О технике безопасности в социальных сетях

Прочитать последние новости, поболтать с подругой, договориться о встрече с коллегой — мы сами не заметили, как стали делать это всё в соцсетях. Удобно же, телефон всегда под рукой. Однако у онлайн-жизни есть оборотная сторона. Аккаунт в социальной сети, со всеми контактами и геотегами, может стать для злоумышленников своего рода ключом к твоим ценностям, секретам и даже финансам. Как продолжать активно пользоваться соцсетями и при этом не попасться на удочку мошенников — читай в нашем материале. Ты сам хозяин своей жизни и кузнец счастья. И в виртуальном мире это правило тоже работает «на ура». Чтобы социальные сети продолжали оставаться благом, стоит лишь соблюдать несколько простых правил.

Знай своих друзей

Прежде всего стоит определиться, кто видит информацию о тебе в соцсетях и с кем ты готов делиться своими планами, событиями и фотографиями. Много ли у тебя реальных друзей — тех, с которыми ты регулярно поддерживаешь связь, общаешься за пределами Сети? А много ли тех, кого ты лишь однажды встретил на рабочей конференции, или тех, с кем не виделся и не общался со школьных времён?

А ещё, возможно, есть вообще незнакомые тебе люди, которых ты добавил просто потому, что они попросились, или у вас общие друзья, или тебе кажется, что ты их всё-таки знаешь, просто не помнишь, где и когда вы познакомились. И если малознакомые, но всё же реальные люди, разумеется, имеют право стать твоими друзьями в соцсетях, то с незнакомцами, пожалуй, стоит быть поосторожнее — не добавлять их в список своих друзей, ведь это запросто может быть рекламный бот, который замучает тебя спам-сообщениями, или, того хуже — недоброжелатель.

Настройки приватности придуманы не просто так

Открытая всему миру страница в социальной сети — это не признак экстраверта и не следствие повышенной коммуникабельности. Сегодня это говорит скорее о беспечности. Что будет, если, например, твой личный телефон узнают мошенники? А благодаря регулярным чекинам и открытым постам любой желающий сможет следить за твоими перемещениями по миру?

Но даже если отбросить непосредственную угрозу благополучию со стороны преступников, повод контролировать, кто и что видит на твоей странице, всё равно есть. К примеру, если ты захочешь сменить работу, твой профиль в соцсети наверняка внимательно изучат рекрутеры и будущий работодатель. Точно ли им стоит видеть твои пляжные фотографии?

В общем, лучше прямо сейчас покопаться в настройках приватности. Они есть в каждой соцсети.

Полный игнор

Нет, мы не про игнорирование социальных сетей в принципе. Мы про игнорирование злобных троллей и «кибервампиров», которые используют интернет и соцсети, чтобы

развлечь себя и других пользователей. Эти провокаторы специально втягивают людей в дискуссию, чтобы вызвать раздражение, развести многочасовой (а то и многодневный) спор, разжечь всеобщую ненависть и злобу. Цель этих споров отнюдь не в выяснении истины, а дискуссия ведётся далеко не конструктивно. Поэтому не стоит тратить на это своё время и нервы.

Отдельная разновидность троллинга — кибербуллинг. То есть намеренное унижение, оскорбление и травля конкретного пользователя. Последствия могут быть очень серьёзными — вплоть до нервных срывов и даже самоубийств.

Так что смело игнорируй злопыхателей. Бань их, сообщай администраторам соцсетей. Главное — не «ведись» на их провокации. И тогда они не смогут причинить тебе никакого вреда.

Пароли: чем сложнее, тем лучше

Взлом и кража аккаунта — не такая уж редкая история. Злоумышленники могут использовать твою личную информацию, чтобы шантажировать тебя. Или они могут рассылать спам-сообщения от твоего имени. Да мало ли как ещё они могут распорядиться твоим аккаунтом в соцсети.

Чтоб не дать им такого шанса, выбирай сложные пароли, в которых будут буквы разного регистра, цифры и прочие допустимые символы. Забудь про такие набившие оскомину варианты, как qwerty или 12345. Не используй в качестве пароля дату своего рождения, имя питомца, фамилию и прочие очевидные комбинации. Во-первых, такой пароль будет легко угадать, если преступник внимательно изучил информацию о тебе в твоём же собственном аккаунте. А во-вторых, простые комбинации можно довольно быстро подобрать с помощью так называемого брутфорса — грубого перебора вариантов (для этого есть специальные программы).

А ещё не лишним будет регулярно менять пароли. Это спасёт твой аккаунт и твоё душевное спокойствие, например, в случае очередной утечки.

Делиться всем со всеми

Мы часто рассказываем и родителям, и детям о том, что чрезмерно делиться персональной информацией о себе крайне вредно. Сегодня через социальные сети о человеке можно узнать практически все: место работы, текущее местоположение и многое другое. Например, по обилию фотографий в квартире или доме можно установить уровень благосостояния семьи. Кроме того, технологии настолько шагнули вперед, что даже большое количество фото или видео с вами может привести к краже цифровой личности — это когда злоумышленник создает фейковую страницу в социальной сети с вашим именем, фотографией и другими данными. Потом он может писать непристойности или оскорбления в этой же соцсети другим пользователям или попросить у ваших друзей дать денег в долг, перевести их на карту.

Ну и напоследок — в качестве подспорья всегда используй защитные программы. Бдительность — это важно и полезно, но только проверенные алгоритмы борьбы с киберугрозами могут защитить тебя и твою социальную жизнь в Сети на 100%.

Источник https://knowledgeblog.ru/blog/43294389304/O-tehnike-bezopasnosti-v-sotsialnyih-setyah