Михаил СМАГИН,
заведующий отделом некнижных носителей информации
Ставропольской краевой универсальной научной
библиотеки имени М.Ю. Лермонтова

Семь уровней неприкосновенности

ПРИНЦИПЫ ЗАЩИТЫ АККАУНТА

Обеспокоенность по поводу блокировки, взлома профиля в «Инстаграме» или утечки авторского контента обычно возникает у нас уже после того, как одна из этих неприятностей случилась. Когда проблема требует неотложного решения, мы начинаем в спешке искать выход. Так поступают и рядовые пользователи, и те, кто ведёт официальные аккаунты учреждений, в том числе библиотек. Но ведь профилактика всегда лучше лечения. Предлагаем взять на вооружение основные правила, которые помогут свести к минимуму риск «аварийных ситуаций».

ПРАВИЛО ПЕРВОЕ

Выберите надёжный пароль

Применяйте сочетания как минимум из шести букв, цифр и других символов (например, «!» и «&»). Не повторяйте варианты, которые вы используете для авторизации в других социальных сетях, а также для входа в свою электронную почту, на какие-либо сайты и прочие интернет-площадки.

Длинную, сложную, уникальную комбинацию злоумышленники не сумеют быстро подобрать или найти в базах данных, украденных в других источниках, а значит, не смогут и взломать ваш аккаунт – по крайней мере, до тех пор, пока не произойдёт утечка сведений из самой сети «Инстаграм».

Для дополнительной защиты регулярно меняйте пароль, особенно при получении соответствующей просьбы от сотрудников техподдержки «Инстаграма», обнаруживших в ходе автоматических проверок безопасности подозрительную активность в вашем профиле.

Что позволяет взаимная привязка аккаунтов:

- создавать геолокации в «Инстаграме» – для этого нужно соединить личный аккаунт с бизнес-страницей в «Фейсбуке» (без такой синхронизации получить геометку не удастся);
- восстанавливать пароли связанных профилей (если, например, вы забыли данные входа на страницу);
- дублировать свой контент из одной сети в другую;
- пользоваться сервисом отложенного постинга (с помощью бесплатного инструмента FacebookCreatorStudio);
- осуществлять продвижение аккаунта (рекламный кабинет «Фейсбука» удобен для объявлений в «Инстаграме», а инструмент Business Manager Facebook – для сбора аналитических данных о количестве просмотров профиля за длительные периоды, тогда как приложение для телефона хранит информацию о посетителях всего 30 дней).

Кстати, не лишним будет делать то же самое и на ваших страничках в других соцсетях и на сайтах.

ПРАВИЛО ВТОРОЕ

Привяжите «Инстаграм»-аккаунт к своему профилю в «Фейсбуке», актуальному номеру телефона и электронной почте

Тем самым вы существенно расширите технические возможности пользования социальной сетью и получите ещё целый ряд преимуществ. При этом очень важно, чтобы ваш профиль в «Фейсбуке» был зарегистрирован на реального человека и вы имели возможность документально (предъявив паспорт) подтвердить ваши личные данные.

ПРАВИЛО ТРЕТЬЕ

Включите двухфакторную аутентификацию в «Инстаграме» и «Фейсбуке»

Это один из самых простых способов защиты личных данных от хакеров. Теперь каждый раз при входе в свою учётную запись в соцсети вам нужно будет ввести не только логин и пароль, но ещё и специальный одноразовый код, полученный из телефонного сообщения.

При попытке злоумышленников получить доступ к вашему аккаунту вам также придёт SMS-уведомление с кодом подтверждения: чтобы свести риск взлома к минимуму, рекомендуется сразу же сменить пароль.

ПРАВИЛО ЧЕТВЁРТОЕ

Строго ограничьте число лиц, имеющих доступ к аккаунту

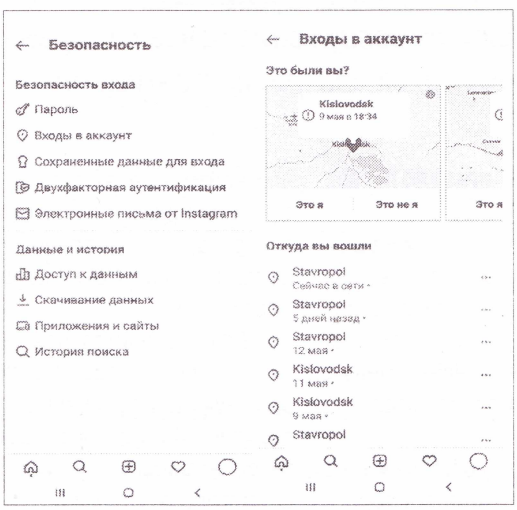
В случае пользования компьютером или телефоном совместно с другими людьми (например, коллегами по службе) обязательно выполняйте полный выход из «Инстаграма» по окончании работы и никогда не ставьте галочку в поле «Запомнить мои данные». Иначе даже после закрытия браузера в ваш профиль сможет войти кто-либо другой.

Помните также, что каждая новая авторизация, особенно если она осуществляется из разных городов, увеличивает вероятность получить ограничения на действия в аккаунте.

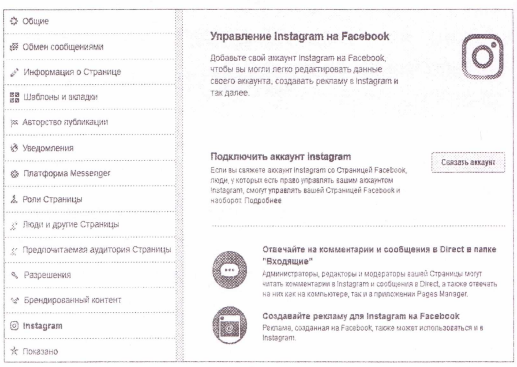
ПРАВИЛО ПЯТОЕ

Проверьте приложения, связанные с «Инстаграмом»

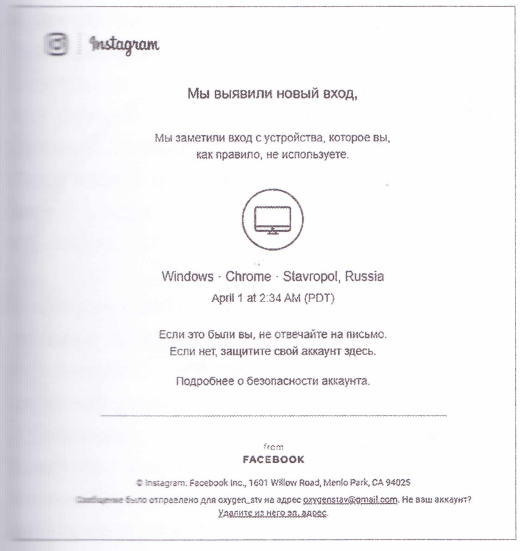
В профиле социальной сети, созданном на общедоступном компьютере, могут быть активированы функции фото- и видеоредакторов, наборы иконок, эмодзи и пр. Очень важно от-



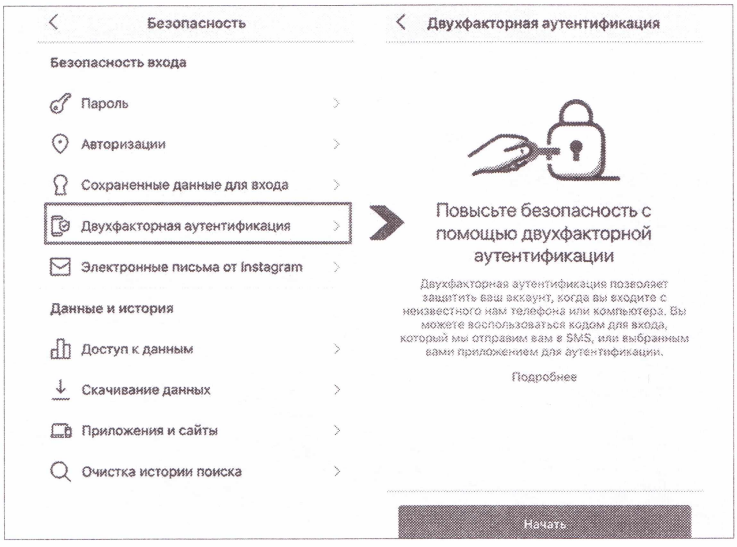
Информация о том, когда, с каких устройств и откуда именно были совершены входы в ваш аккаунт, отражается в разделе «Настройки», в блоке «Безопасность входа» ▶



▲ Синхронизация профилей в «Инстаграме» и «Фейсбуке» даёт возможность кросспостинга (публикации сообщений на одной площадке с автоматическим дублированием их на другой) и обеспечивает конфиденциальность



▲ Служба безопасности «Фейсбука» фиксирует подозрительную активность в синхронизированном аккаунте и информирует об этом по почте



▲ Двухфакторная аутентификация – инструмент дополнительной защиты. Если данная функция активирована, вам придёт SMS-сообщение со специальным одноразовым кодом, который нужно будет ввести при входе в «Инстаграм»

включить те из них, которыми вы не пользуетесь (они могли быть оставлены другими сотрудниками или установлены случайно).

ПРАВИЛО ШЕСТОЕ

Не используйте автоматизированные сервисы

Речь идёт об инструментах, позволяющих с помощью локальных и серверных приложений совершать автоматизированные действия по подписке, расстановке лайков и просмотру историй. Дело тут не в степени эффективности таких сервисов, а именно в безопасности вашего профиля. «Инстаграм» блокирует аккаунты, владельцы которых предпочитают подобные «серые» способы продвижения.

▲ Не стоит подключать автоматизированные сервисы для продвижения своего профиля: привлечения новой аудитории, ведения рекламных кампаний и т. п. Это может привести к взлому или блокировке

ПРАВИЛО СЕДЬМОЕ

Не переходите по ссылкам, присланным в письмах и сообщениях

Не поддавайтесь на предложения получить те или иные бонусы: купон на рекламу, галочку верификации (подтверждающую, что владелец профиля – реальное лицо или организация) и т. п. Если вам на почту пришло письмо от сети «Инстаграм», проверьте факт его отправки в данном приложении, в разделе «Безопасность». Если оно там не отображено, то с вами пытаются связаться мошенники.

Убедитесь, что ваш электронный почтовый ящик защищён. Имейте в виду: все, кто может читать ваши письма, с большой долей вероятности сумеют получить и доступ к вашей «Инстаграм»-страничке. Поэтому при необходимости поменяйте пароли всех почтовых аккаунтов, причём не используйте одну и ту же комбинацию дважды.

Для обычных пользователей хакерская атака – это нечто сложное, требующее высокой квалификации. Однако чаще всего владельцы аккаунтов сами предоставляют злоумышленникам все свои личные данные, адреса и пароли. В итоге завладеть персональной информацией не составляет особого труда. Выводы просты: всегда думайте о последствиях своих действий, соблюдайте перечисленные выше правила и не идите на неоправданный риск. Работайте в «Инстаграме» безопасно.