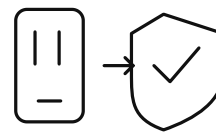


ПАМЯТКА 07



Открыл подозрительную ссылку

Пауза → проверка → действие

Сам факт открытия страницы не равен передаче пароля или установке программы. Сначала вспомните выполненные действия, чтобы выбрать подходящую памятку и не создавать лишнюю панику.

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

Версия для чёрно-белой печати

Как понять, что случилось

- Страница торопит с оплатой, просит войти повторно, показывает чужой домен или предлагает скачать обновление. HTTPS защищает соединение, но не подтверждает честность владельца сайта.
- После открытия мог начаться файл, появиться запрос уведомлений или разрешение браузера. Запишите, что вы нажали; не открывайте сайт повторно ради подробного расследования.

Что сделать сейчас

1. Закройте страницу и прекратите переписку с отправителем. Не нажимайте внутри неё кнопку «антивирус», «очистить» или «отменить взлом»: это может быть часть приманки.
2. Определите действие: только посмотрели; ввели пароль; назвали код; ввели карту; запустили файл или установили приложение. Для последних случаев сразу переходите к соответствующей памятке.
3. Если переданы банковские данные или сделан перевод, немедленно свяжитесь со своим банком через выбранный вами официальный канал. Проверка браузера и уроки могут подождать.
4. Если ничего не вводили и не запускали, проверьте загрузки, не открывая неизвестные файлы. Отмените подозрительную загрузку, обновите браузер и систему штатным способом.

Что дальше

- Проверьте разрешения сайта: уведомления, камера и микрофон не нужны случайной странице с доставкой. Отзовите выданное по ошибке; названия пунктов зависят от браузера.
- Наблюдайте за предупреждениями защиты и необычными входами. Если программа защиты обнаружила угрозу, используйте её штатную проверку, а не загруженную с той страницы утилиту.
- При необходимости сохраните адрес и сообщение как доказательство, не делая ссылку активной для близких. О подозрительном письме можно сообщить через встроенную жалобу почты.

Чего не делать

- Не вводите пароль «для проверки», не устанавливайте сертификаты, профили управления и расширения по подсказке сайта. Не пересылайте ссылку друзьям с просьбой открыть и проверить.
- Не сбрасывайте устройство без причины и резервной копии. Простое открытие ссылки требует иной оценки, чем запуск неизвестного приложения или предоставление удалённого доступа.

Ваш вариант ситуации

Телефон

- Отдельно проверьте, не была ли подтверждена установка приложения, профиля или особого разрешения. Если была – используйте памятку о подозрительной программе и другое устройство для помощи.

Windows

- Скачивание и запуск различаются. Незапущенный файл не нужно открывать, чтобы узнать его назначение; используйте встроенную защиту и помощь специалиста при срабатывании.

Официальная помощь

- Google: фишинг и жалобы support.google.com
- Microsoft: нежелательные программы support.microsoft.com

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

Связанные уроки: [Ссылки, сайты и QR](#); [Если уже случилось](#).

Источники: [Google: Как защититься от фишинга и пожаловаться на него](#) (проверка 2026-10-26); [Microsoft: Защита компьютера от нежелательных программ](#) (проверка 2026-10-26); [Т-Банк: Что делать, если перевели деньги мошенникам](#) (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.