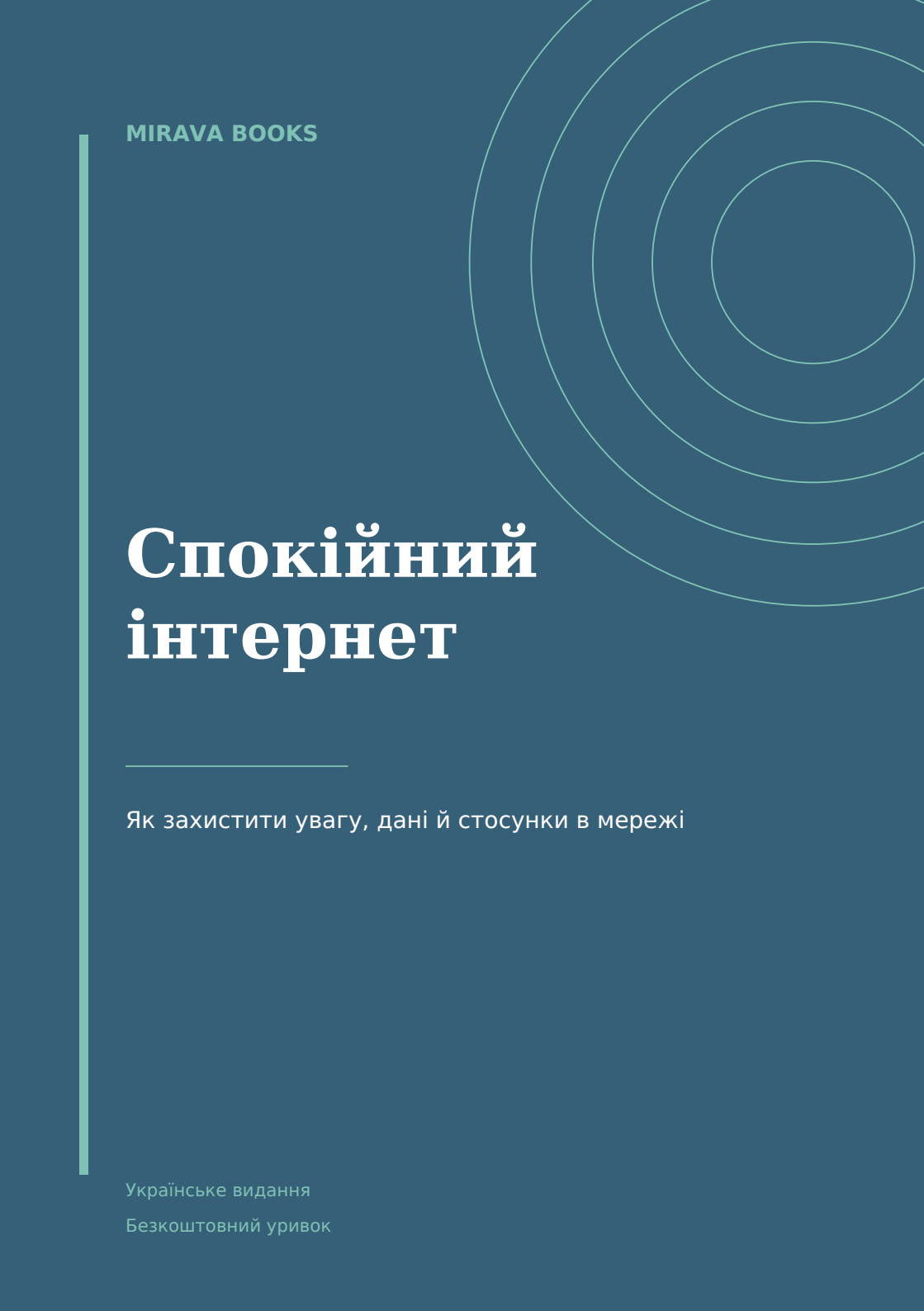




MIRAVA BOOKS

Спокійний інтернет

Як захистити увагу, дані й стосунки в мережі

Українське видання

Безкоштовний уривок

Спокійний інтернет

Як захистити увагу, дані й стосунки в мережі

Українське видання · Оновлене видання · жовтень 2026

Це посібник для сімей і користувачів-початківців, які хочуть захистити акаунти, особисті дані й час у мережі. Читайте по одному розділу та перевіряйте налаштування за офіційною інструкцією свого пристрою або сервісу: назви меню можуть змінюватися. Приклади вигадані, текст підготовлено за допомогою штучного інтелекту. Технічні рекомендації звірено з опублікованими матеріалами BSI та первинними джерелами, указаними наприкінці. За злому, втрати грошей або погроз дійте через офіційну підтримку й компетентні служби; вправи не заміняють термінової допомоги.

MIRAVA · Текст і переклад підготовлені за допомогою ШІ.

Зміст

- 01 Цифровий дім
- 02 Повідомлення, яке квапить
- 03 Особисті дані за потребою
- 04 Телефон без нескінченної стрічки
- 05 Конфлікт у коментарях
- 06 Сімейна цифрова домовленість

Цифровий дім

Один пароль використовується в пошті, грі й магазині. Після витоку цей пароль доводиться замінити в усіх місцях, де він повторювався. Якщо пошта використовується для відновлення інших акаунтів, захист її доступу особливо важливий. Акаунти зручно уявити як кімнати з різними ключами: розкриття одного ключа не має відкривати всі двері. Така метафора пояснює правило, але не обіцяє повної безпеки.

BSI рекомендує окремі сильні паролі для різних сервісів і додатковий захист входу, коли він доступний. Використовуйте довгі унікальні паролі; не будуйте їх на імені чи простій зміні одного слова. Менеджер паролів допомагає створювати й зберігати різні значення. Обирайте засіб зі зрозумілою офіційною інструкцією, захистіть його головний доступ і заздалегідь розберіться, як відновити власний доступ. Не передавайте паролів «помічникам» у листуванні.

Увімкніть двофакторний захист за інструкцією сервісу. Він додає перевірку, наприклад через застосунок або апаратний ключ, але не робить будь-який вхід безпечним: шахрай може виманити й одноразовий код. Не повідомляйте кодів співрозмовнику та не підтверджуйте вхід, якого не починали. Якщо сервіс надає резервні коди, зберігайте їх окремо й захищено, з можливістю знайти після втрати телефону. Перевірте актуальність контакту відновлення.

Практика: складіть список важливих акаунтів без самих паролів. Відзначте, де є повторення й другий фактор. Почніть з одного важливого входу, зберігши доступ до відновлення. Установіть блокування екрана й доступні оновлення пристрою. За підозри на злом використовуйте процедуру відновлення сервісу; зміна одного пароля не завжди завершує усунення інциденту. Не

відкладайте захист інших повторюваних паролів після відомого витоку.

Це безкоштовний уривок. Повна PDF-книга містить усі розділи зі змісту.
Продажі ще не відкриті.

Додаткове читання

[1] BSI — Basistipps zur IT-Sicherheit · www.bsi.bund.de

[2] BSI — Zwei-Faktor-Authentisierung · www.bsi.bund.de

[3] BSI — E-Mail-Sicherheit: Mythen im Faktencheck · www.bsi.bund.de

[4] BSI — Encryption on mobile devices · www.bsi.bund.de

[5] Polizeiliche Kriminalprävention — Messenger-Betrug · www.polizei-beratung.de

[6] Polizeiliche Kriminalprävention — Digitale Beweise sichern ·
www.polizei-beratung.de

[7] British Airways — Manage My Booking: booking reference and surname ·
www.britishairways.com