POPULAR BUT INSECURE

Celebrities want popularity. The more popular they are, the more money and fame they have. Much like celebrities, you want your business to be as popular as possible, so you add features to create a highly interactive and engaging website.
But is being popular always a good thing?

Over 760,000 websites are breached each year.[1] However, ***only 8 percent*** of website owners use proactive website monitoring for suspicious activity, while ***84 percent*** rely on search engines, website hosting providers or site visitors to alert them of malicious activity after they've been compromised.

Hackers often target the most popular and complex websites, because they know these sites are vulnerable. Find out which website features correlate to website attacks, how cybercriminals compromise websites, and what you can do to protect your site and business.

CELEBRITY POPULARITY

Celebrities increase their popularity by engaging and interacting with their fans through:

YOUR SITE'S POPULARITY

Website owners increase their website's popularity and traffic by adding features, such as:

EVEN FAME HAS ITS DRAWBACKS

Paparazzi are constantly trying to catch celebrities **off-guard** and in a **compromised state.**

EVEN THE MOST POPULAR SITES FALL SHORT

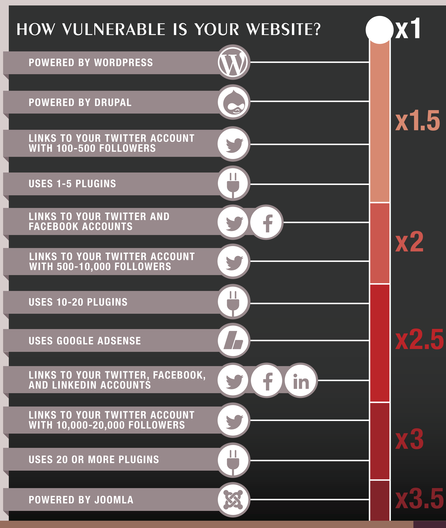
The more engaging and complex your website is, the more likely it is to be **compromised.**

POPULAR WEBSITE FEATURES

The features that make your website popular could also be increasing your likelihood of a cyberattack.*

Below are a few examples of popular website features and how they affect a site's risk of being compromised (compared to the average website).

HOW VULNERABLE IS YOUR WEBSITE?



CYBERCRIMINALS VS PAPARAZZI

You can think of cybercriminals as the paparazzi. You need to constantly defend against malware, vulnerabilities and other cyber threats. Like the paparazzi, cybercriminals will disguise themselves and follow you.

HERE'S HOW CYBERCRIMINALS COMPROMISE YOUR WEBSITE

WEBSITE INFECTIONS BY MALWARE TYPE

A website can be infected with multiple types of malware at any given time. See some of the most common types of malware below, according to SiteLock data.

BACKDOOR FILES

Cybercriminals leave backdoor files as a way to secretly enter and leave a website. Backdoors give hackers the ability to add, modify or delete a site's content.

VISITOR ATTACKS

Hackers use visitor attacks to target the website's visitors, rather than just the site itself.

SHELL PROGRAMS

Shell programs give hackers the control of a website's files and the ability to administer a website.

SPAM

Hackers use spam to post comment spam and manipulate search engine results to increase their rankings.

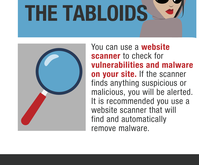
DEFACEMENTS

Cybercriminals use defacements to change the visual appearance of a website or webpage.

SECURING YOUR WEBSITE

Just like celebrities need 24/7 security to protect themselves from the paparazzi, websites need 24/7 website security for protection against cybercriminals.

STAY OUT OF THE TABLOIDS



You can use a **website scanner** to check for **vulnerabilities and malware on your site.** If the scanner finds anything suspicious or malicious, you will be alerted. It is recommended you use a website scanner that will find and automatically remove malware.

There's no Such Thing as Bad Publicity... Except when it comes to Your Business

A web application firewall (WAF) can differentiate human traffic from bot traffic. If a WAF suspects the traffic attempting to enter your site are bad bots, like scrapers, access will be denied.

[1] https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/44924.pdf

* This data is based on the SiteLock® database of over six million websites as of March 2017. Website features do not cause website attacks, but they are associated with an increased likelihood.

SiteLock