**Правила безопасности в социальных сетях**

Социальные сети предоставляют очень большой простор не только для онлайн - мошенников, но и для оффлайновых злоумышленников. Информации, размещенной в них, вполне достаточно, чтобы применять против жертвы самые различные приемы социальной инженерии. Что, как следствие, может привести к тому, что хакеры смогут получить доступ ко многим аккаунтам и даже, возможно, к банковским счетам своей жертвы.

Самая надежная защита – это, разумеется, полный и безоговорочный отказ от любого пребывания в социальной сети. К сожалению, это далеко не всегда возможно, потому что социальные сети уже перестали быть обычной забавой для школьников и студентов. Поэтому, если целиком отказаться от использования социальных сетей невозможно, то постарайтесь придерживаться семи несложных правил безопасного и комфортного общения в них.

1. Обращайте внимание на ссылки, которые сбрасывают вам ваши друзья и особенно незнакомые люди. Подозрения должны вызвать те ссылки, которые состоят из адресов сервисов для сокращения линков: goo.gl, bit.ly и друние. Но тем не менее, даже если ссылка вроде как ведет на страницу внутри самой соц. сети, в которой происходит общение, необходимо к ней приглядеться пристальнее: может оказаться так, что вместо адреса odnoklassniki.ru там будет написано что-то вроде odnok1assniki.ru, и кликнув по ней, вы заразите свой компьютер кейлогером или трояном.

2. Не используйте никаких приложений сторонних разработчиков, которые якобы помогают вам иметь доступ к «закрытым» особенностям соц. сети, повысить свой рейтинг в ней и т.п. Это же самое можно сказать и о любых сторонних сайтах. К примеру, широкое распространение имеют приложения, которые будто бы могут показать вам «гостей» вашего аккаунта в соц. сети «Вконтакте»,в которой на самом деле нет такой функции. Также стоит со всей серьезностью и подозрением относиться к программам для скачивания из социальных сетей различной музыки и видео – в них тоже могут содержаться средства хищения вашего логина и пароля.

 3. В том случае если вам приходит сообщение якобы от имени администрации социальной сети с просьбой или требованием перейти по вложенной ссылке, стоит тщательным образом проверить линк способом, который описан выше. Есть опасность того, что он может вести на фишинговый сайт, дизайн и оформление которого не будет иметь отличий от внешнего вида покинутой соц. сети, но при попытке ввести на нём логин и пароль вы надолго потеряете права доступа к своей страничке. Кстати, уже один факт того, что от вас требуют вводить логин и пароль, когда они уже запомнены браузером или самим сайтом, то это уже повод насторожиться и закрыть вкладку с подозрительным сайтом.

4. Если есть необходимость использовать соц. сети со смартфона или планшета, применяйте лишь официальные приложения тех соц. сетей, с которыми вы работаете. Если таковых нет – посещайте сайт социальной сети через обычный браузер мобильного устройства. Разумеется, приложения, попадающие в Google Play, AppStore или Windows Phone Marketplace тщательно проверяются производителями платформ, но, увы, у них также нет возможностей полностью проверить весь функционал таких программ, поэтому всё равно остается определенная вероятность того, что неофициальное приложение окажется вредоносным.

5. Не используйте стандартных способов восстановления забытого пароля и, если есть такая возможность, привязывайте свою страницу к номеру своего мобильного телефона. Очень часто мошенники получают доступ к аккаунту жертвы с помощью применения сервиса напоминания пароля. Если для успешного использования этого сервиса необходимо, к примеру, назвать девичью фамилию матери, а сама мать тоже зарегистрирована в этой соц. сети, то очевидно, что получить доступ к страничке окажется проще простого. Если сайт позволяет, то наилучшим решением станет придумать «секретный вопрос» самому, а еще лучше сделать привязку страницы к «мобильнику».

6. Задумывайтесь над тем, что пишете о себе в социальных сетях. К сожалению, они предоставляют возможность вам рассказать так много, что практически всегда все эти данные могут быть направлены против вас. Сложно заранее знать, что именно может пригодиться мошеннику, но понятно, что соц. сеть – не место для размещения сканов паспорта и других подобных вещей.

7. Осторожно устанавливайте различные приложения внутри самой социальной сети. Очень многие соц. сети имеют поддержку сторонних приложений, которые можно устанавливать на свою страницу. Эти дополнения могут иметь доступ к вашим персональным данным и, как следствие, красть пароли и логины, поэтому не стоит устанавливать их все. Как правило, если программа достаточно популярна и известна, то она не будет содержать в себе никаких хакерских функций. Если же приложение предлагает получить «VIP-статус» или возможность доступа к неким «секретным» возможностям, которые сама сеть якобы скрывает от своих пользователей, то его ни в коем случае нельзя устанавливать и использовать.