

# IHS DAILY BUSINESS GUIDES

VISIT US AT [INSIDEHS.COM](https://www.insidehs.com)



## Cybersecurity: Detecting Phishing Websites

As we highlighted in an earlier Daily Business Guide, phishing is a cybersecurity problem often delivered via email or social media. However, many businesses do not realise that phishing is a website issue, too.

A phishing website is a fake website that replicates a real site's look and content. When you or your staff click on an email link and land on the fake site, you have opened your business to a phishing attack.

In this Daily Business Guide, we explain how to spot the tell-tale signs of malware, what to do if you land on a phishing website, and how to prevent it from happening again.

---

### HOW TO CHECK THE AUTHENTICITY OF A WEBSITE

It is too easy to click on a link that looks legitimate or misspell a website domain/URL, and you find that you are on a landing page that may not be all you expect.

Unfortunately, even websites you visit regularly may not have high-quality security settings and can become unreliable via hacker infiltration. Suddenly, these sites have embedded malware that can obtain payment details and customer data or infect the visitor's computer systems. Here is what you need to check:

#### 1 The Website URL:

A fake site can often be identified by looking at the URL.

Many phishing URLs include strange words, misspellings, and an expected .com may be a .org or other. The spelling errors may also be visible within the replicated on-page content. If in doubt, don't click the link!

**Top Tip:** *Manually Type the URL into the search box and navigate the site directly.*

## 2 Check The Content:

A few seconds of reviewing the content on the page may save you hours of stress and heartache. Is the content high quality and relevant to the product/service/industry?

Hackers will NOT expect you to read the content. They want you to click the link so that poor content may be evident.

**Top Tip:** *If still unsure, look at the content page. Many phishing sites will not have a contact page; even if they do, they will not have privacy statements or checkboxes.*

## 3 Premature Reaction:

Phishing scams will always want you to act with a very quick response.

Many fake sites will use pop-up windows encouraging immediate click-through with login details, credit card information, and act now actions. So be alert to this.

## 4 Check The Reviews:

The internet offers superb access to everything we need. However, the downside is that it also offers the bad alongside the good.

If unsure, conduct wider research on the site/company/content. Check reviews, who likes and shares content, and who comments, mentions and interacts with the site you are viewing.

We can all spot fake reviews that might indicate a phishing scam, and you should proceed cautiously.

## YOU'VE CLICKED ON A PHISHING SITE! WHAT NEXT?

You need to act quickly to limit the damage.

First, visit [https://safebrowsing.google.com/safebrowsing/report\\_phish](https://safebrowsing.google.com/safebrowsing/report_phish), which will flag the site and help prevent future issues.

And then, if your system is compromised:

- Change your access passwords
- Scan using a trusted antivirus software service
- If you have entered payment details, contact your banking service
- File a police report if there is a serious breach
- Inform the relevant data protection authorities as legally required.

## TRAINING - PREVENTION IS BETTER THAN CURE

Create a guidebook with employee advice about cybersecurity and ensure all your staff are aware of and up-to-date with the latest cybersecurity news and issues.

Include a reporting process with named persons of responsibility, contact details, and confirmed processes for immediate action. Be aware and be safe.

## REQUIRE CYBERSECURITY ADVICE AND ASSISTANCE?

Looking for help? The IHS Marketing Team can support all your marketing needs, including cybersecurity, video development, website and social media audits, research and analysis, actions and activity.

Visit the [www.insidehs.com/dailyupdate](http://www.insidehs.com/dailyupdate) page for more information. Follow Inside Hospitality Solutions on [LinkedIn](#) and subscribe to our [monthly newsletter](#).

## IHS MARKETING CONTACTS

Name	Contact Information
<b>Yuri Duncan</b>	Yuri@insidehs.com
Marketing	+1 317 645 3824
<b>Rich Paliwoda</b>	Rich@insidehs.com
President	+1 917 5703827