

MIRAVA BOOKS

Спокойный интернет

Как защитить внимание, данные и отношения в сети

Русское издание

Бесплатный фрагмент

Спокойный интернет

Как защитить внимание, данные и отношения в сети

Русское издание · Обновлённое издание · октябрь 2026

Это руководство для семей и начинающих пользователей, которые хотят защитить аккаунты, личные данные и время в сети. Читайте по одной главе и проверяйте настройки по официальной инструкции своего устройства или сервиса: названия меню могут меняться. Примеры вымышлены, текст подготовлен с помощью искусственного интеллекта. Технические рекомендации сверены с опубликованными материалами BSI и первичными источниками, указанными в конце. При взломе, потере денег или угрозах действуйте через официальную поддержку и компетентные службы; упражнения не заменяют срочную помощь.

MIRAVA · Текст и перевод подготовлены с помощью ИИ.

Содержание

- 01 Цифровой дом
- 02 Сообщение, которое торопит
- 03 Личные данные по необходимости
- 04 Телефон без бесконечной ленты
- 05 Конфликт в комментариях
- 06 Семейный цифровой договор

Цифровой дом

Один пароль используется в почте, игре и магазине. После утечки этот пароль приходится заменить во всех местах, где он повторялся. Если почта используется для восстановления других аккаунтов, защита её доступа особенно важна. Аккаунты удобно представить как комнаты с разными ключами: раскрытие одного ключа не должно открывать все двери. Такая метафора объясняет правило, но не обещает полной безопасности.

BSI рекомендует отдельные сильные пароли для разных сервисов и дополнительную защиту входа, когда она доступна. Используйте длинные уникальные пароли; не строите их на имени или простом изменении одного слова. Менеджер паролей помогает создавать и хранить разные значения. Выбирайте средство с понятной официальной инструкцией, защитите его главный доступ и заранее разберитесь, как восстановить собственный доступ. Не передавайте пароли «помощникам» в переписке.

Включите двухфакторную защиту по инструкции сервиса. Она добавляет проверку, например через приложение или аппаратный ключ, но не делает любой вход безопасным: мошенник может выманить и одноразовый код. Не сообщайте коды собеседнику и не подтверждайте вход, которого не начинали. Если сервис предоставляет резервные коды, храните их отдельно и защищённо, с возможностью найти при потере телефона. Проверьте актуальность контакта восстановления.

Практика: составьте список важных аккаунтов без самих паролей. Отметьте, где есть повторение и второй фактор. Начните с одного важного входа, сохранив доступ к восстановлению. Установите блокировку экрана и доступные

обновления устройства. При подозрении на взлом используйте процедуру восстановления сервиса; смена одного пароля не всегда завершает устранение инцидента. Не откладывайте защиту остальных повторяющихся паролей после известной утечки.

Это бесплатный фрагмент. Полная PDF-книга содержит все главы из содержания. Продажи пока не открыты.

Дополнительное чтение

[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