Социальные сети занимают в нашей жизни всё больше места. С их помощью решается множество вопросов, в том числе коммерческих. Из социальных сетей можно выяснить массу информации о нас. Мошенники охотно и умело пользуются социальными сетями. Они используют любую лазейку, чтобы добраться до чужих денег и данных, которые тоже стоят денег.

Злоумышленники часто используют социальные сети:

- для выманивания денег через взломанные аккаунты людей из вашего списка контактов;
- для рассылки спама;
- для получения доступа к другим ресурсам, связанным с социальной сетью;
- для получения доступа к данным, которые могут пригодиться для шантажа.

Уникальность каждого аккаунта в социальной сети заключается в содержащейся в нем информации:

- в переписке на странице в социальной сети могут содержаться важные рабочие контакты и данные. Конечно, их вообще не стоит доверять социальным сетям, но все иногда теряют бдительность;
- на вашей странице хранится личная информация, к которой вы вряд ли хотите допускать посторонних: фотографии в закрытых альбомах, список контактов, переписка и т.п.

При наличии полного доступа к вашей странице кто угодно может действовать от вашего имени: рассылать вашим друзьям фишинговые ссылки и сомнительные рекламные сообщения или просить денег взаймы.

Вы можете считать, что ваш ничем не примечательный аккаунт никогда не подвергнется нападению, потому что он никому не нужен. Однако это не так. Аккаунт в социальной сети сегодня даже важнее электронной почты. Передав кому-либо пароль от него, вы передаёте мошеннику доступ:

- к своей личной, иногда интимной, переписке;
- к своим фотографиям, в том числе предназначенным только самым близким людям;
- к своим личным данным, номерам телефонов, адресам электронной почты;
- к учётным записям компьютерных игр;
- к личным кабинетам в онлайн-магазинах.

Мошенник сможет действовать от вашего лица и выманивать деньги у всех, кто находится в списке ваших контактов, а вы можете полностью потерять доступ к своему аккаунту в социальной сети.

На все просьбы сообщить пароль друзьям, знакомым, самым близким людям вы должны ответить отказом. В этой связи игнорируйте письма и сообщения, в которых запрашивают ваш пароль, поскольку это всегда письма от мошенников.

Никогда не публикуйте в Интернете, не храните в почте или в социальных сетях копии ваших документов, в том числе фотографии паспорта и банковской карты. Если какой-то сайт требует для регистрации копию вашего паспорта, постарайтесь оценить возможные риски.

Если вы подозреваете, что кто-то получил доступ к вашему аккаунту в социальной сети, немедленно смените пароль, при этом убедившись, что аккаунт всё еще «привязан» к вашему абонентскому номеру телефона и электронной почте. При «взломе» важно обезопасить ценные личные данные и список контактов, к которым теперь есть доступ не только у вас, поэтому чем скорее вы восстановите доступ к аккаунту и защитите его надёжным паролем, тем меньше ущерба успеют причинить злоумышленники. Если вы использовали пароль от этого аккаунта где-то ещё, эти страницы/ресурсы/аккаунты тоже окажутся под угрозой в случае наличия хоть какого-либо упоминания о них в скомпрометированном аккаунте.

Злоумышленники могут действовать хитро и долгое время не выдавать себя: не делать массовых рассылок и ничего не удалять. Вас должны настораживать самые малейшие признаки чужого присутствия. Если вы подозреваете, что кто-то завладел вашим аккаунтом в популярной сети «ВКонтакте», первым делом откройте меню настройки безопасности и перейдите на вкладку «Последняя активность», где отображаются сведения о последних успешных входах в ваш аккаунт.

Используя браузер для входа в социальные сети, всегда стоит соблюдать простейшие правила:

- вводите пароль от социальной сети только на сайте или в официальном клиентском приложении самой социальной сети;
- благонадёжные сайты никогда не попросят вас ввести имя пользователя и пароль от социальной сети, с помощью которой вы авторизуетесь на этих сайтах.

Вас всегда должны настораживать:

- предложения ввести имя пользователя и пароль от социальной сети на сайте, который вы посещаете впервые и функциональные

особенности которого по своей сути никак не должны быть связаны с персональными данными пользователей социальной сети;

- предложения обновить данные аккаунта в социальной сети, которые присылают вам по электронной почте, особенно, если они содержат форму ввода имени пользователя и пароля;
- всплывающие окна, похожие на форму ввода имени пользователя и пароля от социальной сети.

Если вас автоматически перенаправили на сайт авторизации в социальной сети, проверьте, действительно ли он настоящий. Посмотрите на адресную строку: там должен быть настоящий адрес социальной сети.