ПРАКТИЧЕСКОЕ РУКОВОДСТВО

Цифровая безопасность без паники

Как защитить телефон, деньги, аккаунты и личные данные в повседневной жизни



РУССКОЕ ИЗДАНИЕ • 2026

Фади Кабара

Цифровая безопасность без паники

«Автор»
2026

Кабара Ф.

Цифровая безопасность без паники / Ф. Кабара — «Автор», 2026

Практическое руководство по цифровой безопасности для обычных пользователей и небольших команд. Книга объясняет, как защищать смартфон и компьютер, создавать надёжные пароли, включать многофакторную аутентификацию, распознавать фишинг и телефонное мошенничество, безопасно пользоваться банковскими приложениями, делать резервные копии и действовать после утечки данных. Отдельное внимание уделено социальному инжинирингу, поддельным голосам и сообщениям, защите детей и безопасности малого бизнеса.

© Кабара Ф., 2026
© Автор, 2026

Содержание

Важное предупреждение 5
Предисловие 6
Как пользоваться книгой 7
Глава 1. Безопасность начинается с модели угроз 8
Глава 2. Пароли и многофакторная аутентификация 9
Глава 3. Смартфон и компьютер 10
Глава 4. Фишинг и поддельные сообщения 11
Глава 5. Телефонное и банковское мошенничество 12
Конец ознакомительного фрагмента. 13

Фади Кабара
Цифровая безопасность без паники

Важное предупреждение

Материал предназначен для общего образования и не заменяет индивидуальную консультацию профильного специалиста. Примеры и расчёты приведены для обучения, если не указано иное. Законодательные и медицинские сведения актуальны на 2 ноября 2026 года; перед принятием конкретного решения проверьте действующие нормы, клинические рекомендации, договоры и инструкции.

Предисловие

Эта книга создана как практический маршрут: от понимания базовых принципов к последовательным действиям. Её задача — помочь читателю задавать более точные вопросы, проверять предположения и избегать распространённых ошибок. Она не обещает лёгкого результата и не заменяет консультацию профильного специалиста там, где требуется индивидуальная оценка.

В каждой главе сначала объясняется принцип, затем показывается его практическое значение и предлагается способ проверить, как он работает в конкретной ситуации. Все условные суммы и ситуации являются учебными примерами. Их нельзя автоматически переносить на любой регион, семью, бизнес или состояние здоровья.

Как пользоваться книгой

Читайте главы последовательно, но возвращайтесь к чек-листам при подготовке к реальному действию. Отмечайте вопросы, на которые пока нет ответа, и проверяйте изменяющиеся сведения по первичным источникам. Если решение связано с существенными финансовыми, юридическими или медицинскими последствиями, используйте книгу для подготовки к консультации, а не вместо неё.

Глава 1. Безопасность начинается с модели угроз

Цифровая безопасность — не установка одного антивируса и не покупка самого дорогого телефона. Это понимание того, какие данные и деньги вы защищаете, от кого, каким способом они могут быть украдены и какие последствия будут самыми тяжёлыми. Набор мер для обычного пользователя и для владельца интернет-магазина будет разным.

Начните с инвентаризации: электронная почта, банковские приложения, Госуслуги, мессенджеры, социальные сети, облачные хранилища, рабочие сервисы и устройства семьи. Определите, какие аккаунты позволяют восстановить остальные. Почта часто становится ключом ко многим сервисам, поэтому её защита особенно важна.

Разделите угрозы на массовые и целевые. Массовая рассылка пытается обмануть большое число людей; целевая атака может использовать знание о вашей работе, родственниках или заказах. Не обязательно быть известным человеком, чтобы попасть в адресную атаку: достаточно доступа к деньгам или полезным данным.

План безопасности должен быть выполнимым. Если правила настолько сложны, что человек начинает обходить их, защита фактически не работает. Лучше несколько устойчивых мер — уникальные пароли, многофакторная аутентификация, обновления и резервные копии — чем длинный список, который никто не выполняет.

Глава 2. Пароли и многофакторная аутентификация

Главное правило паролей — не повторять один и тот же пароль на разных сайтах. Если один сервис утечёт, злоумышленник попробует эти данные на почте, банках и социальных сетях. Длинный уникальный пароль снижает риск автоматического подбора и повторного использования.

Менеджер паролей помогает создавать и хранить уникальные комбинации. Защитите его сильной основной фразой и многофакторной аутентификацией. Не храните основной пароль в открытом файле рядом с приложением и не пересылайте его самому себе в обычном мессенджере.

Многофакторная аутентификация добавляет второй фактор: приложение-аутентификатор, аппаратный ключ или подтверждение другим способом. SMS лучше отсутствия второго фактора, но у него есть риски, связанные с перевыпуском SIM-карты и перехватом сообщений. Используйте наиболее надёжный способ, который доступен сервису.

Сохраните резервные коды восстановления в безопасном месте. Если потерять телефон без резервного доступа, можно лишиться собственного аккаунта. При смене устройства заранее проверьте перенос аутентификатора и обновите контактные данные восстановления.

Глава 3. Смартфон и компьютер

Устанавливайте приложения из официальных источников и проверяйте разработчика. Не устанавливайте неизвестный APK по ссылке из сообщения, особенно если собеседник утверждает, что это банковская защита, обновление Госуслуг или приложение для возврата денег. Запрос разрешений должен соответствовать назначению программы.

Устанавливайте обновления операционной системы, браузера и приложений. Они исправляют не только ошибки, но и известные уязвимости. Устройство, которое давно не получает обновления, постепенно становится менее защищённым; для банковских и рабочих задач стоит планировать его замену.

Включите блокировку экрана, короткое автоматическое отключение и возможность удалённого поиска или блокировки устройства. Используйте шифрование, если оно доступно. Не оставляйте разблокированный телефон без присмотра и не подключайте его к неизвестным компьютерам и зарядным станциям без необходимости.

Для работы с важными документами используйте отдельные профили или учётные записи, когда это возможно. Не храните все пароли и сканы документов в одной папке без защиты. Если устройство потеряно, сначала заблокируйте SIM-карту и сеансы важных сервисов, затем измените пароли с доверенного устройства.

Глава 4. Фишинг и поддельные сообщения

Фишинг — попытка заставить человека раскрыть данные или выполнить действие через поддельное письмо, сообщение, сайт или звонок. Сообщение может выглядеть как уведомление банка, маркетплейса, доставки, государственного сервиса или руководителя. Логотип и грамотный текст не доказывают подлинность отправителя.

Проверяйте адрес сайта полностью, а не только логотип. Злоумышленники используют похожие домены, добавляют символы и меняют отдельные буквы. Не переходите по ссылкам из неожиданного сообщения, если требуется авторизация или оплата; откройте приложение самостоятельно или введите адрес вручную.

Срочность — главный психологический инструмент. «Счёт заблокируют через пять минут», «родственник попал в беду», «вам начислена выплата» — всё это заставляет действовать без проверки. Сделайте паузу, свяжитесь с организацией по независимому каналу и уточните ситуацию.

Не отправляйте коды из SMS, push-подтверждений и приложения-аутентификатора человеку, который звонит или пишет первым. Настоящая служба поддержки не нуждается в вашем пароле и не должна просить перевести деньги на чужой счёт для «защиты».

Глава 5. Телефонное и банковское мошенничество

Мошенники могут представляться сотрудниками банка, полиции, следственных органов, оператора связи или службы безопасности. Они используют угрозы, уверенный тон и знание части персональных данных. Информация о вашем имени или банке не доказывает, что звонит настоящий сотрудник.

Если собеседник просит сообщить код, пароль, данные карты, установить приложение удалённого доступа, снять наличные или перевести деньги на «безопасный счёт», прекратите разговор. Самостоятельно позвоните в банк по номеру на карте или в официальном приложении. Не используйте контакт, который прислал собеседник.

По информации Банка России, с 1 января 2026 года расширен перечень признаков мошеннических переводов, которые банки учитывают при проверке операций. Это может приводить к дополнительным вопросам или задержкам, но не означает, что каждый необычный перевод автоматически является мошенническим. При блокировке уточняйте причины у своего банка по официальному каналу.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, купив полную легальную версию на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.