

# Кибергигиена каждый день:

Простые привычки, которые  
защищают ваши аккаунты.



ИИ  
Марк Тьюрин

# Марк Тьюрин

## Кибергигиена каждый день: Простые привычки, которые защищают ваши аккаунты

*<https://litres.ru/74568607>*

*SelfPub; 2026*

### Аннотация

Что вы потеряете вместе с доступом к почте или телефону — и сможете ли вернуть его без паники? Безопасность начинается с понимания, какие аккаунты держат на себе остальные.

Книга поможет составить карту важных аккаунтов, укрепить почту, настроить уникальные пароли и второй фактор, заранее подготовить способы восстановления. Вы научитесь проверять срочные сообщения, звонки, ссылки и QR-коды, действовать при потере телефона или подозрении на захват, проверять активные сессы и права приложений. Разберётесь, почему защищённая сеть не гарантирует подлинность сайта и почему резервная копия не заменяет восстановление аккаунта.

Она для тех, кто пользуется смартфоном, банковскими приложениями, Госуслугами, почтой, мессенджерами и маркетплейсами, но не хочет превращать безопасность во вторую работу. Итог — карта аккаунтов, более надёжный вход и

выполнимый план на случай потери доступа; в обычные дни — короткие проверки вместо постоянной тревоги.

Книга создана с помощью ИИ.

# Содержание

|                                          |    |
|------------------------------------------|----|
| Ваша цифровая связка ключей              | 5  |
| Почта — не просто почта                  | 19 |
| Пароли без повторов и мучительной памяти | 34 |
| Второй фактор — второй замок             | 48 |
| Сообщение, которое торопит               | 63 |
| Конец ознакомительного фрагмента.        | 69 |

# **Марк Тьюрин**

## **Кибергигиена каждый день: Простые привычки, которые защищают ваши аккаунты**

### **Ваша цифровая связка ключей**

На экране телефона легко насчитать два десятка приложений, которыми вы пользовались за неделю. Но список иконок не покажет, как они связаны, где хранятся важные данные и что перестанет работать, если вы потеряете доступ к одному аккаунту. Для этого нужна не опись приложений, а карта зависимостей.

Начните с короткой инвентаризации. Вспомните, чем вы пользовались за последние семь дней: приложениями, сайтами в браузере, личными кабинетами, рабочими программами. Запишите названия или хотя бы категории: банк, почта, Госуслуги, маркетплейс, сервис хранения файлов, рабочая система, социальная сеть. Не старайтесь сразу вспомнить всё. Ваша задача — не перечислить каждую установленную

программу, а увидеть, где проходят важные связи.

Не записывайте пароли, коды подтверждения, секретные ответы, полные номера карт и телефонов. Карта должна показывать устройство системы, а не давать постороннему готовый доступ к ней. Храните её так, чтобы вам было удобно сверяться, но не превращайте в хранилище секретов.

### **Список приложений — только поверхность**

Одна и та же учётная запись может открываться и в приложении, и через браузер. Бывает и наоборот: приложение установлено на телефоне, но отдельного аккаунта в нём нет. Вход может выполняться по номеру телефона, электронной почте или данным, которые вы создали на сайте сервиса. Поэтому важно учитывать не только программы, но и сами учётные записи.

Приложения на телефоне тоже не дают полной картины. Возможно, почтой вы пользуетесь только через браузер, но именно этот аккаунт нужен для восстановления доступа к другим сервисам. Список установленных программ такую связь не покажет.

Чтобы ничего важного не упустить, загляните в приложения, которыми пользовались на этой неделе, в закладки и историю браузера, а также в письма и сообщения об оплатах, покупках, входах и изменениях настроек. Уведомления часто напоминают о сервисах, которые не пришли в голову сразу. Для инвентаризации достаточно названия отправителя или сервиса — не переходите по ссылкам из старых со-

общений.

Уточните, что именно стоит за каждым пунктом. «Банк» — это не просто иконка, а, возможно, приложение, карта, интернет-банк и несколько счетов. «Почта» — конкретный аккаунт, к которому привязаны другие способы входа. «Рабочий сервис» — учётная запись с документами, перепиской или доступами, нужными коллегам. Если услугой пользуются несколько членов семьи, отметьте это отдельно: общий аккаунт и личная учётная запись — разные вещи.

Теперь разделите найденное на три слоя.

Устройство — физический предмет, с которого вы входите: телефон, компьютер или планшет. На нём могут оставаться активные сеансы, сохранённые файлы, уведомления и доступ к почте. Потеря устройства не обязательно означает потерю аккаунтов, но посторонний может получить доступ к уже открытым приложениям.

Аккаунт — учётная запись, которая позволяет сервису распознать вас. Для входа и восстановления могут использоваться пароль, номер телефона, адрес почты, подтверждение с другого устройства или обращение в службу поддержки. Набор способов зависит от сервиса и ваших настроек.

Данные — всё, что вы храните или получаете через устройство и аккаунты: документы, фотографии, переписка, заказы, платёжные сведения, контакты, настройки. Одни данные могут храниться только на устройстве, другие — в личном кабинете, третьи — в обоих местах. Потеря доступа

к аккаунту и потеря самих данных — не одно и то же, хотя иногда одно приводит к другому.

Это различие помогает точнее оценить риск. Если телефон сломан, но вы знаете пароль, имеете доступ к почте и можете войти с другого устройства, последствия могут быть ограниченными. Если телефон был единственным способом подтверждать вход, а почта недоступна, восстановление затянется. А если важные документы хранятся только в памяти устройства, потеря телефона опасна сама по себе — даже если аккаунты удастся вернуть.

### **Невидимые двери**

В цифровой системе одни аккаунты ведут к другим. Адрес электронной почты может использоваться для восстановления доступа к маркетплейсу или рабочему кабинету. Номер телефона — для подтверждения входа или получения уведомлений. На устройстве может оставаться открытая почта, через которую можно запросить восстановление доступа к другим сервисам.

Аккаунт, с помощью которого можно вернуть доступ к нескольким другим, будем называть опорным. Его значение не зависит от популярности сервиса. Малозаметный почтовый ящик может оказаться важнее приложения, которым вы пользуетесь каждый день, если именно на него приходят ссылки для восстановления паролей и уведомления о важных изменениях.

Связи бывают разными. Сервис может использовать почту

только для уведомлений, но не для восстановления. Номер может быть указан в профиле, хотя вход по нему отключён. Одно приложение может показывать данные другого сервиса, но не помогать вернуть к нему доступ. Не делайте выводов по знакомому названию — проверяйте настройки конкретного аккаунта.

Удобно обозначать связь стрелкой. Например, «почта → личный кабинет маркетплейса» означает, что доступ к почте помогает восстановить доступ к маркетплейсу. «Телефон → банк» — что номер участвует в подтверждении действий или восстановлении именно в вашем банке. Если роль номера пока неясна, поставьте вопросительный знак и уточните её в официальном приложении или личном кабинете сервиса.

Обратите особое внимание на цепочки, которые замыкаются сами на себя. Допустим, для восстановления почты нужен код на телефон, а доступ к кабинету оператора, где можно управлять номером, в вашей ситуации зависит от этой же почты. Если вы потеряете и телефон, и почтовый аккаунт, вернуть оба доступа будет сложнее. Такая схема есть не у всех, но лучше обнаружить её заранее.

Номер телефона и устройство — не одно и то же. Телефон можно потерять, повредить или заменить, сохранив номер. И наоборот: устройство может остаться у вас, а доступ к номеру пропасть из-за неисправности SIM-карты или других обстоятельств. На карте отметьте отдельно номер как канал

восстановления и телефон как устройство с активными сессиями.

Для каждого опорного аккаунта выясните, есть ли хотя бы один способ восстановления, который не зависит целиком от того же устройства. Это не значит, что нужно включать все предлагаемые варианты или сообщать дополнительные данные без необходимости. Важно понять, какие способы уже настроены, доступны ли они вам и не ведут ли обратно в тот же тупик.

### **Считайте последствия, а не популярность**

Распределите аккаунты по тому, к чему приведёт потеря доступа. Для этого не нужны сложные расчёты. Достаточно спросить себя: что именно станет недоступно, насколько срочно оно понадобится и какие другие аккаунты окажутся под угрозой или задержкой?

Критичный аккаунт — тот, потеря которого может затронуть деньги, подтверждение личности, работу, важные документы или восстановление других учётных записей. Для одного человека это банковское приложение, для другого — рабочая почта, от которой зависят документы и общение с клиентами. Госуслуги могут быть критичными, если вы регулярно получаете через них государственные услуги или используете связанные с ними функции. Само наличие аккаунта не означает, что все эти возможности подключены: учитывайте, как именно вы им пользуетесь.

Важный аккаунт создаёт заметные неудобства, но его по-

теря не блокирует сразу несколько жизненно необходимых процессов. Например, в личном кабинете могут храниться история покупок и адреса доставки. Это ценно, но последствия потери доступа отличаются от потери средств или рабочих документов.

Повседневный аккаунт нужен для отдельных задач, которые обычно можно отложить или выполнить другим способом. Это не повод пренебрегать его защитой. Просто при ограниченном времени разумнее сначала заняться теми аккаунтами, от которых зависят другие.

Оценивайте два свойства по отдельности. Первое — последствия потери доступа к самому аккаунту. Второе — его связи: сколько других важных сервисов используют его для входа или восстановления. Почта может быть не особенно важна как место для переписки, но стать опорным аккаунтом. А приложение без значимых данных и связей с другими сервисами может остаться повседневным, даже если вы открываете его каждый день.

Не путайте потерю доступа с захватом аккаунта. В первом случае вы не можете войти, но нет признаков, что кто-то действует от вашего имени. При захвате посторонний мог изменить пароль, просматривать данные или отправлять сообщения. Тогда к невозможности войти добавляются действия, которые нужно останавливать. На карте достаточно отметить, где при компрометации возможны денежные операции, изменение данных или доступ к другим аккаунтам.

Если такое произошло, это уже не плановая инвентаризация: действовать нужно по правилам сервиса и через его официальные каналы поддержки.

### **Три практических разбора**

Начнём с почты. Если на адрес приходят уведомления о входах, чеки, сообщения от банка и ссылки для восстановления других аккаунтов, у него много важных связей. Потеря доступа грозит не только пропущенными письмами, но и задержкой восстановления нескольких сервисов. Такая почта должна стоять на карте выше приложения, которое сообщает о новых публикациях и не хранит нужных вам данных.

Проверьте, какие телефоны и дополнительные адреса указаны для восстановления и доступны ли они вам сейчас. Настройка, сделанная когда-то, может оказаться бесполезной: старый номер уже мог перейти другому абоненту, а резервный адрес — забыться. Если сервис показывает устройства и активные сеансы, посмотрите и на них. Это не проверка на взлом, а способ понять, откуда ещё можно попасть в аккаунт.

Теперь банковское приложение. Его важность определяется не частотой использования, а тем, что через него можно делать и какие действия требуют отдельного подтверждения. Для одного пользователя это доступ к счетам и переводам, для другого — ещё и выписки, оплата регулярных услуг или управление картой. Возможности и способы восстановления у банков различаются. Не считайте, что потеря телефона автоматически означает потерю доступа к деньгам, но и не рас-

считывайте, что войти получится с любого устройства. Запишите порядок восстановления, который банк указывает в официальных источниках.

Уточните, как банк связывается с вами и подтверждает действия. Номер телефона может быть важной частью этой схемы, но не обязательно единственной. Не вносите в карту коды из сообщений и реквизиты: достаточно написать «номер используется для подтверждения» или «способ нужно уточнить». Если телефон хранит активный сеанс банка и принимает подтверждения, отметьте обе его роли — устройства и канала связи.

Маркетплейс обычно кажется менее важным: заказ можно сделать повторно, товар купить в другом месте. Но в аккаунте могут храниться адреса, история покупок, незавершённые возвраты, переписка с продавцами и сведения о способах оплаты. Если вы ждёте дорогую доставку или оформляете возврат, временная потеря доступа будет неприятной. Но последствия не обязательно критичны. Подумайте, какие данные и операции важны именно вам, и выясните, как сервис восстанавливает доступ. Не переносите на маркетплейс предположения о банке или Госуслугах: связи нужно проверять отдельно.

Наконец, рабочий аккаунт. Если через него доступны общие документы, переписка или система, которой пользуются коллеги, последствия затронут не только вас. Потеря доступа может задержать работу, а захват позволит отправлять

сообщения от вашего имени или просматривать рабочие материалы. Отметьте, кто отвечает за восстановление: вы сами, администратор организации или служба поддержки. Не записывайте в личную карту рабочие секреты и данные, которые нельзя хранить вне корпоративной системы.

### **Карта на одном листе**

Сведите результаты инвентаризации в таблицу — на бумаге или в защищённом личном файле. Заполняйте только то, что относится к вашей жизни. Если способ восстановления неизвестен, так и напишите: «проверить». Это полезнее, чем уверенное, но непроверенное предположение.

Для основной почты отметьте её ценность: она критична, если через неё восстанавливаются другие аккаунты. В качестве способов восстановления укажите телефон, резервный адрес или другой вариант из настроек и проверьте, доступны ли они. Связанные сервисы — только те, связь с которыми подтверждена. Следующий шаг: проверить способы восстановления и активные сеансы.

Для номера телефона укажите, важен ли он для получения кодов или уведомлений. Восстановление номера проходит по официальной процедуре оператора. Запишите, какие сервисы действительно от него зависят, и выясните, какую роль номер играет в каждом из них.

Для банковского приложения отметьте, что потеря доступа может затронуть финансовые операции и сведения. Способ восстановления ищите в официальных источниках бан-

ка. Если приложение связано со счетами, картами и платежами, укажите их, не предполагая дополнительных связей. Запишите, что делать при потере устройства.

Для Госуслуг оцените важность по тому, какие услуги и функции вы используете. Укажите доступные способы восстановления и только те сервисы, куда действительно входите с этой учётной записью. Проверьте актуальность способов восстановления и реальность связей.

Для маркетплейса отметьте, насколько важны для вас заказы, возвраты и хранящиеся данные. Укажите привязанные способы входа и восстановления, а также проверьте, доступны ли контактные данные.

Для рабочей учётной записи оцените последствия потери доступа к общим материалам и задачам. Уточните, можно ли восстановить её самостоятельно или потребуется помощь администратора. Связи с почтой, документами и рабочими системами указывайте только по фактической схеме.

Этот образец не задаёт универсальных связей. Например, не нужно автоматически считать Госуслуги способом входа в банковский сервис, а банковское приложение — ключом ко всем государственным услугам. Такие связи есть только там, где вы действительно их настроили или используете. Если сомневаетесь, оставьте их неподтверждёнными до проверки.

Чтобы карта оставалась компактной, не вносите каждую покупку, переписку и страницу. Отмечайте аккаунты и каналы, если в них хранятся важные данные, через них можно

распоряжаться деньгами или подтверждать личность либо они помогают восстановить другие аккаунты. Обычно этого достаточно, чтобы уместить главную картину на одном листе.

Теперь соедините связанные аккаунты стрелками. Если почта помогает вернуть доступ к маркетплейсу, проведите стрелку от почты к маркетплейсу. Если в банковском приложении используется номер, соедините их и подпишите роль номера: «код», «уведомление» или «восстановление». Такая связь может быть удобной, пока всё работает, но уязвимой, если оба способа доступа зависят от одного потерянного устройства.

Посмотрите на карту как на схему метро: важны не самые крупные станции, а пересадки, через которые проходит много маршрутов. Аккаунт с несколькими стрелками к важным сервисам заслуживает внимания, даже если вы редко его открываете. Если от одной точки зависят банк, рабочая почта и личные кабинеты, её потеря может вызвать цепную задержку.

## **Первые приоритеты**

Не пытайтесь защитить всё сразу. Выберите две-три точки, где сочетаются серьёзные последствия и важные связи. Часто это основная почта, номер телефона или само устройство, но не обязательно. Если через рабочую учётную запись открываются критичные документы, а почта нужна только для несущественных подписок, порядок будет другим.

Для каждой выбранной точки назначьте одно следующее действие. Например, проверьте актуальность способов восстановления почты, уточните в официальных материалах банка, что делать при потере телефона, или убедитесь, что устройство защищено кодом блокировки и вы знаете, как завершить потерянный сеанс. Действие должно быть конкретным и выполнимым, а не расплывчатым «усилить безопасность».

Проведите короткую проверку независимости. Если устройство пропадёт сегодня, сможете ли вы войти в основную почту с другого? Если перестанет работать номер, знаете ли вы, как получить инструкции от оператора или сервиса без доступа к нему? Если восстановление каждого аккаунта требует одного и того же канала, отметьте это как приоритет. Не запускайте пробное восстановление без необходимости: некоторые сервисы ограничивают частые попытки, а случайный запрос может усложнить доступ.

Карта не должна быть идеальной или оставаться неизменной. Меняются номера, устройства, работа и набор сервисов. Обновляйте её, когда заводите важную учётную запись, меняете номер, отдаёте устройство в ремонт или закрываете опорный аккаунт. На это хватит нескольких минут: подробный каталог всей цифровой жизни не нужен.

Откройте свой список и выберите первую точку, с которой начнёте. Если трудно решить, сравните два показателя: сколько важных процессов остановится при потере доступа

и сколько других аккаунтов зависят от этой точки. Обычно наивысший приоритет там, где заметны оба последствия. Так абстрактное «защитить всё» превращается в понятную очередь действий.

Карта не устраняет риск и не гарантирует быстрого восстановления. Она помогает увидеть, какие двери связаны, какие ключи открывают сразу несколько из них и где у вас нет запасного пути. Следующие главы помогут укрепить выбранные точки с учётом вашей схемы, а не в отрыве от повседневной жизни.

Начать стоит с почты: она часто становится каналом восстановления для других аккаунтов, хотя кажется всего лишь местом для писем. В следующей главе мы разберём, какие двери может открывать почтовый ящик и как проверить, насколько надёжно защищён этот узел.

# Почта — не просто почта

В цифровой связке ключей есть узлы, потеря которых затрагивает не одну дверь. Почтовый ящик — один из них: через него проходят уведомления, ссылки для восстановления и сообщения о новых входах. На экране это может выглядеть как обычный список писем, но роль почты в доступе к другим аккаунтам гораздо шире.

Представьте адрес, на который годами приходили чеки, подтверждения регистрации и сообщения от банка, интернет-магазина и государственных сервисов. Часть писем давно забыта, но адрес всё ещё может быть привязан к этим аккаунтам. Если вы потеряете доступ к почте, последствия будут зависеть от настроек каждого сервиса. Если же в ящик войдёт посторонний, под угрозой окажутся не только письма. Чтобы оценить риск, нужно проследить связи, а не делать вывод по одному адресу.

## Три роли одного почтового адреса

Почтовый адрес часто выполняет сразу несколько функций. Их важно различать: само по себе его наличие в профиле не говорит о том, какие возможности он открывает.

Идентификатор. Адрес помогает сервису определить аккаунт и иногда используется для входа. Но он не обязательно служит единственным способом авторизации. В одном сервисе можно войти по номеру телефона, в другом — через

отдельную учётную запись, а где-то почта нужна только при регистрации.

Канал уведомлений. На адрес приходят чеки, сведения о заказах, предупреждения о новых входах и изменениях настроек. Такие сообщения помогают заметить событие, но не всегда позволяют его отменить. Кроме того, если письма автоматически пересылаются, удаляются или попадают в отдельную папку, часть предупреждений можно пропустить.

Канал восстановления. Если пользователь забыл пароль, сервис может прислать ссылку или код на почту. Но порядок восстановления везде разный: один сервис попросит подтвердить вход через приложение или номер телефона, другой предложит обратиться в поддержку, третий потребует дополнительную проверку. Даже если адрес указан в профиле, это ещё не значит, что восстановление доступно именно через него.

Почтовый аккаунт — самостоятельный сервис со своим паролем, способами подтверждения и настройками безопасности. Адрес лишь связывает его с другими системами. Потерять возможность читать письма — не то же самое, что автоматически лишиться всех аккаунтов, в которых этот адрес когда-то указали. Однако доступ к почте может упростить восстановление некоторых из них.

Условная схема поможет увидеть, как это работает. В центре — почтовый ящик. К нему привязаны аккаунт интернет-магазина, хранилище документов, личный кабинет опе-

ратора связи и аккаунт на государственном портале. Но связь с каждым устроена по-своему. Магазин может присылать чеки и разрешать восстановление через почту. Хранилище — требовать дополнительного подтверждения. Оператор — отправлять уведомления на адрес, а восстановление проводить через приложение или контактный центр. Государственный сервис — использовать собственные правила входа и проверки личности.

Если доступ к почтовому ящику утрачен, пользователь может не получить ссылку для восстановления аккаунта магазина или предупреждение об изменении настроек хранилища. Если же в ящик вошёл посторонний, он может прочитать конфиденциальные письма, узнать, где зарегистрирован адрес, и попытаться запустить процедуру восстановления. Удастся ли ему это, зависит от конкретного сервиса, его проверок и включённых способов защиты. Почта — не универсальный мастер-ключ, но часто она находится рядом с замком.

Задача не в том, чтобы воображать худший сценарий, а в том, чтобы выяснить, какие связи существуют и насколько они важны.

## **Как найти связанные аккаунты**

Начать проще всего с самого почтового ящика. Поиск по письмам часто обнаруживает то, о чём вы уже забыли: старые регистрации, подписки, чеки и сообщения о смене пароля. Ищите не только названия сервисов, но и слова, связанные

с действиями в аккаунте: «подтверждение», «регистрация», «новый вход», «восстановление доступа», «смена пароля», «заказ», «чек», «код». Формулировки у отправителей различаются, поэтому стоит попробовать несколько запросов.

Загляните в архив, корзину, спам и папки, созданные вами. Если доступен поиск по всей почте, воспользуйтесь им. Не открывайте вложения и ссылки из старых писем только ради аудита. Чтобы проверить, существует ли аккаунт, безопаснее открыть приложение или самостоятельно набрать адрес официального сайта и посмотреть настройки профиля. Логотип в письме сам по себе не доказывает подлинность отправителя.

Проверьте и отправленные письма: там могут быть запросы в поддержку или сообщения, которые напомним, как вы пользовались аккаунтом. История покупок и уведомления об оплате подписок тоже помогут найти активные сервисы, даже если регистрационное письмо затерялось.

Сопоставьте найденное с другими источниками. В менеджере паролей может храниться список сайтов и приложений, где сохранены ваши логины. В браузере или телефоне можно найти приложения, в которые вы входили с этим адресом. В банковских личных кабинетах видны регулярные списания за услуги. Но не пытайтесь по одному платежу определить, как устроено восстановление аккаунта: это отдельная настройка. Регистрации, входы и оплаты — подсказки для проверки, а не готовая карта безопасности.

Не все найденные связи одинаково важны. Старый форум, которым вы не пользуетесь, и аккаунт для управления платежами или рабочими документами требуют разного внимания. Если сервис больше не нужен, выясните, можно ли удалить аккаунт или заменить устаревший адрес. Если аккаунт важен, но доступ к нему утрачен, воспользуйтесь официальной процедурой восстановления. Никому не сообщайте коды из писем, даже если собеседник представляется сотрудником поддержки.

Проверьте и обратную связь: не указан ли этот адрес как резервный для другой почты. Такая схема может быть полезной, если способы восстановления действительно независимы. Но если ко второму адресу можно получить доступ только через первый, это не резерв, а замкнутый круг.

Карта связей должна описывать устройство системы, а не хранить секреты. Для каждого важного аккаунта укажите название сервиса, роль почтового адреса, другие способы входа и восстановления, наличие дополнительного подтверждения и дату проверки. Не записывайте туда пароли, одноразовые и резервные коды. Если вы уже ведёте карту важных аккаунтов, добавьте в неё почту как отдельный узел и укажите, от каких сервисов зависит она сама.

### **Как проверять связь, а не только наличие адреса**

Войдите в каждый важный сервис привычным и безопасным способом. Найдите разделы, посвящённые безопасности, входу, контактными данным и восстановлению доступа.

Названия пунктов могут меняться, поэтому ориентируйтесь на текущий интерфейс сервиса, а не на старую инструкцию из письма или поисковой выдачи.

Проверьте, какой адрес указан сейчас и подтверждён ли он. Выясните, используется ли почта для входа, уведомлений, восстановления или сразу для нескольких целей. Посмотрите, какие ещё способы доступны: номер телефона, приложение для подтверждения входа, резервные коды, обращение в поддержку или проверка личности. Не делайте вывод только по тому, что сервис присылает чеки на почту: финансовое уведомление не означает, что пароль можно сбросить тем же способом.

Отдельно проверьте вход через внешнюю учётную запись. Некоторые сервисы позволяют авторизоваться через стороннюю систему идентификации. Тогда почта может быть указана в профиле, но доступ зависит ещё и от этого способа. Зафиксируйте обе связи. Если вы перестанете пользоваться внешним входом или потеряете доступ к связанной учётной записи, нужно будет понять, как войти иначе и изменить настройки. Не отключайте единственный рабочий способ входа, пока не убедитесь, что у аккаунта есть другой.

На проверку одного сервиса уйдёт несколько минут, зато вы избавитесь от распространённого заблуждения: «адрес привязан — значит, всё восстановится через почту». Иногда так и есть. Иногда почта нужна только для уведомлений, а иногда она лишь один из факторов. Для карты достаточ-

но короткой записи: «адрес — уведомление и восстановление; телефон — подтверждение; вход через внешнюю учётную запись; проверено сегодня». Важна точность, а не подробность.

Выберите три аккаунта, потеря которых сильнее всего помешала бы повседневным делам. Это могут быть основная почта, личный кабинет банка и рабочее хранилище документов — или другой набор, подходящий именно вам. Для каждого ответьте на четыре вопроса: для чего нужна почта, какие ещё способы входа доступны, куда направляется восстановление и какие сеансы остаются активными. Если на что-то не удаётся ответить, не тревожьтесь: просто добавьте этот пункт в план проверки.

Связи не всегда очевидны. Например, уведомление об изменении пароля приходит на почту, а для восстановления нужно ещё подтвердить действие по телефону. Или магазин принимает адрес как логин, но перед сбросом пароля просит проверить несколько сведений. Такие детали влияют на последствия. Поэтому в карте лучше написать «восстановление через почту, затем дополнительное подтверждение», а не просто «почта связана».

### **Почта под собственной защитой**

Прежде чем проверять множество связанных сервисов, укрепите сам почтовый аккаунт. Не обязательно в тот же вечер менять настройки во всех приложениях. Сначала убедитесь, что никто посторонний не сможет войти в почту и что

вы сами сумеете восстановить доступ.

Начните с контактов восстановления. Проверьте, что указаны ваш актуальный номер и резервный адрес, которыми вы действительно можете пользоваться. Старый номер уже мог перейти другому человеку, а резервная почта — оказаться заброшенной или зависеть от основного ящика. Обновите устаревшие контакты по официальной процедуре и убедитесь, что изменения подтверждены. Не удаляйте последний доступный способ восстановления, пока новый не заработал.

Затем проверьте способы входа. Для почты нужен пароль, который не повторяется на других сайтах. О том, как придумывать и хранить такие пароли без лишней нагрузки на память, поговорим дальше. Здесь достаточно запомнить правило: пароль почты должен быть уникальным. Если есть основания считать, что он раскрыт или повторяется, замените его на новый.

Включите дополнительное подтверждение входа, если почтовый сервис его поддерживает. Варианты различаются: приложение для генерации кодов, подтверждение на доверенном устройстве, аппаратный ключ или СМС. Выберите способ, которым сможете воспользоваться даже при потере основного телефона. Если сервис позволяет, настройте запасной вариант. СМС может быть удобным решением, но номер зависит от сохранности сим-карты и контроля над ним. Это не причина отказываться от дополнительной защиты, а повод проверить резервные способы.

Если сервис выдаёт резервные коды для входа, сохраните их отдельно от почтового ящика. Не оставляйте единственную копию в письме, доступ к которому эти коды помогают восстановить. Хранить их можно в закрытом физическом месте или защищённом хранилище с независимым способом доступа. Не фотографируйте коды и не пересылайте их другим людям.

Теперь проверьте устройства и активные сеансы. Сеанс — это уже выполненный вход, который позволяет приложению или браузеру продолжать работу без повторного ввода пароля при каждом действии. В списке могут оказаться старый телефон, домашний компьютер, планшет или незнакомый браузер. Сведения в таких списках не всегда точны: местоположение может быть приблизительным, а модель устройства — обозначена непривычно. Оценивайте признаки вместе и подумайте, узнаете ли вы сам вход.

Если устройство явно потеряно или вам не знакомо, завершите соответствующий сеанс. Если сомневаетесь, сначала смените пароль с устройства, которому доверяете, а затем снова проверьте список. Не рассчитывайте, что смена пароля автоматически завершит все открытые сеансы: это зависит от сервиса, а некоторые приложения могут остаться подключёнными. Ищите отдельную команду для выхода с других устройств. Учтите, что она завершит и ваши собственные сеансы, поэтому заранее убедитесь, что сможете войти снова.

Осмотрите приложения и другие способы, которым разрешён доступ к почте. Это могут быть почтовые программы на компьютере и телефоне, подключённые приложения, старые настройки получения писем или специальные пароли для программ. Отзовите доступ у того, чем больше не пользуетесь или чего не узнаете. Для знакомого рабочего приложения проверьте, нужно ли оно ещё. Не удаляйте всё подряд: сначала убедитесь, что сможете вернуть доступ к нужной программе официальным способом.

Особое внимание уделите переадресации и правилам обработки писем. В настройках может быть указан адрес для автоматической пересылки или фильтр, который перемещает, помечает либо удаляет сообщения. Проверьте, что вы сами включили эти правила и понимаете, как они работают. Неизвестная переадресация или фильтр, скрывающий предупреждения о входе, — повод отнести к ситуации серьёзно: удалите настройку, завершите незнакомые сеансы и смените пароль с надёжного устройства. Загляните и в отправленные письма — нет ли там сообщений, которых вы не отправляли.

Почта может быть открыта на нескольких домашних устройствах, в рабочей программе и в браузере на общем компьютере. Отметьте для себя, какие входы принадлежат вам. Если устройство продано, потеряно или больше не используется, удалите его из списка доверенных и завершите сеанс, если это возможно. На общем компьютере обязательно

но выйдите из аккаунта и не сохраняйте пароль. Просто закрыть окно браузера может быть недостаточно.

### **Три ситуации с разными последствиями**

Рассмотрим три условных случая. Они не предсказывают, что непременно случится при потере доступа к почте, а показывают, почему её нужно проверять в контексте других сервисов.

Интернет-магазин. Адрес используется как логин, на него приходят чеки и сообщения о доставке. Пароль можно восстановить через почту, но для изменения платёжных данных магазин дополнительно просит подтвердить действие. Если почтовый ящик защищён, один лишь доступ к нему не обязательно даст постороннему полный контроль над аккаунтом. Но возможность читать уведомления и запустить сброс пароля всё равно делает эту связь важной. Проверьте, какие действия доступны после входа, для каких требуется дополнительное подтверждение и можно ли завершить активные сеансы в магазине.

Банковский или государственный аккаунт. На адрес могут приходить уведомления, выписки и сообщения о событиях, тогда как вход и восстановление зависят от приложения, номера телефона, проверки данных, личного обращения или другого способа. Доступ к почте не равен автоматически доступу к деньгам или государственным услугам. Откройте официальный сайт или приложение и проверьте, как устроены вход и восстановление именно в вашей учётной за-

писи. Если адрес указан давно, а номер телефона изменился, обновляйте контакты по правилам сервиса и не переходите по ссылкам из подозрительных сообщений.

**Рабочая почта.** Если ящик нужен для документов, переписки с клиентами и входа в рабочие системы, его значение выходит за рамки личных данных. Доступ могут иметь несколько сотрудников или администратор, а порядок восстановления — зависеть от настроек организации. Если критичные параметры контролирует организация, не меняйте их в одиночку. Уточните у администратора, какие устройства и приложения подключены, кто получает уведомления о безопасности и как восстановить аккаунт при увольнении или потере устройства. Личный резервный адрес сотрудника не должен быть единственной опорой для общего рабочего доступа.

Во всех трёх случаях полезно задать одни и те же вопросы: что позволяет сделать почта в этом сервисе, какое подтверждение потребуется дополнительно, кому придёт предупреждение и какие сеансы останутся открытыми. Ответы помогут расставить приоритеты. Аккаунт, который только присылает рекламные письма, обычно не требует такого же срочного внимания, как тот, через который меняют контактные данные или управляют важными документами.

**Порядок действий, если почта используется повсюду**

Если один адрес указан в десятках сервисов, может захо-

теться обойти их все и сразу везде заменить контакты. Но начинать стоит с почты: пока центральный узел плохо защищён, добавление новых связей не уменьшит риск. Сначала укрепите его, затем проверьте самые важные ответвления.

В обычной ситуации действуйте так. Убедитесь, что можете войти в почту и восстановить доступ через актуальные контакты. Замените повторяющийся или сомнительный пароль на уникальный, включите дополнительное подтверждение и сохраните резервные коды отдельно. Затем проверьте сеансы, устройства, подключённые программы, переадресацию и правила обработки писем. Завершите неизвестные входы и отзовите ненужные разрешения. После этого переходите к важным связанным аккаунтам — в первую очередь к тем, потеря которых затруднит работу, расчёты или доступ к другим сервисам.

Если признаков постороннего доступа нет, аудит можно разбить на несколько коротких подходов. Сначала проверить почту и контакты восстановления, затем — финансовые и государственные сервисы, а после — покупки, документы и рабочие системы. Отмечайте в карте не только найденное, но и то, что осталось неясным. Пометка «уточнить способ восстановления» полезнее догадки, записанной как факт.

Если вы заметили неизвестные входы, изменённые контакты, чужие сообщения в отправленных или незнакомую переадресацию, действуйте так, словно доступ мог быть скомпрометирован. Возьмите устройство, которому доверя-

ете, смените пароль почты, завершите другие сеансы, проверьте способы восстановления и удалите неизвестные настройки. Затем свяжитесь с поддержкой почтового сервиса через официальный сайт или приложение и проверьте самые важные связанные аккаунты. Если есть риск заражения устройства или доступ к почте уже утрачен, не вводите новые пароли на подозрительном устройстве. Зафиксируйте время и характер событий, но не сообщайте коды подтверждения тем, кто предлагает «быстро вернуть» аккаунт.

Если связанных сервисов много, не пытайтесь сразу составить идеальную карту. Начните с короткого списка: почта, банк, государственные услуги, мобильная связь, рабочие документы и аккаунты, через которые можно восстановить другие важные учётные записи. Остальные добавляйте по мере необходимости. Проверяйте адреса, номера и способы входа, когда меняете телефон или отказываетесь от старой почты. Устаревшая связь может помешать законному владельцу восстановить доступ.

Если вы давно используете один адрес для всего, это не значит, что нужно срочно создавать несколько новых ящиков и переносить туда все сервисы. Дополнительный адрес полезен только в том случае, если вы готовы регулярно защищать его и поддерживать в актуальном состоянии. Иначе он станет ещё одним забытым аккаунтом. Надёжная система — не та, в которой больше адресов, а та, где вы знаете, за что отвечает каждый из них и как восстановить к нему доступ.

После проверки почта должна занять заметное место на карте зависимостей. Укажите не только связанные сервисы, но и то, на что опирается сам почтовый аккаунт: актуальный номер, резервный адрес, второй фактор, доверенные устройства и способ получения кодов. Отметьте отдельно, что единственная копия кодов восстановления не хранится в самой почте. Так карта покажет не просто связи, но и возможные круги зависимости.

Вместо общего вопроса «насколько надёжно выглядит мой адрес» проверьте несколько практических вещей: можете ли вы войти с доверенного устройства, актуальны ли контакты восстановления, узнаете ли вы все активные сеансы, нет ли неизвестной переадресации и понятно ли, как восстановить важные связанные аккаунты. Ответы превратят тревожное предположение в конкретный план.

Почта хранит переписку и одновременно помогает управлять доступом к другим сервисам. Поэтому сначала защитите её как самостоятельный аккаунт, а затем отметьте на карте все найденные зависимости. Когда связи понятны, следующий шаг очевиден: защитить сами пароли так, чтобы утечка одного сервиса не открывала остальные.

# **Пароли без повторов и мучительной памяти**

Один и тот же пароль кажется удобным, пока не выясняется, что он связывает аккаунты, которым лучше оставаться независимыми. Почта, личный кабинет банка, Госуслуги и забытый интернет-магазин — разные двери, но повторяющийся ключ превращает их в одну связку. Поэтому после того, как вы определили самые важные аккаунты и проверили способы восстановления доступа, следующий шаг — не выучить десятки секретов, а перестать использовать один и тот же пароль в нескольких местах.

## **Один пароль связывает независимые аккаунты**

Утечка данных с небольшого сайта не обязательно означает, что пароль попадёт к злоумышленнику в готовом виде. Сервис мог хранить его в защищённом виде, инцидент мог затронуть лишь часть пользователей, а данные могли устареть. Но если сочетание адреса электронной почты и пароля всё же стало доступно, его можно автоматически проверить на других популярных сервисах. Такой способ называют подстановкой учётных данных: программа проверяет уже известные пары «логин — пароль» в надежде, что пользователь повторил их.

Здесь не нужно угадывать пароль или взламывать каждый

аккаунт по отдельности. Достаточно найти пароль в одном месте и проверить его в других. Если он совпадает, неважно, что сайты принадлежат разным организациям и не передают друг другу сведения. Связь между ними создал сам пользователь.

Представьте цепочку: один и тот же адрес электронной почты и пароль использовались для регистрации на форуме, в интернет-магазине и в личном кабинете, связанном с важными делами. Форум сообщает об утечке. Злоумышленник проверяет найденное сочетание на других сервисах. Если ему удаётся войти в почту, он может попытаться сбросить пароли на площадках, где этот адрес указан для восстановления. Одного повтора достаточно, чтобы локальная проблема стала цепочкой.

Уникальный пароль не отменяет всех рисков: аккаунт всё ещё может пострадать от фишинга, заражённого устройства, слабого восстановления доступа или ошибки самого сервиса. Но такой пароль не откроет автоматически остальные двери. Уникальность ограничивает ущерб: секрет, раскрытый на одном сайте, не подойдёт к другим.

Особенно опасно повторять пароль для почты и аккаунтов, которые зависят от неё при восстановлении доступа. Почта часто получает ссылки или коды для сброса пароля. Если вход в неё защищён тем же секретом, что и менее важный сайт, этот сайт фактически может стать обходным путём к почтовому ящику. Поэтому пароль почты должен быть от-

дельным и нигде больше не использоваться.

Повтором считается не только полное совпадение. Если один пароль заканчивается текущим годом, другой — прошлым, а третий содержит название сервиса, это всё ещё предсказуемое семейство вариантов. Обнаружив один образец, злоумышленник может проверить и похожие. Замена одной буквы цифрой или добавление восклицательного знака в конце обычно не создают нового, независимого секрета.

Это не повод стыдиться старых привычек или менять всё за один вечер. Повтор паролей появился не на пустом месте: аккаунтов много, а память у человека одна. Решение должно облегчить задачу — иначе легко вернуться к прежней схеме. Рассмотрим три подхода, которые чаще всего кажутся разумными.

### **Три системы хранения**

Можно повторять один пароль или несколько похожих, запоминать разные фразы либо доверить хранение менеджеру паролей. Первый вариант экономит усилия, второй нагружает память, третий требует защитить хранилище и продумать восстановление доступа.

### **Повторяющийся пароль**

Преимущество очевидно: не нужно искать запись или вспоминать, какой вариант использован. Для одного неважного аккаунта повтор может показаться безобидным. Но пользователь обычно не помнит все места, где применял пароль, а сайты со временем меняют правила входа и восста-

новления. Даже забытый старый аккаунт может годами хранить сочетание «почта — пароль», которое окажется полезным злоумышленнику.

Если вы подозреваете, что повторяли пароль, не нужно сначала разыскивать все регистрации за всю жизнь. Защитите прежде всего самые важные точки: основную почту, аккаунты, через которые можно восстановить доступ к другим сервисам, финансовые кабинеты и другие учётные записи, потеря которых серьёзно осложнит повседневные дела. Задайте для каждой свой пароль, а с менее значимыми аккаунтами разберётесь позже.

### **Запоминаемые фразы**

Разные фразы лучше одного повторяющегося пароля, если они не составлены по одному простому шаблону. Человеку проще запомнить несколько слов, чем случайную последовательность букв и знаков. Но словесная форма сама по себе ещё не делает пароль надёжным.

Фраза из названия любимого фильма, имени питомца и года рождения может казаться личной и потому непредсказуемой. На деле такие сведения порой открыты в профилях, публикациях или материалах, доступных знакомым. Популярные цитаты и очевидные сочетания тоже легко перебрать автоматически.

Если вам нужно придумать фразу, которую предстоит вводить вручную и помнить, выберите несколько несвязанных слов случайным образом. Не используйте личные фак-

ты, известные цитаты и одну и ту же схему для разных сервисов. Четыре или больше случайно выбранных слова могут составить длинную фразу, но само число слов не гарантирует надёжность: важны и случайность выбора, и уникальность для конкретного аккаунта. Если сервис ограничивает длину или запрещает пробелы, подстройте фразу под его правила, не добавляя предсказуемо название сайта или текущий год.

Такой способ удобен для небольшого числа секретов, например для главного пароля менеджера. Но для десятков аккаунтов он быстро превращается в задачу на память: приходится использовать похожие варианты или записывать фразы. Если записи всё равно необходимы, специализированное хранилище обычно удобнее и безопаснее случайных замечаний.

## **Менеджер паролей**

Менеджер паролей хранит учётные данные в защищённом хранилище. Для каждого сервиса он может создать отдельный случайный пароль и подставить его при входе. Пользователю не нужно запоминать десятки наборов символов — важно уметь безопасно получать доступ к самому хранилищу.

Менеджер меняет характер задачи. Вместо вопроса «Как придумать и запомнить ещё один пароль?» возникает другой: «Как защитить главное хранилище и не потерять к нему доступ?». Риск не исчезает, а сосредотачивается в одном месте. Хорошо настроенный менеджер помогает не повторять

пароли, но сам по себе не защитит от любого обмана или заражённого устройства.

Менеджер также может сопоставлять сохранённые данные с адресом сайта и предлагать их для входа. Это полезная подсказка, но она не отменяет осторожности: проверьте, что открыта нужная страница, а приложение или расширение установлено из официального источника. Не входите в хранилище по подозрительной ссылке из письма или сообщения.

### **Длина, уникальность и предсказуемые замены**

Пароль оценивают не по тому, насколько сложно его набрать, а по тому, насколько трудно угадать. Важны две характеристики: длина и непредсказуемость. Чем длиннее случайная последовательность, тем больше вариантов нужно перебрать. Но длинная фраза из очевидных слов может оказаться слабее короткого случайно сгенерированного пароля. А даже очень надёжный секрет теряет смысл, если его повторяют.

Замена букв похожими цифрами — не надёжный способ сделать пароль случайным. Схемы вроде «заменить букву цифрой, добавить знак в конце и год» давно предсказуемы. Они могут соответствовать требованиям сайта к разным типам символов, но не обеспечивают той же защиты, что случайный выбор. Если сервис требует заглавную букву, цифру и специальный знак, настройте генератор на эти условия, а не маскируйте знакомое слово вручную.

Для пароля, созданного менеджером, разумный ориентир

— 16 символов и больше, если сервис их принимает. Это не универсальная граница безопасности: один сайт может ограничивать длину, другой — запрещать часть символов. Выберите максимально длинный вариант, который сервис принимает без проблем, и обязательно делайте его уникальным. Если пароль приходится вводить вручную, длинная случайная фраза может оказаться удобнее набора знаков.

Перед сохранением проверьте, что пароль не содержит очевидный шаблон — например, название сайта, имя пользователя или текущий год — и не повторяет секрет, уже использованный для другого аккаунта. Менеджер может сгенерировать новый пароль автоматически; запоминать его не потребуется.

## **Как выбрать хранилище**

Менеджеры паролей различаются способом хранения данных, синхронизацией, восстановлением доступа и работой на разных устройствах. Не стоит выбирать хранилище только по громкому обещанию «самого надёжного». Сначала ответьте на несколько практических вопросов.

Совместимость. Сможете ли вы открыть хранилище на своих устройствах и при обычном подключении к сети в России? Проверьте, есть ли приложение или веб-версия для устройств, которыми вы действительно пользуетесь. Если вы входите с телефона и компьютера, неудобная совместимость быстро подталкивает к повторному использованию паролей.

Защита данных. Найдите в официальной документации

объяснение, шифруются ли данные и где именно это происходит. Одни решения шифруют хранилище на устройстве до синхронизации, другие могут работать иначе. Не полагайтесь только на рекламные формулировки: важно понимать, что произойдёт, если возникнет проблема с сервером сервиса или вашим устройством.

Восстановление доступа. Что случится, если вы забудете главный пароль или потеряете телефон? Уточните, есть ли запасной способ входа, какие данные понадобятся для восстановления и может ли служба поддержки вернуть доступ. В некоторых хранилищах главный пароль нельзя восстановить через поддержку. Это помогает не допустить чтения содержимого посторонними, но означает, что забытый секрет может закрыть доступ и владельцу.

Перенос данных. Выясните, синхронизируется ли хранилище и как устроено резервное копирование. Если возможен экспорт, узнайте, в каком виде создаётся файл. Незашифрованный экспорт может содержать все пароли обычным текстом. После переноса его нельзя оставлять в папке загрузок, электронной почте или облачном хранилище без дополнительной защиты.

Вход на сайты. Посмотрите, распознаёт ли менеджер адрес страницы и предлагает ли нужную запись, можно ли отключить автозаполнение или настроить автоматическую блокировку. Чем проще соблюдать безопасные правила в обычный день, тем вероятнее, что вы будете им следовать.

Разработчик и установка. Устанавливайте приложение или расширение из официального источника, проверяйте имя разработчика и наличие обновлений. Не храните пароли в неизвестном дополнении, найденном по случайной ссылке. Если вы находитесь в России, учитывайте также, доступен ли сервис и его поддержка в тех условиях, в которых вы собираетесь им пользоваться.

Перед переносом всех данных проведите небольшой тест. Создайте запись для неважного аккаунта, проверьте вход на втором устройстве, заблокируйте хранилище и откройте его снова. Затем разберитесь, как восстановить доступ при потере телефона. Если процесс оказался запутанным, лучше выяснить это на пробной записи, а не в момент, когда срочно понадобится войти в почту или финансовый кабинет.

### **Главный пароль — ключ к хранилищу**

Главный пароль менеджера должен быть уникальным. Не используйте для него пароль от почты, банковского кабинета или любого другого сервиса. Если он повторяется, утечка в другом месте может поставить под угрозу всё хранилище.

Этот пароль предстоит помнить, поэтому подойдёт длинная фраза из нескольких случайных, не связанных друг с другом слов. Не стройте её на дате, имени, любимой цитате или очевидном сочетании слов. Если менеджер умеет создавать случайные словесные фразы, воспользуйтесь этой функцией. Если выбираете слова сами, не берите их из личных сведений и не используйте такую же конструкцию для

других важных паролей.

Не сохраняйте главный пароль в том же менеджере, который он открывает. Если для восстановления нужен дополнительный код или файл-ключ, храните его отдельно от устройства с менеджером. Бумажную запись можно оставить дома в защищённом месте, недоступном посторонним. Не носите её вместе с телефоном и не прикрепляйте к устройству.

Заранее решите, что будете делать, если потеряете устройство. Например, доступ к хранилищу может синхронизироваться с другим вашим устройством, а резервная копия — храниться отдельно и быть зашифрованной. Не создавайте незашифрованный список паролей «на всякий случай». Если менеджер предлагает резервное восстановление, выясните, какие секреты для этого нужны и кто сможет получить к ним доступ.

Сохраните отдельно сведения о восстановлении самого менеджера, не смешивая их с паролями, которые они должны защищать. Если для восстановления используется почта, её пароль тоже должен быть уникальным и надёжным. Восстановление — не мелкая техническая деталь: от него зависит, сможете ли вы вернуть доступ и не станет ли этот путь слабым местом всей системы.

Не вводите главный пароль в форму, открытую по неожиданной ссылке. Запустите приложение самостоятельно или перейдите по сохранённому правильному адресу. Менеджер снижает риск повторного использования паролей и помога-

ет заметить несоответствие сайта, но всё равно нужно проверять, куда именно вы вводите главный секрет.

## **Общие устройства и границы доступа**

На личном телефоне или компьютере защищайте хранилище паролем учётной записи устройства, блокировкой экрана и автоматической блокировкой самого менеджера. Если устройство остаётся открытым, другой человек может воспользоваться уже разблокированными приложениями, даже не зная главного пароля.

Если одним компьютером пользуются несколько членов семьи, заведите каждому отдельную учётную запись в операционной системе. Не сохраняйте пароли в общем профиле браузера и не оставляйте менеджер открытым. Общий планшет с единой учётной записью — не личное устройство: автозаполнение может предложить ваши данные тому, кто возьмёт планшет следующим.

На чужом или общественном компьютере не открывайте менеджер и не соглашайтесь сохранять пароль в браузере. Режим приватного просмотра не делает устройство доверенным: он может не сохранять историю, но не исключает установленную программу для записи нажатий клавиш или чужой доступ к системе. Если вам пришлось войти в важный аккаунт с чужого устройства, выйдите из него, а позже с личного устройства завершите активный сеанс, если сервис это позволяет.

Рабочее устройство может контролироваться организаци-

ей и администратором. Следуйте правилам работодателя: не переносите корпоративные пароли в личный менеджер, если для них предусмотрено отдельное хранилище, и не сохраняйте личные данные в общедоступном рабочем профиле. Важно не только выбрать надёжную программу, но и понимать, кто имеет доступ к самому устройству.

## **Переход без генеральной уборки**

Начните не с полного списка всех регистраций, а с аккаунтов, потеря которых сильнее всего повлияет на вашу жизнь. Приоритеты у всех разные, но обычно в первую очередь стоит проверить основную почту, учётные записи с финансовыми операциями, важные государственные и рабочие сервисы, а также аккаунты, через которые можно восстановить доступ к другим.

Переход удобнее провести в несколько этапов.

Сначала выберите способ хранения. Если остановились на менеджере, установите его из официального источника и проверьте на пробной записи, как он работает на ваших устройствах. Если пока не готовы пользоваться менеджером, придумайте отдельные длинные фразы для небольшого числа самых важных аккаунтов. Не считайте похожие варианты уникальными.

Затем создайте главный пароль, подготовьте безопасный план восстановления и проверьте, как блокируется хранилище. Не переходите к массовой смене паролей, пока не убедитесь, что можете открыть менеджер и восстановить к нему

доступ.

После этого меняйте пароли по одному. Начните с почты и аккаунтов, связанных с восстановлением доступа к другим сервисам. Для каждого создайте новый уникальный пароль и сразу сохраните его, чтобы не полагаться на память. После смены убедитесь, что новый пароль работает и актуальные способы восстановления доступны вам.

Наконец, постепенно устранили старые повторы. Если пароль использовался в нескольких местах, а вы не помните во всех ли, сосредоточьтесь на важных и действующих аккаунтах. Меняя пароль в очередном сервисе, не переносите туда прежний секрет в слегка изменённом виде. Если вы получили достоверное уведомление о компрометации, ввели пароль на поддельной странице или сохранили его на недоверенном устройстве, смените его сразу, не дожидаясь очереди.

Результат этой работы — не идеально заполненное хранилище и не рекордное количество символов. Важно, чтобы у каждого ценного аккаунта был свой пароль, вы знали, как открыть хранилище, и понимали, как восстановить доступ. Новые регистрации можно будет добавлять по мере необходимости — без многодневной генеральной уборки.

Уникальные пароли уменьшают вероятность того, что проблема одного сайта распространится на почту, финансы или другие важные аккаунты. Но пароль — лишь один замок: его могут выманить, а устройство — потерять или скомпрометировать. Следующий уровень защиты добавляет ещё

одно подтверждение входа, чтобы украденного секрета оказалось недостаточно.

## **Второй фактор — второй замок**

Уникальный пароль не даст утечке в одном сервисе открыть другой аккаунт, а защищённая почта поможет не потерять доступ к остальным. Но даже хороший пароль можно украсть через поддельную страницу входа, выманить под видом проверки или получить из базы самого сервиса.

При обычном входе второй фактор — это дополнительное подтверждение после пароля. Резервный способ восстановления доступа нужен на случай, если привычный способ входа недоступен, например телефон потерян. Это отдельный путь, а не ещё один фактор, который сервис проверяет при каждом входе. Резерв тоже нужно защищать: если его получит посторонний, он может воспользоваться им вместо вас. Ни второй фактор, ни резерв не отменяют необходимости проверять запросы и не поддаваться на уговоры передать код.

Для примера возьмём личную почту. Аккаунт не самый эффектный, зато через него часто восстанавливают доступ к другим сервисам. Рассмотрим три ступени: вход только по паролю, вход с дополнительным подтверждением и, наконец, заранее подготовленный резервный способ. Важно: третья ступень помогает не потерять доступ, но сама по себе не добавляет защиту к каждому обычному входу.

### **Пароль на испытании**

На первой ступени у аккаунта есть уникальный пароль. Это хорошая основа: если данные для входа в другой сервис утекли, автоматически использовать их здесь уже не получится. Но уникальность не защищает от всех способов кражи.

Пароль могут перехватить на поддельной странице, похожей на настоящую форму входа, или записать вредоносной программой на заражённом устройстве. Он может утечь при взломе самого сервиса. Наконец, пользователь может сам ввести его на странице из неожиданного письма. Бывает и так, что пароль не крадут вовсе, а получают доступ к уже открытому сеансу — например, похищают данные, которые позволяют продолжить вход без повторного ввода пароля.

В этой модели пароль — единственная проверка. Если он попал к постороннему, сервису может быть достаточно его предъявить. Иногда при входе с нового устройства или из непривычного места сервис задаёт дополнительные вопросы. Но рассчитывать на такую проверку как на постоянную защиту нельзя: правила у разных сервисов отличаются и могут меняться.

Добавим второй фактор — дополнительное доказательство права на вход, например код с устройства, которое находится у пользователя. При обычном входе сервис сначала проверяет пароль, затем просит подтвердить его ещё одним способом. В большинстве таких сценариев украденного пароля недостаточно: злоумышленнику понадобится также

средство подтверждения.

Аккаунт не становится неприступным, но задача для атакующего усложняется. Массовая проверка украденных паролей уже не всегда приводит к входу, а случайно найденного в старой переписке пароля может не хватить. Второй фактор особенно полезен, если злоумышленник получил пароль, но не контролирует средство подтверждения или способы восстановления доступа.

Однако второй фактор закрывает не все угрозы. Если вредоносная программа контролирует устройство, пользователь вводит пароль и код на поддельной странице, похищен активный сеанс или захвачен используемый канал подтверждения, например номер телефона для SMS, защита может не сработать. Правильный вывод не в том, что с кодом можно больше ни о чём не беспокоиться. Второй фактор снижает риск, но не отменяет внимательности и не гарантирует защиту от социальной инженерии.

### **Лестница из трёх ступеней**

Первая ступень — только пароль. Он должен быть уникальным и достаточно сложным, но остаётся единственным ключом. При утечке или обмане этого ключа злоумышленник может сразу войти в аккаунт.

На второй ступени к паролю добавляется подтверждение при обычном входе. Теперь нужно пройти две проверки. Дополнительный способ должен быть доступен вам, но не попадать в ту же точку риска, что и пароль. Если пароль и прило-

жение с кодами находятся на одном незапертом устройстве, его потеря может поставить под угрозу оба средства доступа.

Третья ступень — пароль, дополнительное подтверждение при обычном входе и заранее подготовленный резервный способ восстановления доступа. Он нужен вам, если телефон сломается, потеряется, сбросится или сменится. Такой резерв не заменяет второй фактор и не повышает защиту каждого обычного входа: он помогает владельцу вернуться в аккаунт, когда привычное подтверждение недоступно. При этом резервный код или другой запасной путь тоже может стать целью злоумышленника.

Большинство неудобств возникает не при включении второго фактора, а позже — в поездке, после ремонта телефона или при входе с нового устройства. Поэтому важно проверить не только защиту обычного входа, но и то, как вы восстановите доступ, если основной способ подтверждения исчезнет.

## **Выбор способа подтверждения**

Набор вариантов для обычного входа зависит от сервиса. В настройках могут быть коды из приложения, SMS, подтверждение в приложении сервиса или физический ключ безопасности. Некоторые сервисы также предлагают ключ доступа — он может быть самостоятельным способом входа, а не дополнительным фактором поверх пароля. Резервные коды и восстановление через поддержку относятся к запасным путям, а не к обычному подтверждению при каждом

входе. Названия и порядок действий различаются, поэтому следуйте подсказкам именно того сервиса, которым пользуетесь.

Приложение для кодов генерирует короткие одноразовые комбинации. После первоначальной настройки они обычно появляются и без подключения к интернету: приложение и сервис рассчитывают код на основе общего секрета и времени. Срок его действия невелик, поэтому такой код нельзя хранить как постоянный пароль.

Приложение не зависит от SMS и обычно работает там, где нет мобильной связи. Но оно привязано к устройству или к предусмотренной для него резервной копии. Если телефон потерян, сброшен или заменён, коды могут исчезнуть вместе с ним. Некоторые приложения позволяют переносить или синхронизировать данные. В таком случае безопасность зависит и от защиты учётной записи, и от способа синхронизации. Не рассчитывайте заранее, что новый телефон автоматически восстановит всё содержимое старого.

С SMS всё проще: код приходит на указанный в настройках номер. Не нужно запускать отдельное приложение, а сама настройка обычно понятна и тем, кто не хочет разбираться в дополнительных программах. Если это единственный доступный вариант, его всё равно лучше включить, чем остаться с одним паролем.

У SMS есть слабые места. Доступ к сообщению зависит от номера и оператора связи. Телефон можно потерять, SIM-

карту — переставить или перевыпустить, а номер — со временем отключить или передать другому абоненту. Возможны и попытки обманом получить контроль над номером или выманить код. Наконец, сообщение может задержаться или не прийти — например, из-за проблем со связью или во время поездки.

Приложение для кодов уменьшает зависимость от телефонного номера, но само по себе не защищает от фишинга. Если пользователь введёт свежий код на поддельной странице, злоумышленник может быстро передать его настоящему сервису и успеть воспользоваться им. Поэтому вводите код только в официальной форме входа, которую открыли самостоятельно, а не по ссылке из неожиданного сообщения.

Некоторые сервисы предлагают подтвердить вход уведомлением на уже подключённом устройстве. Это удобно: иногда достаточно нажать кнопку или сверить появившиеся цифры. Но не одобряйте запрос только потому, что он настойчиво появляется на экране. Если вы не начинали вход, отклоните его. Повторяющиеся уведомления могут быть попыткой утомить пользователя, чтобы он согласился автоматически.

Если сервис поддерживает физический ключ безопасности, он может лучше защищать от поддельных страниц: проверка связана с настоящим адресом сайта, поэтому скопированную форму обычно сложнее использовать для входа. Но ключ можно потерять, и далеко не все сайты и приложения

его поддерживают. Для важного аккаунта можно зарегистрировать второй ключ как запасной фактор для обычного входа и хранить его отдельно. Такой ключ — не то же самое, что процедура восстановления аккаунта. Если сервис предлагает резервные коды или другой способ восстановления, подготовьте его отдельно. Единственный ключ на одной связке с ключом от квартиры — плохой план.

Некоторые сервисы позволяют использовать ключ доступа или входить с помощью биометрии на устройстве. Это может быть не дополнительный код поверх пароля, а самостоятельный способ входа. Часто биометрическая проверка лишь подтверждает, что устройство разблокировал владелец; сервису при этом не обязательно передавать изображение лица или отпечаток. Детали зависят от реализации. Какой бы вариант вы ни выбрали, выясните заранее, что произойдёт при потере устройства и какие способы входа или восстановления останутся.

Не обязательно выбирать самый сложный метод только потому, что он звучит надёжнее. Если приложение с кодами неудобно и есть риск отключить его после первой трудности, доступное подтверждение по SMS может быть практичнее, чем отсутствие второго фактора. Если аккаунт особенно ценен, а сервис поддерживает физический ключ, стоит рассмотреть и его — не забыв зарегистрировать запасной фактор и отдельно подготовить восстановление доступа. Хороший способ защиты — тот, которым вы можете безопасно

пользоваться и который сумеете восстановить.

## **Зависимость между ключом и замком**

Дополнительное подтверждение полезно настолько, насколько защищён канал, по которому оно приходит. Если код для почты отправляется на другой почтовый ящик, доступ к которому восстанавливается через первый, цепочка замыкается. А если на потерянном телефоне без блокировки одновременно хранятся пароль, приложение с кодами и открытая почта, несколько слоёв защиты могут оказаться под угрозой сразу.

Это не значит, что факторы нужно обязательно разнести по разным зданиям. Важно понять, какие средства доступа находятся в одной точке риска. Пароль может храниться в защищённом хранилище, код — в приложении на телефоне, а резервные коды — в отдельном надёжном месте. Такая схема не исключает всех опасностей, но потеря одного устройства не должна автоматически лишать вас каждого пути входа.

Ещё один возможный обходной путь — восстановление аккаунта. Если злоумышленник может сбросить пароль через незащищённую почту или устаревший номер, дополнительный фактор при обычном входе может не помочь. Поэтому после его включения проверьте адреса и номера для восстановления: доступны ли они вам и защищены ли сами. Если речь о рабочей учётной записи, выясните, кто отвечает за восстановление: вы, администратор или служба поддержки организации. Не полагайтесь на догадки вместо рабочих

правил.

Наконец, дополнительное подтверждение не обязательно остановит того, кто уже получил доступ через открытую сессию. Если сервис показывает список устройств и активных сеансов, время от времени просматривайте его и закрывайте незнакомые или старые подключения. При потере телефона отзовите доступ этого устройства, если сервис позволяет. Если есть подозрение на взлом, смените пароль с доверенного устройства и проверьте способы восстановления.

### **Резервный код — не запасной пароль**

Резервные коды — это запасной путь на случай, если обычное подтверждение недоступно. Сервис может разрешить ввести такой код вместо привычного второго фактора. Это не обычный второй фактор, который используется при каждом входе: код заранее выдан для исключительной ситуации и часто действует только один раз. Правила зависят от сервиса. Относитесь к набору как к комплекту запасных ключей: тот, у кого он окажется, может получить доступ к аккаунту.

Сохраните коды сразу, пока вы вошли в аккаунт и телефон под рукой. Не откладывайте на потом: именно при потере устройства выясняется, что файл не скачан, а копии ни у кого нет. Убедитесь, что она открывается и читается, затем поместите её туда, где посторонний не получит коды вместе с телефоном.

Можно распечатать коды и хранить лист в закрытом ме-

сте дома. Другой вариант — защищённое хранилище паролей, если доступ к нему не зависит целиком от того же потерянного телефона. Для особенно важной учётной записи разумно держать один надёжный резерв вне повседневного устройства. Не храните коды открытым текстом в галерее, обычных заметках или переписке с самим собой: содержимое может синхронизироваться, попасть в резервную копию или стать доступным тому, кто разблокировал телефон.

Укажите, к какому аккаунту относятся коды, но не храните рядом пароль и все подсказки к нему. Не отправляйте коды в чат и не пересылайте их на почту, доступ к которой зависит от защищаемого аккаунта. Использованный код отметьте. Если сервис позволяет выпустить новый набор, старые коды могут перестать работать после обновления. Уточните это в инструкции и замените сохранённую копию.

Резервный код и восстановление через поддержку — не одно и то же. Код выдаётся заранее и позволяет пройти предусмотренную сервисом проверку. Обращение в службу поддержки может потребовать дополнительных действий, занять время или закончиться отказом, если данных для проверки недостаточно. Не рассчитывайте, что поддержка гарантированно заменит код. Лучше выяснить правила сервиса до того, как вы окажетесь вне аккаунта.

### **Код не для собеседника**

Одноразовый код легко принять за безобидное подтверждение: цифры короткие, а срок действия небольшой. Но с

его помощью можно войти в аккаунт, изменить настройки или подтвердить конкретную операцию. Всё зависит от текста сообщения и действия, которое вы начали.

Не передавайте код входа, восстановления или подтверждения операции собеседнику — даже если он представляется сотрудником банка, почтового сервиса, государственного портала, оператора связи или службы поддержки. Не диктуйте код по телефону, не отправляйте в сообщении и не показывайте во время демонстрации экрана. Вводить его нужно только самостоятельно — в официальном окне той операции, которую вы начали.

Если звонок или сообщение застали врасплох, завершите разговор и откройте сервис привычным способом: через установленное приложение или самостоятельно набрав адрес. Не переходите по присланной ссылке и не устанавливайте приложение для удалённого доступа по просьбе собеседника. Чтобы проверить информацию, найдите официальный канал связи сами. Особенно важно это при разговоре о банковских операциях: код может подтверждать не «личность для разговора», а перевод, вход или изменение настроек.

Если код пришёл без вашего запроса, это ещё не означает, что аккаунт уже взломан. Кто-то мог ошибиться номером или только начать попытку входа. Но пересылать код человеку, который просит его «отменить» или «проверить», нельзя. Отклоните неожиданный запрос на подтверждение, не вводите код и проверьте входы и настройки аккаунта. Если за-

метили признаки чужого доступа, смените пароль с доверенного устройства, завершите незнакомые сеансы и проверьте контактные данные для восстановления.

## **Смена телефона без закрытой двери**

Перенос доступа лучше спланировать, пока старый телефон ещё работает. Сначала выясните, какие способы подтверждения подключены к важным аккаунтам и можно ли добавить новое устройство, не удаляя прежнее. Затем подготовьте резервные коды и убедитесь, что восстановление не завязано на номер или почту, от которых вы скоро откажетесь.

Перенесите доступ до сброса или передачи старого телефона. Если сервис разрешает подключить приложение с кодами на новом устройстве, выполните перенос по официальной инструкции. Проверьте вход на новом телефоне, пока старый способ ещё доступен. Подключили новый фактор — сначала убедитесь, что он работает, и только потом удаляйте прежний.

Не проверяйте готовность плана, выходя из единственного активного сеанса. Оставьте его открытым, настройте новый способ, сохраните резервные коды и, если это безопасно и допускается сервисом, попробуйте войти через отдельное окно или другое доверенное устройство. Не закрывайте последнюю работающую сессию, пока не убедитесь, что новый вход и резервный способ доступны.

При смене номера сначала обновите его в важных аккаун-

тах и только после этого отказывайтесь от старой SIM-карты. Если прежний номер уже недоступен, не пытайтесь наугад перебрать варианты восстановления. Следуйте официальной процедуре возврата доступа. При потере SIM-карты или телефона свяжитесь с оператором через официальный канал и уточните, как заблокировать номер или выпустить новую SIM-карту. С рабочей почтой обратитесь к администратору организации, с банковским доступом — в банк по контакту, который нашли самостоятельно.

При утрате устройства по возможности заблокируйте его или выполните удалённый выход, а при потере SIM-карты свяжитесь с оператором. Если обычный способ подтверждения больше недоступен, воспользуйтесь заранее подготовленным резервным путём или официальной процедурой восстановления. После входа завершите сеансы потерянного телефона и проверьте, не изменились ли пароль, номер, почта для восстановления и подключённые факторы. Если есть основания считать, что посторонний видел пароль, смените его. Для банковских и других финансовых сервисов отдельно проверьте операции и сообщите организации о незнакомых действиях.

## **Выбор одного аккаунта**

Чтобы воспользоваться этой лестницей, не нужно сегодня менять все цифровые привычки. Выберите аккаунт, потеря которого осложнит важные дела или восстановление других доступов. Часто разумно начать с личной почты, если че-

рез неё сбрасываются пароли. Если на почте уже настроено надёжное дополнительное подтверждение, следующим кандидатом может стать банковский кабинет, государственный сервис или рабочий аккаунт с доступом к важным данным. Настройки у каждого сервиса свои — ищите их в официальном приложении или на сайте, который открыли самостоятельно.

Действуйте последовательно. Найдите раздел безопасности и входа, выберите поддерживаемый сервисом способ подтверждения и убедитесь, что готовы им пользоваться. Если вариантов несколько, оцените не только удобство, но и зависимость от телефона, номера и другого аккаунта. Отдельно выясните, какие резервные способы восстановления предлагает сервис, и сохраните резервные коды, если они доступны. Проверьте, что сможете прочитать их без основного телефона. Затем проверьте обычный вход, не закрывая единственную действующую сессию.

Перед тем как закончить, ответьте себе на три практических вопроса: что понадобится при входе с нового устройства, где хранится резервный код или запасной фактор и что вы сделаете, если телефон потеряется сегодня? Сложных ответов не требуется. Достаточно знать, куда обратиться, где найти резерв и как отозвать доступ потерянного устройства.

Если выбранный сервис не поддерживает дополнительное подтверждение, не пытайтесь подключить его самостоятельно и не доверяйте стороннему сайту, который обещает

«усилить защиту». Уникальный пароль, защищённые способы восстановления, уведомления о входе и проверка активных сеансов всё равно полезны. А для второго фактора выберите другой важный аккаунт, где он доступен.

Надёжность зависит не от количества включённых переключателей, а от связки: уникальный пароль, дополнительное подтверждение при обычном входе и отдельно подготовленный резерв для восстановления доступа. Второй фактор снижает риск чужого входа, а резерв помогает законному владельцу вернуться в аккаунт, если привычный способ недоступен. Но даже правильно настроенная защита не отменяет проверки запросов и внимания к сообщениям, которые требуют немедленно действовать.

# Сообщение, которое торопит

Уникальные пароли и второй фактор мешают постороннему войти в аккаунт. Но защиту можно обойти иначе: убедить владельца самому открыть нужную страницу, ввести пароль или сообщить код. На экране появляется знакомое название службы и короткое требование: подтвердить операцию, иначе случится что-то неприятное.

Фишинг — это попытка обманом получить данные или подтолкнуть человека к опасному действию. Сообщение при этом не обязательно выглядит грубо или небрежно. В нём могут быть логотип, правильное обращение, номер заказа, часть адреса — детали, похожие на настоящие. Поэтому лучше разбирать сообщение не по первому впечатлению, а последовательно: понять, чего от вас хотят, проверить отправителя и ссылку, а затем найти независимый способ подтвердить запрос.

**Текст: что требуют и как давят**

**Представим сообщение о доставке:**

«Служба доставки: адрес указан не полностью. До 18:00 оплатите 49 рублей, иначе отправление вернётся отправителю. Подтвердить данные: ссылка».

В сообщении есть всё, что делает его правдоподобным: знакомая услуга, небольшая сумма и понятный срок. Если человек действительно ждёт посылку, он легко примет его за

продолжение обычного процесса. Но пока перед нами лишь утверждения отправителя. Они не подтверждают ни проблеме с адресом, ни необходимость платежа, ни то, что сообщение пришло от службы доставки.

Отделите требование от объяснения. В примере предлагают перейти по ссылке, подтвердить данные и заплатить. Если этого не сделать, обещают вернуть отправление. Крайний срок — 18:00. Так яснее видна суть сообщения: это не просто уведомление о доставке, а просьба выполнить действие под угрозой потерять посылку.

Давление обычно строится на страхе, выгоде или срочности. Страхом грозят блокировкой аккаунта, списанием денег, потерей доступа или посылки. Выгодой приманивают выплатой, скидкой или компенсацией. Срочностью торопят: осталось несколько минут, заявка аннулируется сегодня, ответ нужен немедленно. Все эти приёмы мешают спокойно проверить сообщение. Человека подталкивают действовать по чужому сценарию: нажать именно эту кнопку, позвонить именно по этому номеру, ввести данные именно на этой странице.

Ни страх, ни обещание выгоды сами по себе не доказывают обман. У доставки есть сроки, у банка бывают важные уведомления, у сервиса — плановые изменения доступа. Но срочность не делает сообщение подлинным. Она лишь заставляет получателя думать, что пауза опасна. Лучший ответ на давление — не пытаться разгадать сообщение по интона-

ции, а выйти из предложенного маршрута и проверить сам факт отдельно.

Попробуйте переформулировать уведомление нейтрально. Не «срочно подтвердите, иначе аккаунт заблокируют», а «отправитель утверждает, что аккаунт нужно подтвердить». Не «верните выплату до конца дня», а «сообщение предлагает перейти по ссылке и ввести реквизиты». Без нажима проще задать проверяемый вопрос: действительно ли служба просит эти данные?

Ошибки в тексте тоже не служат надёжным тестом. Опечатки и странные обороты встречаются в мошеннических рассылках, но бывают и в легальных уведомлениях. И наоборот: аккуратный текст ничего не доказывает. Его могли составить автоматически, скопировать с официального образца или просто грамотно написать. Внешний вид может насторожить или успокоить, но не подтверждает личность отправителя.

### **Отправитель: имя на экране и адрес за ним**

В почте первым обычно видно имя: «Служба поддержки», «Банк», «Доставка», «Администратор». Оно помогает ориентироваться в письмах, но не подтверждает, кто их отправил. Откройте сведения об отправителе и посмотрите полный адрес, а не только подпись, аватар или логотип.

В адресе могут быть малозаметные отличия: лишнее слово, подмена или перестановка символов, непривычный домен после знака @. Знакомое название иногда включают в

адрес, хотя основной домен принадлежит кому-то другому. Сверяйте его с контактами, которые вы заранее проверили по независимому источнику: например, с данными в установленном приложении или документами по услуге. Если вы не знаете, каким должен быть адрес, не пытайтесь угадать по названию компании.

Даже полный адрес не даёт безошибочного ответа. Письмо может прийти с настоящего адреса, если почтовый аккаунт отправителя взломан. Легальная организация может рассылать уведомления с технического адреса, который не похож на название бренда. А мошенник может подделать отображаемое имя или подобрать адрес, который выглядит убедительно. Поэтому адрес важен, но проверять нужно не только его.

Почтовые системы используют технические способы проверки подлинности отправителя. Иногда программа показывает предупреждение или сообщает, почему письмо попало в спам. Эти сведения полезны, но не делают письмо безусловно безопасным: проверка может не отображаться, работать не во всех случаях или не защитить от письма, отправленного со взломанного аккаунта. Чтобы принять безопасное решение, разбираться в технических заголовках не нужно.

В коротких сообщениях имя отправителя тоже может ввести в заблуждение. Надпись вместо номера телефона не всегда подтверждает личность. Новое сообщение может появиться в той же переписке, где раньше приходили настоя-

щие уведомления, но это не гарантирует его подлинность: из-за особенностей доставки в знакомой цепочке иногда оказываются сообщения от другого отправителя. И знакомое имя контакта в мессенджере не доказывает, что аккаунтом сейчас распоряжается его владелец.

Проверьте и сам повод для общения. Вы ждали это уведомление? В нём упоминается заказ или действие, которое вы действительно совершали? Совпадение с реальностью всё равно ничего не гарантирует: сведения о покупках и контактах могли попасть к посторонним, а массовое сообщение могло просто прийти в подходящий момент. Совпадение — ещё один факт для проверки, а не разрешение переходить по ссылке.

**Ссылка: маршрут, который предлагает отправитель**

В сообщении ссылка часто спрятана за обычной кнопкой: «Посмотреть заказ», «Защитить аккаунт», «Отменить операцию». Надпись может не совпадать с адресом, на который ведёт кнопка. Но даже если адрес виден, в большинстве случаев безопаснее не проверять его нажатием, а открыть нужный сервис самостоятельно.

На компьютере при наведении курсора часто появляется адрес назначения в нижней части окна. На телефоне удержание ссылки в некоторых приложениях открывает меню или предварительный просмотр, но поведение зависит от программы. Если вы не уверены, что произойдёт, не экспе-

риментируйте: не нажимайте ссылку, кнопку или изображение. Просто откройте сервис привычным способом.

Разбирая адрес, важно найти домен, а не выхватить из строки знакомое слово. В адресе условного вида «портал.и-мя-сервиса.чужой-домен.рф» название сервиса стоит слева, но основной домен — «чужой-домен.рф». Поддомены и слова перед ним легко подобрать так, чтобы создать нужное впечатление. Знакомое название где-то в адресе ещё не означает, что сайт принадлежит этой организации.

Адрес может отличаться одним символом, содержать похожие буквы из разных алфавитов, лишние слова или знаки. Сокращённая ссылка скрывает конечный адрес, а QR-код может вести на страницу, о владельце которой он ничего не сообщает. Не обязательно разгадывать все варианты на ходу. Если неожиданная ссылка требует войти, заплатить или подтвердить данные, проверьте запрос через приложение или сайт, который открыли сами.

# 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.