

MIRAVA BOOKS

A Calmer Internet

Protecting attention, data, and relationships online

English edition

Free excerpt

A Calmer Internet

Protecting attention, data, and relationships online

English edition · Revised edition · October 2026

This guide is for families and new users who want to protect accounts, personal data and time online. Read one chapter at a time and check settings against your device or service's official instructions: menu names can change. The examples are fictional; the text was prepared with the help of artificial intelligence.

Technical recommendations were checked against published BSI material and the primary sources listed at the end. For compromised accounts, lost money or threats, use official support and appropriate services; exercises cannot replace urgent help.

MIRAVA · Text and translation prepared with AI assistance.

Contents

- 01 Your digital home
- 02 The message that rushes you
- 03 Personal data only when needed
- 04 A phone without an endless feed
- 05 Conflict in comments
- 06 A family digital agreement

01

Your digital home

One password is used for email, a game and a shop. After a leak, it must be changed wherever it was reused. If email restores other accounts, protecting it is especially important. Imagine accounts as rooms with separate keys: exposing one key should not open every door. This explains the principle without promising complete security.

BSI recommends separate strong passwords for different services and additional sign-in protection where available. Use long, unique passwords rather than a name or minor variations on one word. A password manager helps create and store different values. Choose a tool with clear official instructions, protect its main access and understand recovery beforehand. Do not share passwords with “helpers” in messages.

Enable two-factor protection according to the service's instructions. It adds a check, for example through an app or hardware key, but does not make every login safe: scammers can obtain one-time codes too. Do not give codes to another person or approve a login you did not start. If recovery codes are provided, store them separately and securely where you can find them after losing a phone. Check your recovery contact.

Practice: list important accounts without passwords. Mark reuse and second-factor protection. Begin with one important login while preserving recovery access. Set a screen lock and install available device updates. Suspected compromise requires the service's recovery procedure; changing one password may not resolve the incident. After a known leak, do not delay replacing other reused passwords.

This is a free excerpt. The complete PDF contains every chapter listed in the contents. Sales have not opened yet.

Further reading

[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