20 правил безопасного общения в социальных сетях

Где был вчера, куда идет сегодня и где он/она будет завтра – запросто можно узнать из аккаунта соцсети. Пользовательские аккаунты в соцсетях, сайтах знакомств и т.п. – идеальны, если ты… сыщик, судебный пристав, коллектор или мошенник.

Как проводить время в соцсетях безопасно

Но охотникам до чужой личной жизни все возможности соцсетей известны. Мы же разберемся с принципами самозащиты личности в социальных сетях. Чтобы посторонние персонажи не смогли узнать слишком много. Береженого, сам знаешь, кто бережет.

1: Прочти пользовательское соглашение

При регистрации ты заполняешь обязательные пункты аккаунта, в конце имеется пункт согласия с условиями пользовательского соглашения данной соцсети. Ты знаешь об этом пункте – точно видел его кучу раз при регистрациях на различных интернет-ресурсах! Как обычно поступаешь – тупо кнопку «согласен со всеми условиями» жмешь, не читая самих условий? Зря ты так. ***Вдруг там указано что-то вроде «любые данные и материалы, введенные пользователем, являются бесспорной собственностью ресурса»?***

Приведенная выше формулировка означает, что владельцы соцсети (сайта) могут делать с публикуемым тобой (размещенными в аккаунте) контентом, что угодно им. Слить мошенникам, например. Или того хуже – напрямую в издания желтой прессы продать все фотки-видео из «скрытого» от чужих глаз соцаккаунта. И не засудишь их – сам нажал на «согласен».

2: Минимум личных данных в аккаунте

Ты не на допросе — не сообщай всей подробностей своей жизни

«Где учился» — школа-ВУЗ, но без подробного направления институтского курса обучения. Ты не на работу устраиваешься и все жизненные подробности указывать незачем. Социалки предлагают желающим указывать приятелей-подружек, мужей-жен и детей – зачем тебе это делать? Ты свою семью с родней знаешь отлично, они тебя тоже знают. А чужому народу знать про твои семейные и дружеские отношения ни к чему.

Вообще, стоит заполнять только обязательные пункты раздела «о себе». Которые звездочкой помечены. Если какая-либо социалка требует больше «обязательных» сведений – не стоит регистрироваться в ней.

3: Чем меньше фото-видео – тем лучше

Современные гаджеты – смартфоны и планшеты – наряду с доступной интернет-связью облегчают социальные коммуникации в современном обществе. И делают пользователей наивными. Мода на селфи-фото, видео и текстовое описание своей жизни в социальных аккаунтах, причем в детальных подробностях – современная норма. Глупая «норма», между прочим.

«Волшебная жизнь» медийных кумиров из инстаграмма, твиттера или фейсбука манит тебя? Не беспокоишься за выставление своей личной жизни напоказ? Напрасно. У разноплановых «звезд» имеются секьюрити, адвокаты и выгодно оплачиваемые договоренности с соцсетями (бесплатно они себя голыми выкладывают, как же!).

4: Никогда не указывай домашнего адреса

В рубрике «где живешь» достаточно вписать страну и город. Без района, улицы и, тем более, дома-квартиры. Некоторые социалки разрешают «скрывать» внесенный полный адрес от посторонних пользователей (незарегистрированных или не являющихся признанным другом). Это конечно милая функция. Только зачем вообще свой реальный адрес вводить?

Адреса в интернете постят пользователи, которые делают в сети бизнес. А тебе адрес сообщать всему интернету не нужно.

5: Лучше иметь 100 рублей, чем 100 друзей (время такое)

Дружба в соцсетях не более чем, имитация настоящей дружбы

Прежде, чем принимать очередное подтверждение «дружбы» в соцсетях, внимательно изучи аккаунт человека, напрашивающегося «на подружиться». Тем более, если ты его не знаешь по прошлой жизни. Если аккаунт нового «друга» закрыт от доступа «не друзьям» и ты не можешь составить предварительного мнения об этом персонаже – сразу отказывай в дружбе. Нафиг надо.

Чем выше благосостояние определенного человека, тем меньше у него «обычных» друзей – это факт. Бизнес-партнеры, родня не глубже родителей-сестер-братьев – они в «социальных» друзьях, это понятно. Но если какие-то детсадовские-школьные-вузовские знакомые клянчат дружбу… Причем ты их толком не помнишь, да и не общался с ними в прошлом практически… Нужны ли тебе такие приятели?

Твои одноклассники по начальной школе — давно выросли и заматерели в жизни !

6: Личная безопасность на сайтах знакомств

Найти себе девушку-парня на сайтах знакомств проще, чем в реальной жизни – шире круг потенциальных «знакомцев». Однако разномастные мошенники-садисты тоже используют сайты знакомств в качестве охотничьих угодий.

Неважно, платный или бесплатный ресурс знакомств – «темные» персонажи имеются на любом подобном ресурсе. Поэтому первые встречи с настойчивым приятелем-подругой должны происходить только в безопасной зоне – в людных местах, причем выбранных тобой.

7: Благосостояние, выставляемое напоказ

Фотографии годовых цацек и пачек баксов — всего лишь афроамериканские понты

Фотографии своих дорогих украшений, гаджетов, предметов антиквариата и т.п. размещать на странице своего социального аккаунта, по меньшей мере, глупо. Да, это действует на друзей-подруг в плане зависти, однако… это также привлекает внимание воров. С их точки зрения фотографии золотых побрякушек и премиум-гаджетов – прямое приглашение ограбить тебя. Поэтому постить фото своих ценностей по социалкам не следует.

8: Номер кредитной карты

В общем-то, это классическая рекомендация – не указывать номер своей кредитной банковской карты нигде, кроме защищенных платежных систем. Где ты платить собираешься за что-либо приобретенное. Короче – в социальных сетях данные своих кредиток публикуют или сообщают кому-либо только клинические идиоты.

9: Вход в соцаккаунт без галочки на «запомнить меня»

Проверь, чтобы галочки этой не стояло

Роскошь входить/выходить в соцсеть с сохранением пароля доступна только на персональном компьютере или смартфоне, принадлежащем лично тебе. Если компьютер общий (для всех домашних), находится по рабочему месту в офисе, либо вообще случайный – интернет-кафе или у приятеля дома – не следует оставлять свой пароль и логин в нем. Убедись, что галочка «запомнить меня» не стоит при вводе логина-пароля (она обычно «по умолчанию» активна) – они не будут сохранены на данном ПК. Данная простая мера защитит твой соцаккаунт от угона, либо использования в рассылке спама, либо кражи личных данных (контента).

Снять галочку в «запомнить меня» легко – трудно исправить ситуацию после того, как в твой аккаунт влез посторонний.

10: Не заявляй своего местоположения в социальной сети

Некоторые пользователи соцсетей находят удовольствие в постоянном указании своего текущего местонахождения. Следуя лозунгу жульверновского «Наутилуса» — «mobilis in mobile» — эти люди движутся по городам и населенным пунктам, не расставаясь с соцсетью, постоянно сообщая свой текущий пункт нахождения и следующее местоположение. Преступникам не составит труда выбрать удобный момент и ограбить дом/квартиру такого пользователя. «На дурака не нужен нож…»

11: Твой номер телефона – не для всех

Не нужно выставлять на общее внимание свой телефонный номер. Если, конечно, соцаккаунт не используется тобой в коммерческих целях. Доставучие звонки от сетевых «троллей» или мошенников – оно тебе надо?

12: «Выгодные» торговые предложения, поступающие через социальные сети

Новинки гаджетов или модных аксессуаров за полцены? Они же ворованные.

Разноплановые продажно-выгодные предложения сыпятся на тебя отовсюду по интернету, это норма наших дней. Так отчего бы не воспользоваться прямыми обращениями продавцов товаров, пишущих тебе со своих соцаккаунтов? А не стоит этого делать, тем более, если цена реально низкая – это воры, товар они так сбывают.

Полиция после покупку твою конфискует и ни шиша не вернет денег. Потому что в легальных магазинах надо закупаться, а не у сетевых сбытчиков краденого!

13: Периодическая смена своих паролей к аккаунтам соцсетей

Пароль к каждому своему аккаунту в социальных сетях необходимо менять, по меньшей мере, раз в год. Причем с добавлением символов к цифробуквенному ряду. И не использовать один и тот же пароль в нескольких аккаунтах. Иначе «хакеры» уведут твою соцстраничку или спамить через нее будут.

14: Не каждый вложенный файл в сообщении следует открывать

Тебе прислали сообщение с вложенным в него файлом, причем отправитель очень советует посмотреть этот файл. Только ты не знаешь этого отправителя – какой-то «левый» персонаж, хоть и настойчивый. Смело открываешь вложение, там картинка или еще какая фиговина, но с хитрым подвохом – с момента ее открытия все твои нажатия кнопок в аккаунте запоминаются и пересылаются постороннему «хакеру». Картинка-вложение содержит хакерский скрипт, созданный для перехвата твоего пароля от соцсети.

В общем, если не знаешь или не уверен в личности автора сообщения с вложением – не открывай вложение. Кстати, чем более неизвестный отправитель настаивает на открытии вложения, тем больше вероятность, что это хакер. Особенно не следует открывать сообщения, пришедшие к тебе, но адресованные не тебе – типа, случайно не туда отправленные.

15: Дай телефон позвонить

Слушай, дай телефончик — маме позвонить!

Сегодня смартфон – не просто телефон. Это универсальный гаджет, совмещающий в себе кучу функций, в т.ч. телефона и КПК. А поскольку ты сохраняешь пароли от своих социальных аккаунтов в своем смартфоне (кто вообще будет запароливать соцаккаунты на своем смарте?) – посторонний звонильщик может получить к ним доступ. Пока делает вид, что звонит. Решай сам, кому разрешать звонить со своего смартфона, а кого прямо посылать… к телефону-автомату (правда, их почти нет уже).

16: Проблема угроз в соцсетях решается через админов и модеров

Вступать в агрессивно-ругательный диспут с неким персонажем из соцсети глупо. Нервы портить, да злиться без толку. Все просто – пиши сообщение администрации социальной сети с указанием ссылок на бранную переписку и аккаунт ругателя. И всех дел!

В пользовательском соглашении соцсетей (которое нужно читать всем – первый пункт этой статьи!) всегда указывается, что пользователи не могут проявлять агрессию

и т.п. Короче, администрация банит за паршивое поведение нерадивых пользователей (блокирует доступ к акку).

17: Чтобы не украли твою страницу в соцсети…

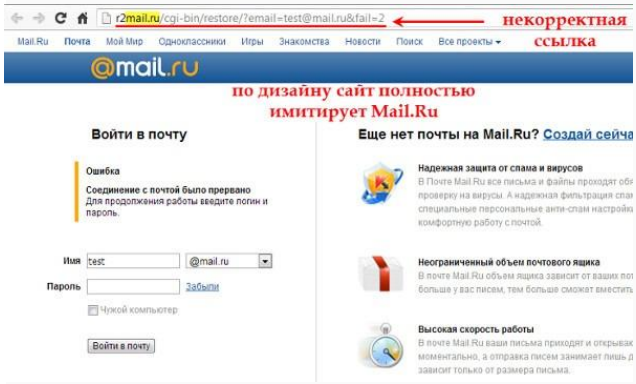
… Нужно настроить способы идентификации себя любимого. Если не к IP-адресу привязать свой аккаунт (ай-пи адреса меняются при входе с разных гаджетов и через разных поставщиков интернета), то указать два e-mail – основной и дополнительный. Тема с «секретным вопросом» уже не работает (черта с два вспомнишь потом, какой ответ сам поставил) – привязывай социальный аккаунт к номеру мобильника. Хакеру сменить пароль в соцаккаунте, где требуется подтверждение действия по телефону, будет практически невозможно.

18: Изучение функционала социальной сети

У каждой соцсети, в каждом ее пользовательском аккаунте имеются кнопки функционала, обеспечивающего безопасность личности, открывшей данный соцаккаунт. Их необходимо найти, изучить инструкции пользования ими (инструкции находятся обычно в разделе «вопросы-ответы»).

19: Если социальная сеть не способна (не желает) обеспечить твою безопасность…

… Немедленно закрывай свой аккаунт в ней. Удаляй страницу полностью – сам, если есть такая возможность, или через администрацию соцсети (по обращению к ней). Зависать в социалке, которая не обеспечивает необходимого уровня безопасности для тебя – незачем. Пустая трата времени, плюс еще и с риском для твоего кошелька/репутации.



Сайт-обманка для перехвата аккаунтов и паролей

20: Твой пароль от аккаунта в социальной сети – только твой

Мошенники-хакеры ищут новые способы добыть пароли пользователей из соцсетей. Они создают одностраничные сайты-имитации с дизайном, тупо скопированным с популярной социалки. Затем рассылают письма к пользователям, чьи e-mail удается найти – мол, введите свой пароль, пройдя по ссылке (ссылка ведет на мошеннический сайт-клон). Типа, «мы хотим убедиться, что это ваш аккаунт» или «вы действительно владелец этой страницы» и похожее бла-бла-бла…

Ни одна крупная и настоящая социальная сеть не рассылает сообщения вроде — «подтвердите свой пароль, у вас на странице замечены мошеннические действия, иначе аккаунт будет удален» — своим пользователям. Помни – ты не обязан сообщать свои пароли от интернет-ресурсов какому-то третьему (постороннему) лицу.