деньги, так и к собственного оператору сотовой компании. Нередко, заявление, написанное руководству, с описанием своей проблемы, позволяет вернуть деньги обратно.

**Виртуальное ничто за реальные деньги**

Истории о том, что виртуальные предметы можно продавать и покупать лет 20 назад могли лишь вызвать улыбку у читателя фантастической прозы. Сегодня такое положение дел, уже мало смущает людей близко связанных с виртуальной реальностью. В социальных сетях уже в полной мере распространены услуги по продаже виртуальных вещей от красивых смайликов до эфемерных игровых кредитов.

Пользователи, со временем впавшие в зависимость различной степени тяжести от социальных сетей не могут отказать себе в покупке виртуального дополнения своей жизни. Это ведь настолько естественно для тех, у кого границы виртуальной и реальной жизни все больше размываются. Такие виртуальные покупки еще больше засасывают пользователя в виртуальный мир, ведь действия, которые он там производит, очень схожи с жизнью в реальном мире.

**Фальшивые странички для кражи ваших данных**

В глобальной сети уже достаточно давно прогрессирует хорошо продуманный вид мошенничества, целью которого является завладение вашей учетной записью для того чтобы похитить Вашу контактную и социальную информацию или управлять аккаунтом для подачи информации от Вашего имени. Этот вид хакерской атаки называется *фишингом* и состоит в том, чтобы подсунуть ничего не подозревающему пользователю подложную веб-страницу с формой для ввода логина и пароля. После передачи данных пользователь может перейти уже к настоящей странице социальной сети, вот только вся секретная информация уже будет отправлена злоумышленнику.

Схема подлога достаточно проста. На почту или мессенджер пользователя приходит сообщение с предложением завести дружбу в социальной сети, скачать интересную игру, послушать музыку, посмотреть новый видеоролик. При этом хорошо замаскированная ссылка, указывающая на ресурс, ведет к точной копии страницы какой-нибудь социальной сети. Все это может быть закамуфлировано настолько профессионально, что пользователь даже не догадается об обмане и сам передаст мошеннику все свои данные.

Никогда не переходите по ссылкам с подобных электронных писем и сообщений. Для большей безопасности вводите адрес нужного веб-ресурса в адресную строку браузера вручную.

**Обман на доверии актуален во все времена**

Любая схема мошенничества основывается на доверии. В социальных сетях такой вид преступления для злоумышленников имеет наиболее благодатную почву. Представьте, что от Вашего хорошего друга или родственника приходит сообщение с просьбой одолжить немного электронных денег, скачать новую программу или перейти по отправленной ссылке. При этом если Ваш приятель стал жертвой злоумышленников, похитивших его данные от учетной записи, то выполнив такую просьбу Вы можете, либо навсегда лишиться отправленных денег, либо заразить свою систему вирусом от закачанного контента. Конкретный вид ущерба зависит от цели, с которой мошенники решат связаться с Вами. Такая преступная схема становиться все более популярной в социальных сетях, ведь только здесь можно получить полный доступ к базе лиц с доверительными отношениями.

Будьте осторожны, получая подобные предложения от друзей, не поленитесь дополнительно связаться с Вашими знакомыми по другим каналам (например, мобильной связи), чтобы уточнить пришедшую информацию с просьбой о каких-либо действиях.

**Публичная информация делает вас уязвимыми**

Чем больше Вы оставляете информации о себе на социальных веб-страницах, тем более упрощаете задачу мошенникам, собирающим подобные сведения для нахождения подходящих жертв. В милицейских сводках появляется все больше сведений о преступниках, нашедших своих жертв посредством социальных сетей. Будьте благоразумны, оставляя о себе те или иные данные на страницах Интернета. Ваша безопасность в Ваших же руках.