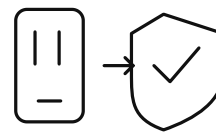


ПАМЯТКА 08



Ввёл пароль на чужом сайте

Пауза → проверка → действие

Считайте этот пароль раскрытым, даже если сайт показал ошибку. Приоритет - настоящий сервис, повторяющиеся пароли и способы восстановления; одного закрытия вкладки уже недостаточно.

Цифровая безопасность · Иван Юрьевич · Версия 1.0 · Редакционная проверка: 2026-10-26

Версия для чёрно-белой печати

Как понять, что случилось

- После ввода вы заметили чужой домен, неожиданный повторный вход или просьбу дополнительно сообщить код. Ошибка формы не означает, что введённые сведения не были отправлены.
- Появились уведомления о входе или сбросе доступа. Не подтверждайте их автоматически: сначала независимо откройте настоящий аккаунт и проверьте события безопасности.

Что сделать сейчас

1. Прекратите работу с поддельной страницей. С безопасного устройства самостоятельно откройте настоящий сервис, проверьте контакты восстановления и смените раскрытый пароль на уникальный.
2. Проверьте активные устройства, завершите посторонние сеансы и отзовите неизвестные приложения. Смена пароля не всегда автоматически закрывает все подключения; читайте предупреждения конкретного сервиса.
3. Если такой пароль использовался в почте, банке или других аккаунтах, защитите их отдельно. Начните с основной почты и средств; при банковском риске сразу обращайтесь в банк.
4. Если на подозрительном устройстве устанавливалась программа или был удалённый доступ, не меняйте на нём секреты. Используйте отдельное чистое устройство и памятку о приложении.

Что дальше

- Включите доступное дополнительное подтверждение или ключ доступа и сохраните резервный способ. Проверьте, что восстановительная почта и телефон принадлежат вам и остаются доступными.
- Проверьте недавнюю активность: отправленные сообщения, изменение адреса, покупки и разрешения. Если вы не можете войти, используйте официальное восстановление вместо многократного ввода старого пароля.
- Запишите время и адрес подделки для обращения в поддержку. Предупредите близких, если с аккаунта уже уходили сообщения; не публикуйте сам пароль в объяснении происшествия.

Чего не делать

- Не меняйте только одну букву в старом пароле и не используйте новый вариант сразу в нескольких сервисах. Не отправляйте пароль человеку, который обещает проверить утечку.
- Не выходите из последнего рабочего аккаунта до проверки восстановления. Не соглашайтесь на QR-вход или передачу второго фактора в ответ на обещание «отменить ошибочный вход».

Ваш вариант ситуации

Пароль раскрыт, код не передан

- Действуйте с паролем и сеансами; дополнительная защита могла остановить вход, но не делает раскрытый пароль снова безопасным. Не подтверждайте неожиданные запросы.

Передан ещё и код

- Прочитайте, какое действие подтверждал код, и откройте отдельную памятку. Код мог разрешить перевод, смену контакта или чужой вход, поэтому меры различаются.

Официальная помощь

- Google: проверка взломанного аккаунта support.google.com
- Mail: защита ящика help.mail.ru

Версия 1.0. Редакционная проверка 2026-10-26. Читайте эту памятку на learn.ivan-it.net/memos/entered-password.

Связанные уроки: [Пароли и восстановление](#); [Защита входа и сеансы](#); [Если уже случилось](#).

Источники: [Google: Как защитить взломанный аккаунт Google](#) (проверка 2026-10-26); [Mail: Защитить почту](#) (проверка 2026-10-26); [Google: Как защититься от фишинга и пожаловаться на него](#) (проверка 2026-10-26).

Возможности сервисов меняются; результат восстановления и возврат денег не гарантируются. При риске денег немедленно обращайтесь в свой банк. Учебный сайт не заменяет официальную поддержку.