Признаки фальшивого сайта:

1. Адрес страницы выглядит странно: в нем есть лишние слова или опечатки, или он находится на непривычном домене. Проверьте, как должен выглядеть подлинный адрес, — например, найдите ресурс с помощью Google — и уходите со страницы, если адреса не совпадают.

2. Сайт выглядит неаккуратно: в текстах встречается множество ошибок и опечаток, раздел новостей не обновлялся очень давно. Подлинные сайты всегда вычитаны редактором и отрисованы профессиональными дизайнерами, а если есть новостная лента, она более или менее актуальна.

3. Сайт запрашивает излишнюю информацию. Например, для начисления банковских бонусов система просит ввести имя пользователя. Однако, если вы уже вошли в аккаунт, — а только в этом случае вам могли предложить какие-либо бонусы, — то зачем вводить имя пользователя повторно?

4. Используется незащищенное соединение. Компании и сайты, заботящиеся о собственной безопасности и безопасности пользователей, используют защищенное соединение по протоколу https. Отсутствие символа замочка перед адресом сайта и https:// в адресе — повод усомниться в подлинности сайта.

5. Непривычная форма ввода. В окне авторизации запрашивают не такую информацию, как обычно: например, всегда просили ввести имя пользователя и пароль, а сейчас — адрес электронной почты и пароль.

6. Неработающие элементы сайта. Многие фальшивые сайты не являются полными копиями настоящих, часто имитация поверхностная. Ссылки на таких подделках обычно или никуда не ведут, или перенаправляют на пустую страницу, а иные и вовсе могут быть частью рисунка!

7. Ваш антивирус, браузер или поисковый сервис предупреждают о том, что сайт опасен.

8. Сайт содержит так называемый «визуальный шум»: нужный контент полузакрыт всплывающей рекламой; сайт мигает контрастными предупреждениями о необходимости обновить браузер или, скажем, о выигрыше в лотерею; сайт издает звуки...

Что делать, если я оказался на поддельном сайте?

- **Закрыть вкладку.** То есть как можно быстрее уйти с этого сайта. Это первое и основное действие, которое нужно совершить, если вы поняли, что находитесь на поддельном сайте.

- **Помочь другим.** Например, вы наткнулись на поддельный сайт Банка. Теперь найдите через поисковик подлинный сайт Банка и напишите в его службе поддержки, что существует клон-подделка. Служба безопасности Банка предпримет меры, например, обратится в органы правопорядка — и другие пользователи будут защищены от мошенников. Вы просто сделаете хорошее дело.

- **Если вы ввели свой пароль,** как можно скорее сообщите об этом в Банк, срочно найдите через поисковик подлинный сайт, за который вы приняли подделку, авторизуйтесь там и измените свой пароль. Пароль, который введен на сайте-подделке, скомпрометирован.

- **Новый пароль не должен быть связан со старым**. Ваш старый пароль на 100% в руках мошенников, которые знают ваше имя пользователя и могут подобрать новый пароль, если он похож на старый.

- **Если этот пароль использован на еще каких-то ресурсах, там его тоже нужно заменить**. Напомним: не нужно использовать один и тот же пароль на разных ресурсах.

Рекомендации:

- Не вводите на сайте никакие данные, пока не убедитесь в том, что страница настоящая.

- Помните, что опасным может быть абсолютно любой сайт, и обязательно обращайте внимание на признаки, по которым можно определить вредоносный сайт.

- Покиньте сайт при появлении первых подозрений в подделке.

- Проверяйте окна авторизации на подлинность, даже если они возникают во время работы на надежных сайтах.

- Если вы перешли на некий сайт, и с него сразу скачалась какая-то программа (все браузеры сообщают о подобных загрузках), это совершенно точно мошеннический сайт. В этом случае недостаточно просто закрыть сайт. Порядок действий таков:

1. Закрыть вкладку с сайтом.
2. Закрыть браузер. Закрывать браузер, не закрывая вкладку, не стоит: браузеры обычно запоминают открытые вкладки; при следующем запуске он снова откроет вредоносный сайт.
3. Зайти в папку «Загрузки» и удалить скаченный файл. Если он удалился в корзину, то почистить корзину.

4. Запустить антивирус и просканировать диск.

Автоматическое скачивание неизвестной программы при переходе на сайт — это очень опасно.