

Web Professionals Security Survey

TWENTY NINETEEN

How agencies approach website security
and protect their clients' websites.



40%

of web professionals
need help explaining
website security
topics to clients.

For web professionals with 20+ clients, the likelihood of experiencing a hack increases to

55%





44%

of web professionals have
dealt with a hacked website.

Table of Contents

INTRODUCTION	6
OVERVIEW	7
SECURITY INFORMATION	10
SECURITY SERVICES AND TOOLS	12
HACKS & ATTACKS	16
CONCLUSION	19



Introduction

This report analyzes over 1,000 survey responses from web professionals, including web designers, developers, freelancers, and marketing agencies. The respondents consisted of Sucuri and GoDaddy customers, whose responses produced statistics associated with:

- Professional business models
- Service offerings and tools
- Approaches to website security
- Planning for hacks and attacks

The Web Professional Security Survey is produced to better understand how agencies run their businesses and the challenges they face when dealing with security incidents. This report uses data collected in 2018.

Overview

The term web professional refers to any website service provider, including:

- Website developers and designers
- Marketing agencies and SEO
- Brand reputation agencies
- Web hosting providers
- Freelancers
- Managed service providers (MSPs)

When asked how many clients the website professionals were responsible for, these were the results:

Looking further into this data, we see that the large majority in this bucket manage less than eight websites. This doesn't necessarily mean that these websites are small, some of them can have over a thousand pages requiring a lot of work to keep updated and optimized.

Website professionals offer a variety of services and the number of clients doesn't always reflect the size of the business. Some larger agencies service only a handful of clients, and startups or specialized service providers may choose to limit the number of clients they take on.

Agencies that offer marketing services, such as SEO and advertising, make up nearly a third of all responses.

How Many Clients Are You Responsible For?

1-5 CLIENTS (229)

38.5% 

6-20 CLIENTS (162)

27.2% 

21-50 CLIENTS (79)

13.3% 

51-100 CLIENTS (43)

7.2% 

100+ CLIENTS (82)

13.8% 

How Many Websites Are You Responsible For?

LESS THAN 8 WEBSITES (295)

49.6% 

8-20 WEBSITES (139)

23.4% 

21-50 WEBSITES (75)

12.6% 

51-100 WEBSITES (42)

7.1% 

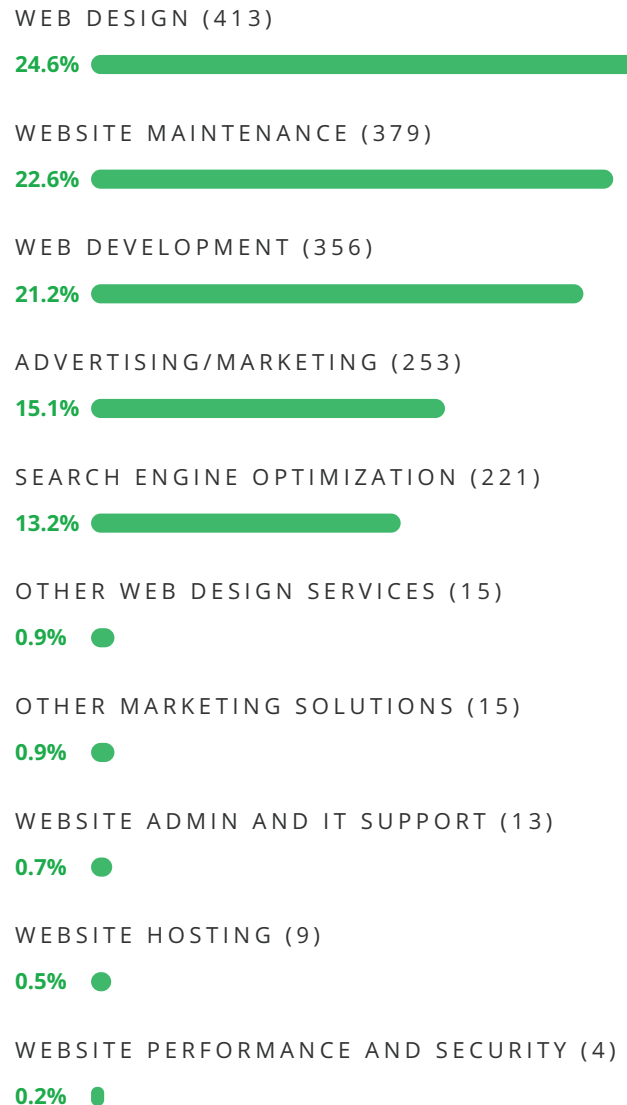
100+ WEBSITE (44)

7.4% 

The second largest group is Website Maintenance, which refers to agencies that set up a website with domain, hosting, and even SSL certificates. Sometimes they are also responsible for handling updates, hardening, and website security.

With only 0.2% of respondents saying that they offer website security as a service, there is an **opportunity for web professionals to differentiate** themselves by promoting website security in the early stages of client relationships.

What Services Do You Offer?



Recommended Webinars

Making Money with Sucuri's Partnerships

[Watch Full Webinar >>](#)

Website Security Primer for Digital Marketers

[Watch Full Webinar >>](#)

A hosting service provider offers the management of website servers and databases on behalf of their clients, whether it is self-hosted or through a larger hosting company.



Website hosting companies of all sizes feel the pain when it comes to end-user website security. Clients expect their hosting company to help them address website security incidents such as being hacked, blacklisted, or attacked.

A Content Management System (CMS) allows web professionals to build sites faster. Some are best for ecommerce websites, others are more suitable for blog pages or business-oriented websites.

Recently, we released our [Hacked Trend Report for 2018](#), which analyzed 25,466 infected websites including specific CMS applications. The results in this report do not imply that these platforms are more or less secure than others, it merely reflects the overall popularity of the CMS.

What CMS Do You Use?

WORDPRESS (438)



DO NOT USE A CMS (189)



JOOMLA! (75)



.NET (65)



MAGENTO (56)



DRUPAL (47)



Recommended Guides

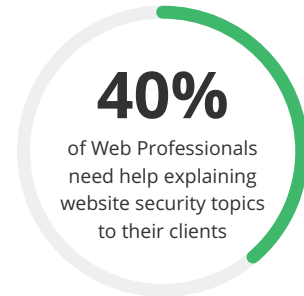
We have prepared guides for some of these popular platforms, such as our [WordPress Security Guide](#) and [Magento Security Guide](#).

[Clean Your Hacked Website >>](#)

Security Information

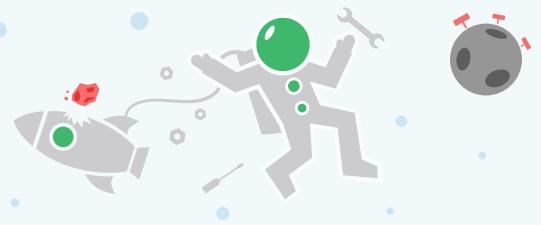
In this section, we will take a look at how web pros handle security threats. Do they have a [security plan](#) in place? How do security incidents impact their businesses?

Managing a website is a huge responsibility and security can be one of the biggest challenges. We have an email course designed to help web service providers add website security to their portfolio.



Recommended Email Course

[Subscribe to the Sucuri Agency Email Course >>](#)

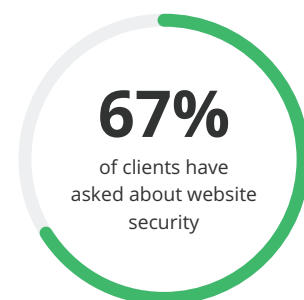


Sucuri can help you explain how important a website security solution is for any website owner. We have a [marketing kit](#) with a checklist, email templates, guides, and case studies that convey the importance of implementing security.

Because it's clear that we all need a safer internet, we wanted to know if clients are concerned about the security of their websites.

The majority of web professionals have been asked about website security at some point during the client relationship. With 68% of clients asking web professionals about security, it is concerning to see how few respondents offer security features.

If you want to become a thought leader in website security, we recommend [subscribing for email updates](#) about vulnerability disclosures, blog posts, webinars, and guides to stay current on the latest industry news.



A hosting service provider offers the management of website servers and databases on behalf of their clients, whether it is self-hosted or through a larger hosting company.

Over half of participating agencies say that they have a designated budget to invest in website security. Having the right security partner is ideal in offering their customers the best website security solution in the market.

SUCURI CONSULTATION

Get a Free Website Security Consultation

[Contact Us Now >>](#)

It is concerning that 45% of participants do not have a budget allocated for their customers' website security. This is despite the fact that 90,000 websites are hacked each day (according to [Hosting Facts](#)) and the [Google Transparency Report](#) shows a large majority of blacklisted sites have been compromised by hackers.

No matter the size or type of business you have, an attacker will gladly steal your traffic and resources.

How Much Budget Do You Have to Invest In Website Security?

ZERO (77)

45.6% 

UP TO \$100 PER MONTH (64)

37.9% 

UP TO \$500 PER MONTH (18)

10.7% 

UP TO \$1,000 PER MONTH (5)

3.0% 

\$1,000+ PER MONTH (5)

3.0% 

Security Services and Tools

We asked web professionals what they currently do to secure their clients' websites. Let's take a quick look at some of the security features being offered.

I - Backups

Having a proper website backup solution in place means that the website can be restored to its previous state in case a problem were to occur. However, a backup alone does not offer website security.

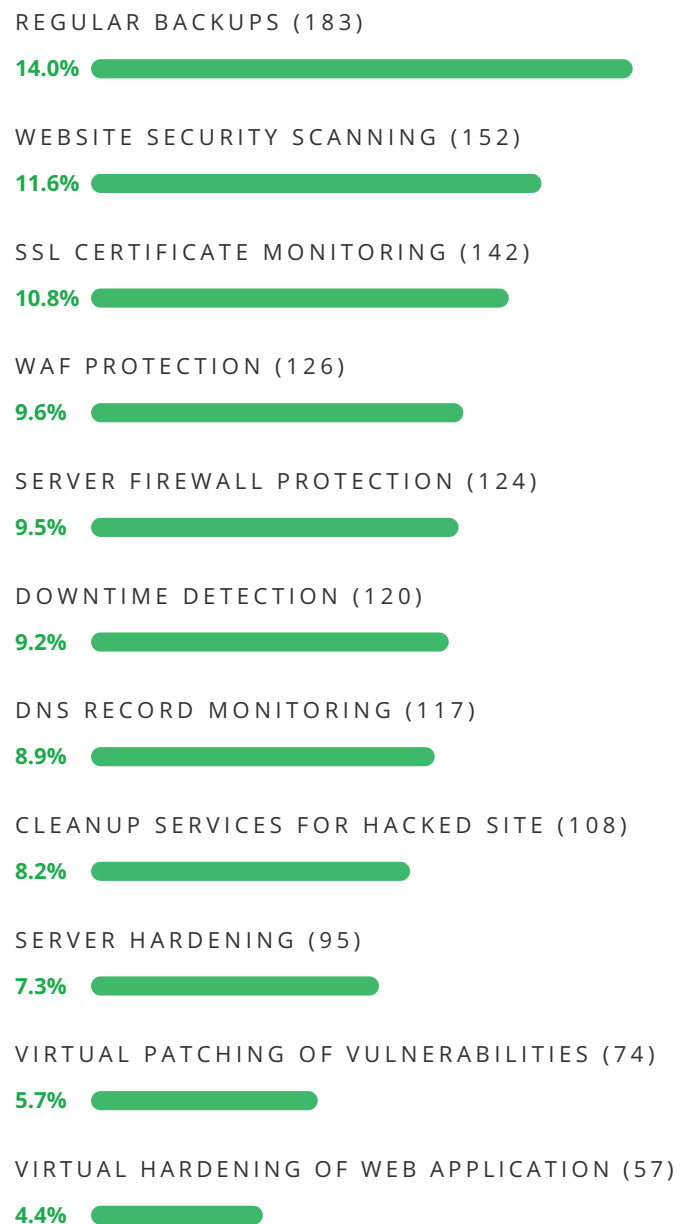
[Website Backup Strategy >>](#)

II - Website Security Scanning

How can you know if there is a problem in advance without monitoring the website environment? We recommend having a robust monitoring solution that includes server-side scanning as well as remote scanning.

[Free Website Scan with SiteCheck >>](#)

What Security Features Are Included In Your Service?



III - SSL (Secure Socket Layer)

With an SSL certificate, your website can use the HTTPS protocol to securely transfer information. This is crucial for ecommerce sites and membership sites with user logins. SSL is also a confirmed ranking signal in search engines.

[Install a Free SSL Certificate >>](#)

IV - Web Application Firewall (WAF)

A WAF serves as a barrier for website attacks and hacks. It blocks malicious requests, allowing only legitimate traffic. A WAF is capable of blocking DDoS attacks, vulnerability exploitation attempts, and unauthorized access.

[Learn How a WAF Works >>](#)

V - Clean Up Services

Removing website malware can be a daunting job. It takes a lot of expertise and time to find hidden backdoors and infections without breaking the website. We believe remediation tasks may not be the best use of a web provider's assets.

[Read the How to Clean a Hacked Website Guide >>](#)

VI - Hardening and Patching

Hardening your website involves adding code or making changes to the server configuration to reduce the attack surface. Patching means updating extensions and themes to prevent vulnerabilities from being exploited. A WAF automatically enables virtual hardening and virtual patching.

[Compare the Best WAFs Available >>](#)

We have asked web pros about how they secure their client's websites. Whether these are included in the service offering or not, this is how most web professionals protect their projects.

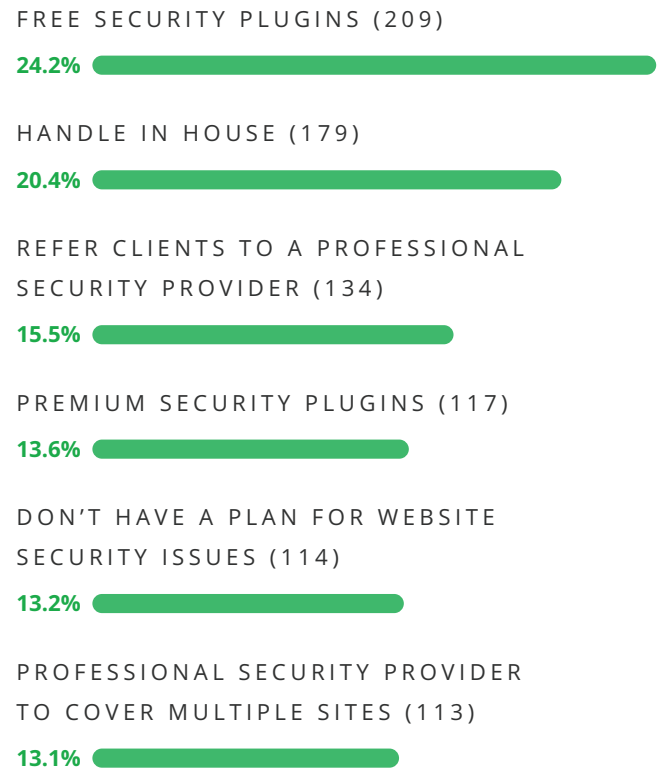
Free plugins are a good start to securing a website, however, these are best accompanied by a website firewall to block hack attempts. Sucuri has developed a [free Security Plugin](#) for WordPress.

Coming in second (20.4%), security issues are handled in house. What this means is that whenever a problem with a website arises, someone within their team will manage these events on an ad-hoc response.

Around 13% of web professionals responded that they **do not have a plan for website security.**

This is concerning, because a security incident can result in loss of data, sales, time, and brand reputation. There can also be long-term damage to SEO rankings if the security issue is not addressed quickly.

How Do You Secure Your Clients' Website?





44%

Almost half of the web professionals surveyed have dealt with a hack.

Hacks & Attacks

Ok, we have talked about setting up security. How well do web professionals maintain a secure environment? The most notorious threats to website security stem from vulnerabilities that are introduced by add-on modules, plugins, themes, and extensions.

The best possible practice is to have a website firewall installed since a WAF will virtually patch the website completely, protecting it even from [zero-day attacks](#).

The Sucuri blog always reports on [vulnerabilities disclosures](#). You can sign up for the blog email feed and never miss an update.



Almost half of the web professionals surveyed have **dealt with a hack**.

It all starts with knowing there is a possible threat around the corner that can be a setback in your day-to-day operations.

How Frequently Do You Install Security Patches For Your Clients'?

AUTOMATIC UPDATES ENABLED (208)

36.9%

AS SOON AS POSSIBLE (172)

30.5%

CLIENTS ARE RESPONSIBLE (72)

12.8%

WHENEVER I HAVE TIME (69)

12.2%

WHEN PROMPTED OR CLIENT REQUESTS (30)

5.3%

I DON'T (13)

2.3%

Interestingly enough, when respondents have fewer than five clients, this number drops to 30.5% having experienced a hack.

For web professionals who have more than 20 clients, the likelihood of **experiencing a hack increases to 54.7%.**

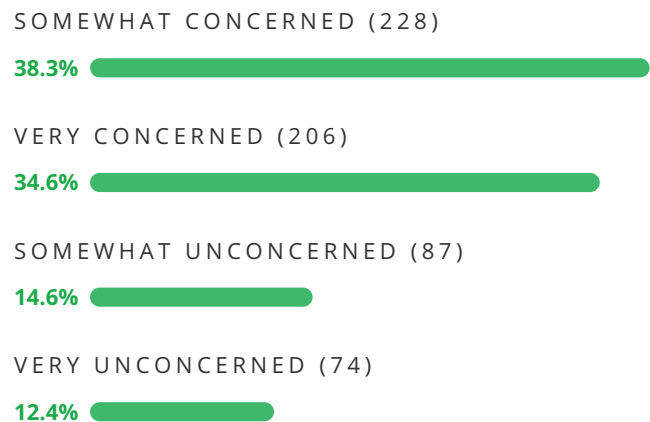
Over two-thirds of those surveyed were somewhat or very concerned about experiencing a cyber attack.

For web pros that have already experienced a cyber attack this number climbs to 81.9%.

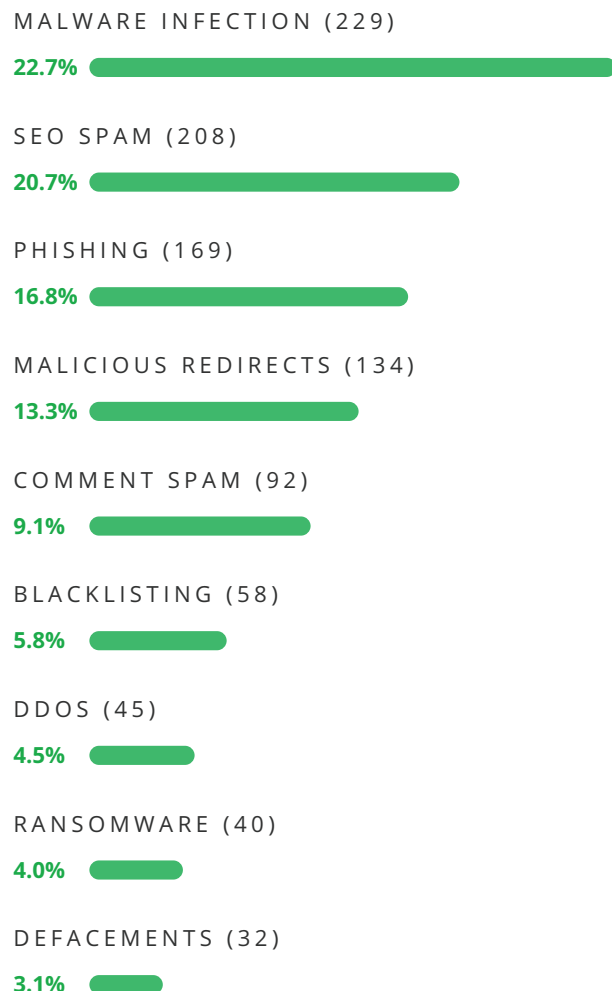
Let's take a closer look at some of the most commonly observed hacks and attacks as mentioned by the web pros surveyed.

According to our annual [Website Hack Trend Report](#), 51.3% of all infection cases in 2018 were related to SEO spam campaigns. This is one of the fastest growing malware families, can be difficult to detect, and have a strong economic engine driven by impression-based affiliate marketing.

How Concerned Are You About A Cyber Attack On Your Clients' Website?



What Issues Have Clients Experienced?



When asked about how a hack disrupted their businesses, it was not a surprise that loss of time was the most prominent response.

There are always events we recover from—the financial impact of an attack and the information lost. We then have others that are a bit more difficult to recover from: Loss of reputation, loss of business, etc. And finally, you have those that will never be recovered: Time invested in setting up your website, in maintenance and in recovery.

How Did The Hack Disrupt Your Business?

LOSS OF TIME (166)

39.3%

LOSS IN CLIENT CONFIDENCE & BRAND REPUTATION (101)

23.9%

DID NOT DISRUPT MY BUSINESS (70)

16.6%

LOSS OF REVENUE (51)

12.1%

LOSS OF CLIENT PROJECTS (29)

6.9%

PROMPTLY REPAIRED - NO LOSS (3)

0.7%

UNABLE TO REPAIR (2)

0.5%

Conclusion

This report aimed at shedding light to the web service providers relation with website security. Our main objective is to show how important website security is no matter the size of your business.

Takeaways from this report include:

- Over 50% of respondents manage less than 20 clients, and 20% manage more than 50.
- The most popular services provided are web design, development, and maintenance.
- **Less than 1%** of respondents offer website performance and security as a service.
- About half of web professionals manage web hosting for their clients.
- While WordPress makes up 50% of CMS used by survey respondents, **20% do not use a CMS.**
- Around 40% of respondents need help explaining website security to their clients.
- **Almost 70%** of respondents say that clients have asked about website security.
- Budgeting for security can be a blocker, with 45% of respondents having no budget for security.
- The most popular security features offered to clients are backups, scanning, and monitoring.
- **Less than 10%** of respondents provide protection, cleanup services, and hardening.
- A large percent of respondents use free security plugins (24%) or handle security issues in-house (20%).
- Approximately 40% of respondents pay for website security or refer their clients to a provider.
- Only 36% of survey respondents have automatic updates enabled.
- About 72% of web professionals are **concerned about experiencing a cyber attack** on client sites.
- Over **40% of respondents have dealt with a hack** on clients' sites in the past.
- When a hack occurs, 35% of respondents say it has **impacted client confidence or brand reputation.**
- Dealing with a **website hack results in loss of time for 40%** of survey respondents.

Thank you for taking the time to read our report. If there is any additional information you think we should be tracking or reporting on, [we want to hear from you.](#)

Real People. Real Security.

With Sucuri, you get a highly technical team of security professionals distributed around the world, each trained in identifying and fixing any issues you might face.



SUCURI

1-888-873-0817

| sales@sucuri.net

| www.sucuri.net

© 2019 Sucuri. All Rights Reserved.

Sucuri is a website security provider for demanding organizations that want to ensure the integrity and availability of their websites. Unlike other website security systems, Sucuri is a SaaS cloud-based solution built on state of the art technology, excellent customer service, and a deep passion for research.