Контрольный список **на тему социальных сетей**

Социальные сети дают возможности для общения и обмена информацией. Однако в большинстве случаев пользуясь бесплатными предложениями, мы вынуждены платить за них высокую цену, делясь своими персональными данными. Мы поделимся с вами 10 советами по безопасному использованию социальных сетей.

1. В отношении профилей в социальных сетях всегда действует следующее правило: не сообщайте о себе слишком много личной информации!
2. Для разных социальных сетей используйте разные пароли, которые должны быть надежными!
3. В настройках профиля можно увидеть, какие данные о вас видят все и кто имеет доступ к вашему профилю.
4. Проверьте настройки, касающиеся защиты ваших данных, и установите ограничения на определенные права, например на персонализированную рекламу.
5. В качестве изображения профиля выберите фоновую картинку или нейтральную фотографию, чтобы избежать возможных неловких последствий.
6. Прежде чем загружать в сеть какой-либо контент, подумайте, действительно ли вы хотите им делиться, и если да, то с кем. Хотели бы вы, чтобы в Интернете всегда были ваше изображение или статус?
7. Будьте осторожны, получая запросы на установление контакта. Является ли их отправитель реальным лицом и заслуживает ли он доверия? Совет: будьте особенно осторожны, если кто-то, представляясь вашим знакомым или родственником, просит у вас деньги или персональные данные, например номер мобильного телефона.
8. Если в какой-либо социальной сети вас или других лиц кто-то преследует («кибersталкеры» и «тролли»), например, если с вами навязчиво пытаются связаться против вашей воли — опубликуйте соответствующую информацию в этой же сети.

9. Если какие-либо тексты, изображения, видеоматериалы или комментарии являются, по вашему мнению, оскорбительными и враждебными по отношению к определенным группам людей, запишите эту информацию и сообщите об этом. Например, сюда: meldestelle-respect.de и hateaid.org.
10. Не нажимайте на все ссылки без разбора. Социальные сети все чаще используются в качестве инструмента для получения персональных данных и доступа к учетным записям («фишинг»).

Как понять, что новость является фейком

Читая или пересылая новости в соцсетях, всегда спрашивайте себя: является ли эта информация правдивой?

- Кто автор этой новости? Есть ли источник?

  Совет: если вы видите ссылку на внешний новостной портал, обратите внимание на выходные данные этого портала. Законодательство Германии требует, чтобы на немецких веб-сайтах присутствовали выходные данные (Impressum). Выходные данные обычно публикуются в нижней части страницы.

- Как выглядит новость? Крикливые заголовки с множеством восклицательных и вопросительных знаков в сопровождении эффектных изображений может быть первым признаком фейка.
- Кто написал эту новость? Что известно об этой личности?
- Была ли эта новость уже опубликована в авторитетных источниках и на заслуживающих доверия сайтах газет или новостных порталах?

  Совет: проверяйте факты. На сайтах mimikama.org, tagesschau.de/faktenfinder или correctiv.org можно узнать, какие фейковые сообщения активно распространяются на текущий момент.

- Где, когда и кем было сделано это изображение или видео? Что оно содержит на самом деле?

  Совет: при помощи инструмента обратного поиска изображений от Google images.google.de или Bing можно проследить, откуда изначально появилось изображение и в каком контексте использовалось.

- Является ли новость актуальной? Есть ли у нее дата и соответствует ли она действительности?

Сомневаетесь? Тогда обратитесь за независимой консультацией! Подробную информацию вы получите у специалистов Центра защиты прав потребителей. **www.verbraucherzentrale.de**

verbraucherzentrale
Brandenburg

Gefördert durch:
LAND BRANDENBURG
Ministerium für Soziales, Gesundheit, Integration und Verbraucherschutz

Verbraucherzentrale Brandenburg e.V.
Projekt „Smart Surfen – Mehr Teilhabe durch digitalen Verbraucherschutz“
Babelsberger Str. 12, 14473 Potsdam
www.verbraucherzentrale-brandenburg.de
Illustrationen: Raphael Bräsecke, illustrationsagentur.com