Security by Obscurity

The term, "security by obscurity" implies that the less popular and attention grabbing your website is, the less likely it is to be targeted by cybercriminals. ***The truth is, there's no such thing as "too small to hack."*** Given that a majority of small businesses manage or maintain their own websites, they typically aren't aware of the time or resources required to protect their most valuable business asset. Most will set up a website then operate under a "set it and forget it" mentality.

What are Cybercriminals After?

Every Website is at Risk

According to recent SiteLock data, **WEBSITES EXPERIENCE**

22 ATTACKS PER DAY

on average – that's over

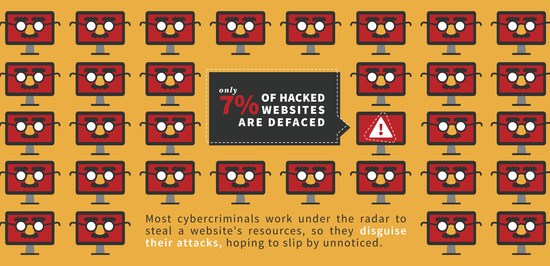
8000 ATTACKS PER YEAR

Cybercriminals target more than just eCommerce sites. In fact, just **1% OF COMPROMISED SITES ARE ECOMMERCE.**

99% of hacked websites are comprised of sites you might not expect, like **BLOGS, SMALL BUSINESSES AND NON-PROFIT SITES.**

Why Would a Cybercriminal Want to Attack *MY* Website?

Any website, regardless of number of features or amount of traffic, will always be at risk of cyber threats. Many people think hackers are primarily interested in defacing sites, and that any site that has been compromised will be visibly defaced. In reality,



Most cybercriminals work under the radar to steal a website's resources, so they **disguise their attacks**, hoping to slip by unnoticed.

Why My Blog?

A small blog might seem like a random target, but hackers will take advantage of an active comment section to insert spam links or steal traffic and resources.

21% OF HACKED WEBSITES ARE INFECTED WITH **SPAM.**

SPAM
Cybercriminals use spam to boost their search engine rankings by inserting backlinks and spam content on websites.

21% OF HACKED WEBSITES HAVE **TRAFFIC STOLEN.**

STOLEN TRAFFIC
Hackers steal web traffic for their own benefit. For example, they will send traffic to pharmaceutical sites in hopes of making a profit.

6% OF HACKED WEBSITES HAVE **RESOURCES STOLEN.**

RESOURCE THEFT
Cybercriminals steal bandwidth or other computing resources to aid in sending automated attacks.

Why My Small Business?

Many small business sites are not actively managed, making them ideal targets for shell programs.

39% OF HACKED WEBSITES ARE INFECTED BY **SHELL PROGRAMS.**

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

Why My Non-Profit?

A non-profit site may store donor information, which cybercriminals try to access using a backdoor file.

73% OF HACKED WEBSITES ARE INFECTED BY **BACKDOOR FILES**

BACKDOOR FILES
Cybercriminals use backdoor files to gain access to sensitive customer data, like credit card info or email addresses

Be Certain Your Website is Secure

Obscurity should never be your only security defense.

SCAN FOR CLARITY
Use a **website scanner** to find SEO spam, vulnerabilities and malware on your website or blog. Be sure to use a scanner that can automatically remove the malware from your site.

BLOCK AMBIGUITY
Use a **web application firewall (WAF)** to help protect your site from bad bots and other malicious traffic. A WAF can differentiate human traffic from bot traffic, allowing only good traffic to enter the site. It can also help prevent hackers from uploading files or changing a site's content.

HAVE A BACK-UP
Make sure to do **frequent backups** on your website. Website attacks can destroy site content, so backups are crucial to recovering damage.

SiteLock

*This data is based on the SiteLock® database of over six million websites as of March 2017.