



Контрольний список на тему соціальних мереж

Соціальні мережі надають можливість взаємодіяти один з одним та обмінюватися інформацією. Однак, здебільшого користуючись безкоштовними пропозиціями, ми змушені платити високу ціну: ми платимо за них своїми персональними даними. Нижче наведено 10 рекомендацій щодо безпечного користування соціальними мережами.

1. До профілів у соціальних мережах завжди застосовується таке правило: не повідомляйте про себе надто багато особистої інформації!
2. Для різних соціальних мереж використовуйте різні паролі, до того ж вони мають бути надійними!
3. У налаштуваннях профілю перегляньте, які дані про вас доступні всім і хто має доступ до вашого профілю.
4. Перевірте налаштування конфіденційності даних, які було встановлено за замовчуванням, і обмежте певні права — наприклад, на персоналізовану рекламу.
5. Для зображення профілю обирайте фонову картинку чи нейтральну фотографію, щоб уникнути подальших можливих незручних моментів.
6. Перш ніж завантажувати будь-які матеріали в інтернет, поміркуйте, чи хочете ви ділитися ними, а якщо так, то з ким саме. Чи хочете ви, щоб ваша фотографія або статус назавжди залишилися в мережі?
7. Будьте обережні, отримуючи запити на встановлення контакту. Чи є їх відправник реальною особою та чи викликає він довіру? Порада: виявляйте особливу пильність, якщо хтось видає себе за знайомого або члена сім'ї та просить у вас гроші чи персональні дані, наприклад, номер мобільного телефону.
8. Якщо в будь-якій соціальній мережі вас або інших осіб хтось переслідує («кіберсталкери» та «тролі»), наприклад, якщо з вами нав'язливо намагаються зв'язатися проти вашої волі — повідомте про це в цій же мережі.
9. Документуйте та повідомляйте про текстові повідомлення, зображення, відео чи коментарі, які ви вважаєте образливими чи такими, що розпалюють ненависть до певних груп людей. Наприклад, сюди: meldestelle-respect.de та hateaid.org.

10. Не переходьте за всіма посиланнями, які ви бачите. Соціальні мережі все частіше використовуються для отримання ваших персональних даних та доступу до облікових записів в інтернеті («фішинг»).

Як розпізнати фейкові новини

Коли ви переглядаєте новини чи ділитесь ними в соціальних мережах, завжди запитуйте себе: «Чи дійсно це може бути правдою?».

- Хто повідомив цю новину? Чи є джерело?

Порада: якщо ви бачите посилання на зовнішній новинний портал, зверніть увагу на вихідні дані цього portalу. Згідно з німецьким законодавством, німецькі вебсайти повинні містити вихідні дані (Impressum). Зазвичай вихідні дані розміщуються в нижній частині сторінки.

- Як написана новина? Крикливі заголовки з великою кількістю знаків оклику та запитань у поєднанні зі вражаючими зображеннями можуть бути першою ознакою фейку.
- Хто написав новину? Що відомо про цю особу?
- Чи повідомляли інші авторитетні джерела та достовірні вебсайти газет або новинних випусків про цю новину?

Порада: користуйтеся пошуковиками фактів. На mimikama.org, tagesschau.de/faktenfinder та correctiv.org ви можете дізнатися, які неправдиві повідомлення наразі активно поширюються.

- Де, коли та ким було зроблено фото чи відео? Що на ньому насправді зображено?

Порада: за допомогою інструмента зворотного пошуку зображень від [Google images.google.de](http://Google.images.google.de) або Bing можна відстежити походження зображення та дізнатися, в якому контексті воно вже використовувалося.

- Чи є новина актуальною? Чи вказано її дату та чи відповідає вона дійсності?

! Ви не впевнені? Отримайте незалежну консультацію! Додаткову інформацію ви можете отримати в Центрі захисту прав споживачів: www.verbraucherzentrale.de