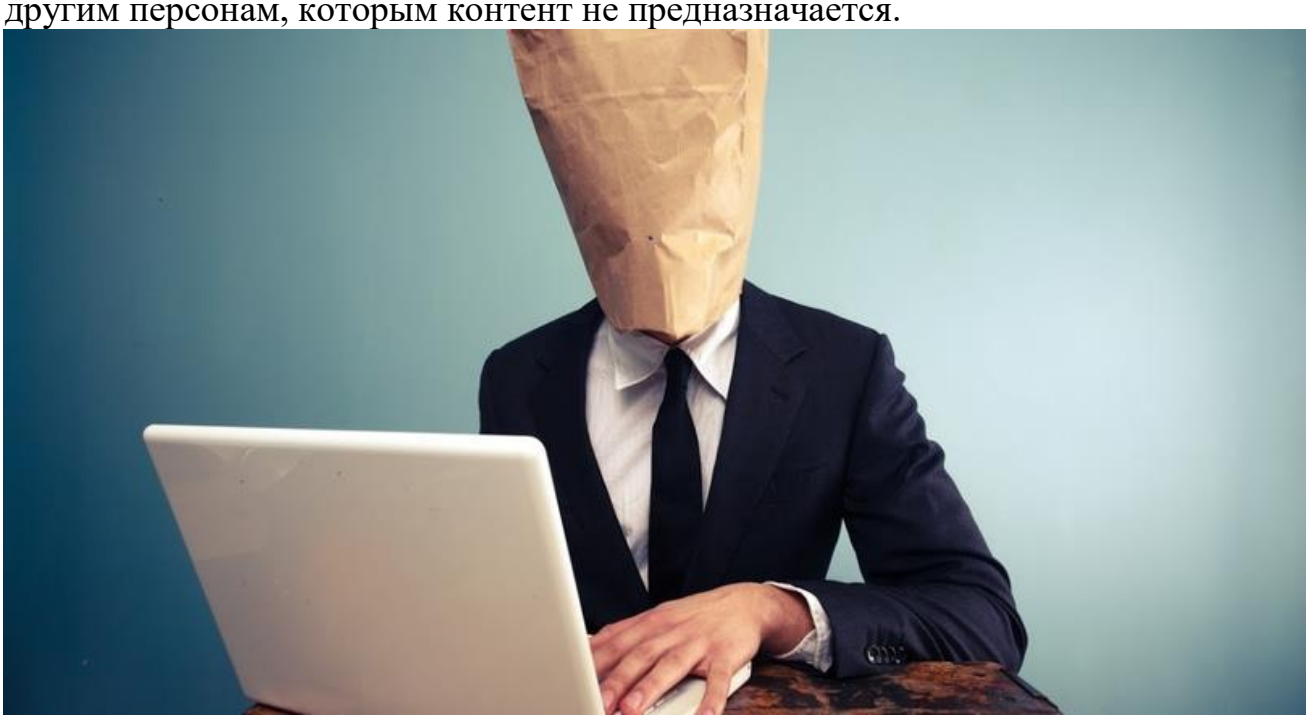
Правила безопасного общения в соцсетях

Из-за удобства социальных сетей и огромного количества возможностей, доступных в них, у человечества выработалась настоящая зависимость. Многие даже не подозревают об опасностях, которые таит в себе интернет-жизнь, а страница в соцсетях может стать настоящим сокровищем для хакеров. Чтобы не оказаться жертвой мошенников, стоит знать рекомендуемые экспертами правила поведения в Сети.

Приватность

Открывая свою страницу в социальных сетях всему миру, человек облегчает задачу злоумышленникам. Чем меньше известно о владельце аккаунта, тем сложнее взломать страницу или использовать данные в личных целях. Особенно тщательно нужно скрывать номер телефона и отметки геолокации. Также стоит ограничивать круг лиц, имеющих возможность увидеть личные фотографии, поскольку они могут попасть к работодателю или другим персонам, которым контент не предназначается.



Друзья

Все глобальные социальные сети предлагают пользователю выбирать круг “доверенных” друзей, которые смогут просматривать всю публикуемую информацию. Следует определить в этот список лишь тех, кто является знакомым в реальной жизни или виртуальным другом, а исключить нужно подозрительных личностей или полностью неизвестных. Именно они могут оказаться недоброжелателями или ботами, которые будут постоянно рассылать спам-сообщения.

Игнорирование

В Сети полно злобных людей, которые специально выводят собеседника на многочасовую дискуссию, чтобы потрепать нервы. Такие споры не приводят к истине и почти никогда не заканчиваются миром, поэтому не стоит тратить собственное время на выяснение отношений с абсолютно незнакомым человеком. Помимо троллинга, в Интернете распространен кибербуллинг, когда пользователи намеренно унижают друг друга, доводя до нервного срыва или даже самоубийства, поэтому таких особей лучше полностью игнорировать.

Информация

Следует фильтровать информацию о себе, публикуемую в Сети. Например, это касается места жительства и работы, досуга и прочих нюансов, которые стоит скрывать от незнакомцев. Технологии дошли до того, что злоумышленники могут без лишних усилий копировать аккаунт человека и от его имени публиковать оскорбления, непристойности или просить у друзей денег в долг.

Пароли

Злоумышленники стремятся взломать чужой аккаунт для разных целей, например, они могут использовать личную информацию, рассылать спам-сообщения от имени пострадавшего или шантажировать владельца. Чтобы защитить свой аккаунт от такой угрозы, следует выбирать сложные пароли с буквами разного регистра, цифрами и прочими допустимыми символами. Нельзя использовать очевидные комбинации, например, дату рождения, свое имя или кличку домашнего питомца. Остальные простые сочетания легко перебрать при помощи специальных программ.