

БЕЗОПАСНАЯ РАБОТА С САЙТАМИ



Злоумышленники давно научились создавать фальшивые сайты, и даже ваши рабочие и корпоративные сервисы могут стать их мишенью.

Давайте разберемся, как распознавать такие подделки, чтобы обезопасить вашу работу и защитить данные.

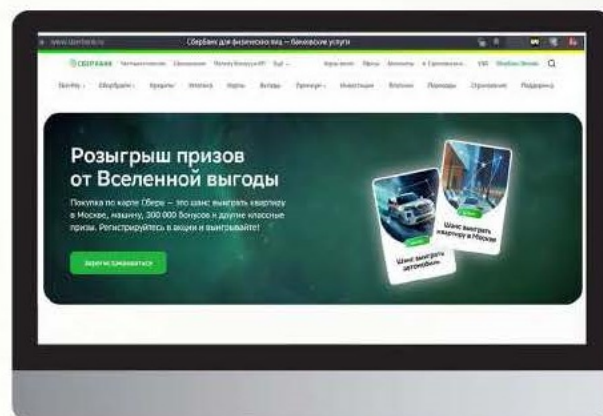
Дизайн и наполнение сайта

- Поддельные сайты часто имеют низкое качество оформления: нестандартные шрифты, устаревший стиль, ошибки в тексте.

- Обратите внимание на логотипы и фирменные элементы – если они выглядят размытыми или отличаются от оригинальных, это повод насторожиться.

- Некоторые мошеннические сайты копируют дизайн известных ресурсов, но могут отличаться цветами, кнопками или расположением элементов.

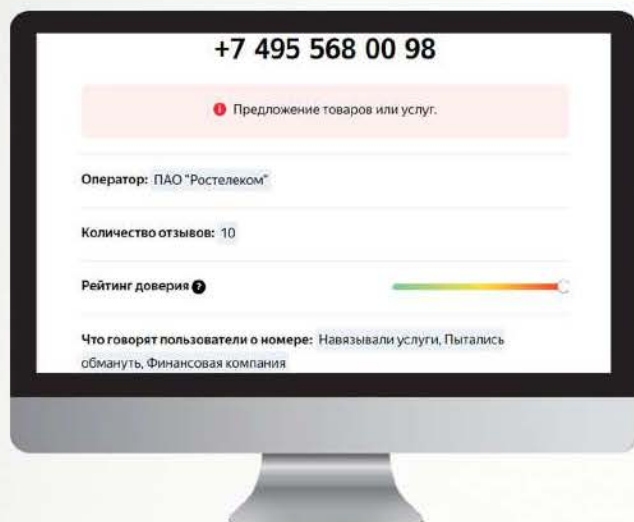
СПРАВНИТЕ:



Оригинальный сайт



Мошеннический сайт



Проверка информации на сайте

- У надежных сайтов есть контактные данные: юридический адрес, телефон, email. Их отсутствие – тревожный знак, но даже если они указаны, это не гарантирует подлинность сайта. Сравните эти данные с официальными источниками.
- Посмотрите ИНН или ОГРН организации с помощью сервисов проверки компаний – часто мошенники подставляют чужие реквизиты.
- Отсутствие политики конфиденциальности и условий использования может говорить о сомнительной природе сайта.
- Проверьте указанный стационарный номер телефона – напишите его в Яндекске и посмотрите, есть ли отзывы на этот номер и т.п.

Дата создания сайта

- Фальшивые сайты существуют недолго, поэтому проверьте дату их создания через специальный сайт - whois.ru.
- Если сайт новый, но выглядит как старая известная компания – это подозрительно.
- Посмотрите, обновляется ли информация на сайте. Если тексты старые или одинаковые на всех страницах, это тревожный сигнал.

ОБРАТИТЕ ВНИМАНИЕ >>>>>>

Created (англ. «созданный») - в этой строке указана дата создания сайта. Если сайт создан недавно, возможно, он мошеннический. Отправьте ссылку на него в подразделение ИБ для проверки.



Подозрительное поведение сайта

Повод задуматься, если:

- Сайт просит ввести личные данные.
- Вас просят заново ввести логин и пароль, хотя вы уже вошли.
- Появляются всплывающие окна с просьбой срочно что-то сделать.
- Сайт наполнен рекламой, которая ведёт на другие подозрительные сайты.
- Обещают «уникальные предложения» или огромные скидки.



Проверка безопасности сайта

При заполнении каких-то форм на сайте, убедитесь, что сайт начинается с **https://** и рядом есть значок замка – это признак защищённого соединения.

Это не значит, что сайт настоящий. Это лишь означает, что отправленные данные не будут перехвачены злоумышленником.

Если остались сомнения

- Если вы сомневаетесь в безопасности сайта, обратитесь в подразделение ИБ – они помогут проверить его надёжность.
- Если не сообщить о подозрительном сайте, мошенники могут украсть логины, пароли и другую конфиденциальную информацию.
- Несвоевременное обращение может привести к утечке данных, финансовым потерям или взлому корпоративных систем.

Вредоносные загрузки

- Не загружайте файлы с сайтов, которым не доверяете.
- Если сайт предлагает скачать файл – скорее всего, это вирус.
- Остерегайтесь сайтов, предлагающих «обновить» ваш браузер или антивирус – это может быть обман.
- Если сайт сам запускает загрузку файла, лучше сразу закрыть его и не запускать скачанный файл.

← → ↻  **https://**

← → ↻  **http://**