

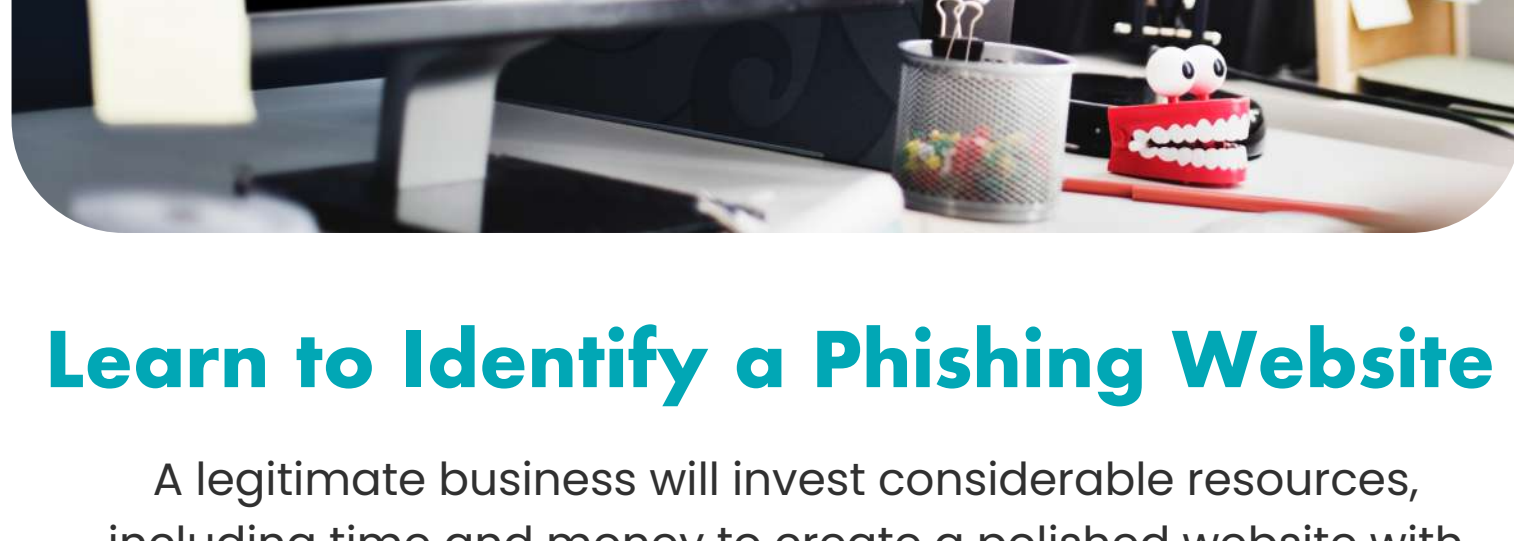


Safe Browsing Habits: Avoiding Malicious Websites and Downloads

It's no secret that browsing the internet is like navigating an open minefield full of malware and malicious software. Many websites are specially designed to appear trustworthy and appealing so you could submit your sensitive information or unknowingly download malicious files.

Once these files are in your hard drives and network, they will start stealing information or may even encrypt your computer to demand a hefty ransom.

Learning how to navigate these websites and avoiding suspicious links are fundamental to online safety. Let's look at a few tips on how you can avoid malicious websites and harmful downloads.

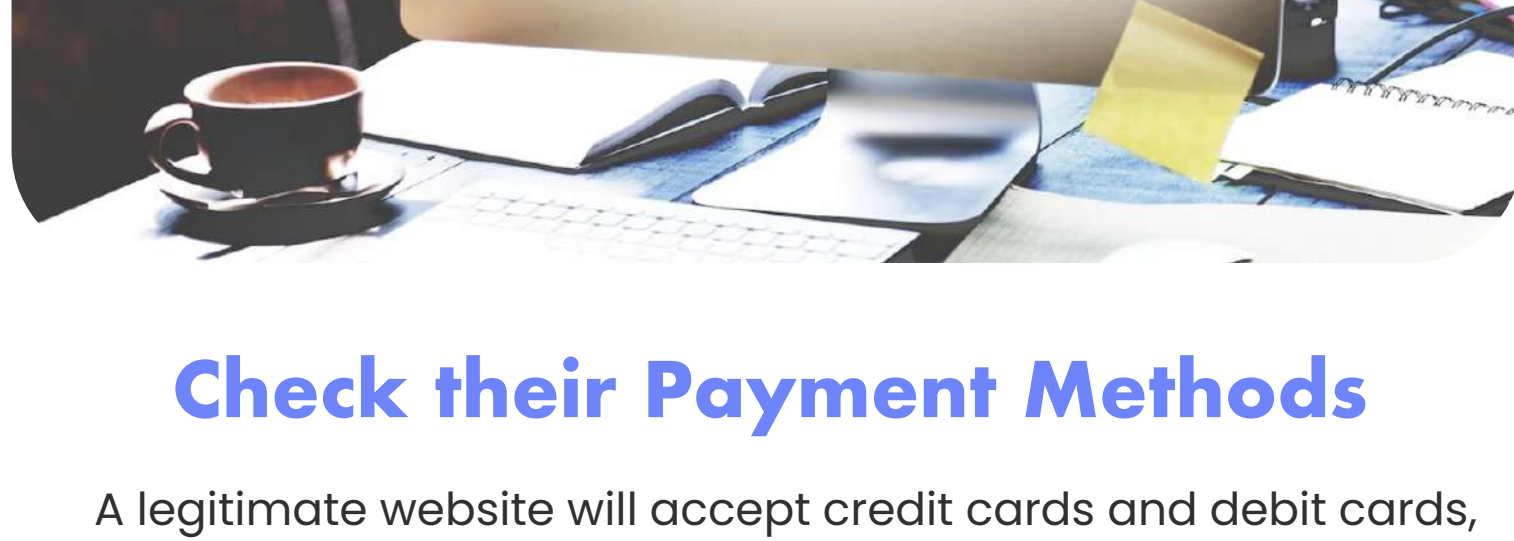


Learn to Identify a Phishing Website

A legitimate business will invest considerable resources, including time and money to create a polished website with high-quality and relevant graphics and a well-designed user friendly experience. A phishing website will often look substandard with various red flags that are easily identifiable.

You'll notice various grammar mistakes, broken English, low-resolution images, and spelling errors. Phishing websites often don't have a 'contact us' page – because there is no means of reaching the perpetrators.

However, legitimate businesses will prominently display their contact details, including their social media links, postal addresses, geographical locations, phone numbers, and email addresses. Websites that do not provide this information could be carrying out suspicious activity.



Check their Payment Methods

A legitimate website will accept credit cards and debit cards, as well as other popular online payment tools such as PayPal and Stripe. However, a phishing website may often ask for a bank transfer or even a gift card. Some phishing websites may ask you to wire the money to a Bitcoin address – which is a major red flag.

In most cases, if a user fell victim to a fraudulent website, they may be able to claim their money back if the purchase was made with a credit or debit card. However, there is no way to get their money back if they used a bank transfer and not if they sent the money through Bitcoin.

A legitimate website will always provide multiple payment methods. Note that many legitimate websites accept Bitcoin, but they also provide more popular and secure payment options such as PayPal and Stripe.



Check their Online Reviews

Online reviews can help you identify if a website is fraudulent or legitimate. Before you make any online purchase or provide your personal information, you should thoroughly research the company to determine if they are legitimate and check its reputation. If the website has defrauded visitors in the past, its victims might share their negative experiences.

It is also worth noting that bad actors can easily fake online reviews, so you should always look for reviews at a trusted source such as Trustpilot.

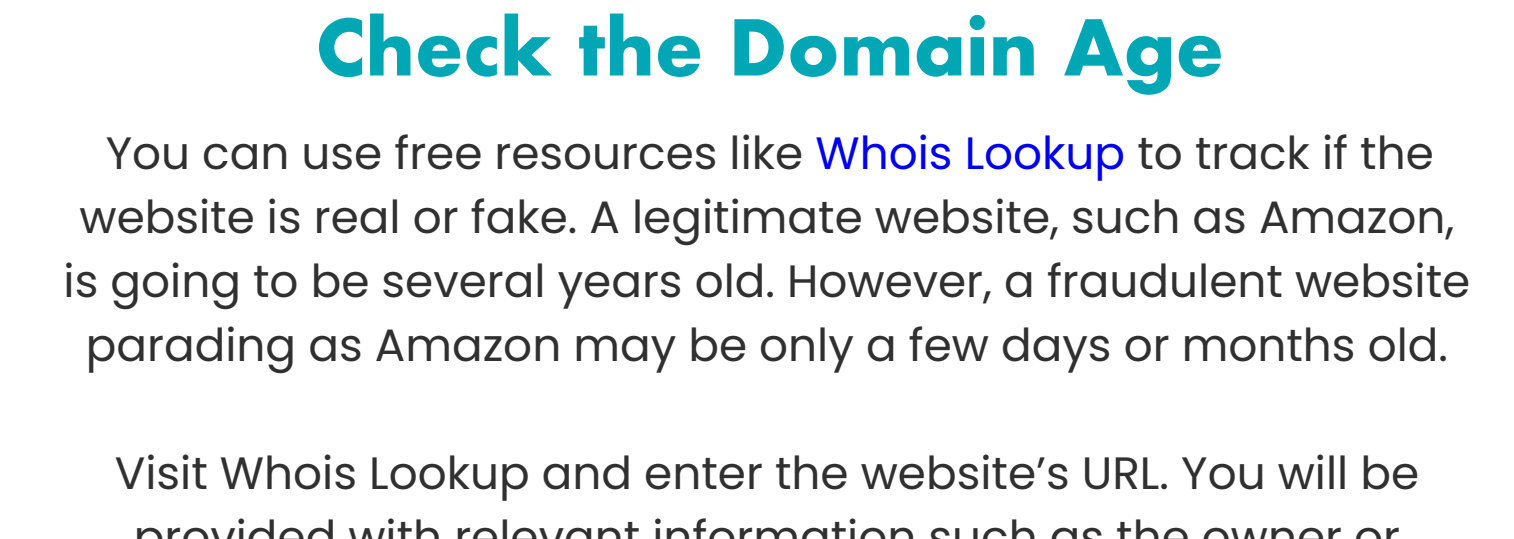
The easiest way to identify fake reviews is to look for the following red flags:

- The reviews are very similar, and the writing style is oddly similar.
- The reviews are very recent – this isn't always a red flag. However, a legitimate website will have several reviews dating back many months or years.
- Very few reviews – this is possible if the company is still new. However, if the site seems fraudulent and they don't have many online reviews, you may want to avoid it

Never Submit Private Information if the Website is Insecure

Your browser may alert you if the website is insecure by giving you a security alert, such as "this website is insecure". This alert is either an indication of a fraudulent website or a sign that the website owners are not managing their website securely.

A secure website will have a padlock icon to the left of the URL address. Clicking on the padlock icon will provide you with relevant information on the website security certificates and cookies.



Check the Domain Age

You can use free resources like [Whois Lookup](#) to track if the website is real or fake. A legitimate website, such as Amazon, is going to be several years old. However, a fraudulent website parading as Amazon may be only a few days or months old.

Visit Whois Lookup and enter the website's URL. You will be provided with relevant information such as the owner or organization's name, country of registration, and domain age.

Pro tip: Use the [Wayback machine](#) to check out how the website looked in the past.

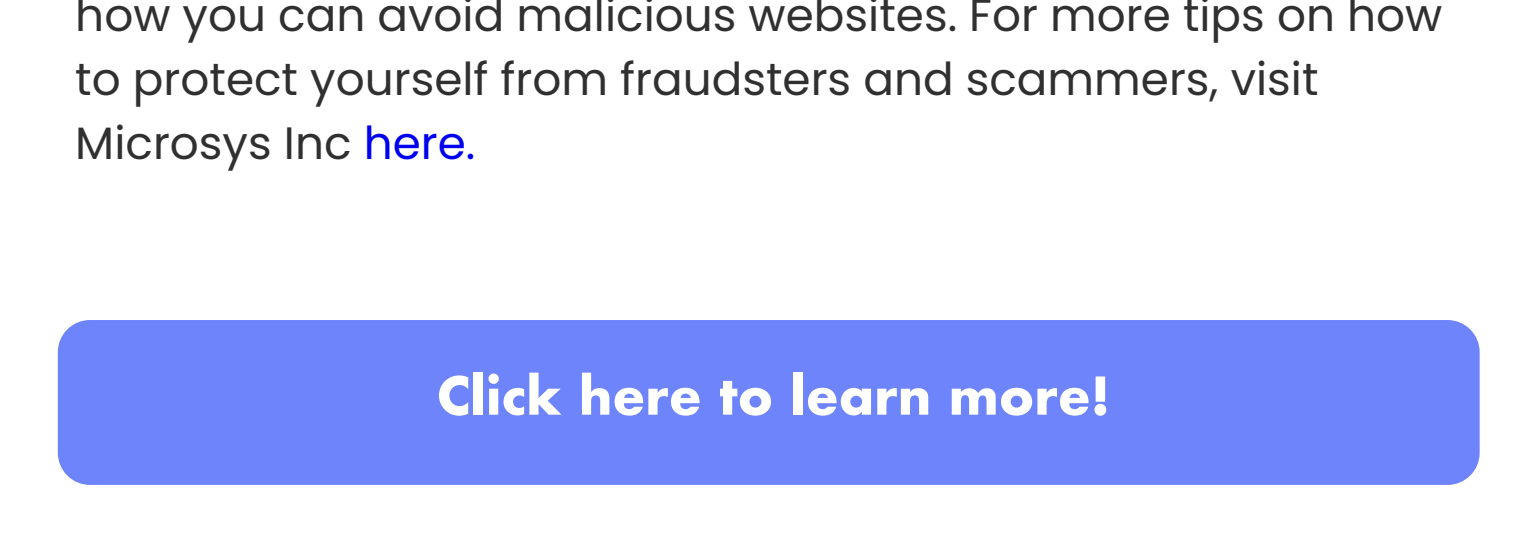
Carefully Inspect the Domain Name

The easiest way to tell if you're on a fake website is when the URL does not match the official website of the organization. For example, scammers may use domain names that are very similar to the official URL. In some cases, they may even contain the official URL within the fake domain name.

Let's look at a few examples of spoofed website domains:

- PaayPal.com (adding an extra "a")
- Walmart.comsecure-site.com
- Netflix-support.org (combining the legitimate domain name with a different business extension)

Make sure to always double check if you are on the right domain before entering sensitive information.



Never Click Links in Emails

It's one of the oldest tricks in the book – to trick you into opening an attachment that contains malicious software. This malware can infect your device and steal your confidential data. It could also steal your personal information and business passwords or take over your accounts to infect other colleagues and friends.

Always be careful when an email has an attachment, even if it comes from a familiar sender. Always double check before clicking on the attachment. Further, you should do the following:

- Ask the sender to confirm if they intentionally sent the email to you. It isn't uncommon for people to get a virus or have their accounts compromised. The best thing you can do is to contact this sender elsewhere because if their account is compromised, someone else may be responding to your message.
- If you don't know the sender but believe the email is legitimate, contact the organization to confirm if they sent the message to verify its legitimacy,
- If you don't know the sender and the attachment is clearly something you aren't in need of; just delete it and move on.

So there you have it, a quick look at safe browsing habits and how you can avoid malicious websites. For more tips on how to protect yourself from fraudsters and scammers, visit Microsys Inc [here](#).

[Click here to learn more!](#)