

## StopTheHacker Case Study: Christopher Imaging

[Christopher Imaging, Inc.](#) is a full-service photography lab for traditional and digital photographic imaging. A third-generation family business led by CEO Todd Christopher, the company employs 25, and consists of three business divisions including a wholesale and professional sales lab, a consumer mini-lab and a portrait studio.

Christopher Imaging staff are proud of their reputation as professional photography specialists. Their reputation is bolstered by a staff of dedicated technicians with an average of 10 years seniority. They are a well-established small business with an online presence including two websites allowing customers to conveniently explore photography service offerings, view samples, place orders, and create their own mat collages without requiring an in-store visit.

### Website Blacklisting: A Malware Challenge

Christopher Imaging is one of many small businesses on the web that have increasingly fallen victim to website malware attacks. These often undetected attacks can prevent customer engagement, shrink revenues, and degrade business reputation. Every day more than 6,000 websites fall prey to web malware attacks and are blacklisted by Google as security threats, effectively removing them from search results.

For Christopher Imaging the discovery of a web malware attack on their sites came at a particularly critical time. Without their awareness, multiple malware injections had been launched, presenting a serious security breach immediately after the company's participation in a large photography event with 300 attendees—a crucial time for Christopher Imaging, which participates in only a handful of events each year to gain exposure.

“I had customers calling me stating that the website was not safe to visit,” said Christopher. “When they went to our sites, a security warning would pop up. I was actually alerted to the problem by customers who wanted to view our work from the event, so it was really bad timing that people couldn't view it. It sent me into a panic.”

The discovery of the web malware attack caught Christopher Imaging off guard and unprepared to handle the online crisis. Christopher immediately searched Google for his business sites to confirm the problem, while at the same time trying to figure out what was going on. He discovered that two of the websites had been infected, preventing customers from ordering, stopping lab production, and diverting potential sales to competitors.

“When I realized our sites were down and started searching Google, I realized that Google had blacklisted us. I was trying to figure out what was going on—why Google had us blacklisted, and why our site was shut down,” Christopher said. “I immediately contacted Google, and they confirmed that we were blacklisted as a result of a malware infection.”

### **An online crisis solved through StopTheHacker website scanning and malware removal**

Though Google blacklisting seemed to be the immediate source of online frustration, Google was also the resource Christopher Todd turned to for a finding a solution to the crisis. After confirming the infection and subsequent Google blacklisting, he also turned to Google to look for solutions to the problem. His search led him to review the websites of a number of potential malware protection providers, but StopTheHacker, a leading website security service company, is where his website malware troubles stopped.

“I found StopTheHacker on the Internet and learned they are more on the cutting edge of this type of service. Once I found them and read about their use of AI-based analytics and machine learning to detect and resolve new malware attacks, it didn’t take me long to give them a call. ”

That call quickly made a believer out of Christopher. Through its suite of malware detection, removal and website protection services, StopTheHacker was able to get Christopher Imaging’s website back up and running quickly, restoring visitors’ to access their photos within hours of the security breach. While the breach could have significantly impacted sales and exposure, Christopher Imaging was able to turn the situation around in short order.

“I was very pleased at the speed of StopTheHacker’s response. What I really appreciated was their personal involvement in our problem. They took control over a situation I didn’t have the background to resolve on my own,” Christopher said. “ And it turns out they became a quick and easy solution for me. Now both of our Christopher Imaging sites are now protected by StopTheHacker to prevent future malware attacks, yet we have the added flexibility to turn on and off certain protection features as needed. Working with StopTheHacker turned a negative into long-term a positive.”

**Benefits of StopTheHacker for Christopher Imaging:**

- Automatic prevention, detection and recovery from malware and hacker attacks.
- Continuous threat scans providing constant website security protection.
- Self-adapting capabilities that constantly monitor new strains of malware, building profiles.
- Reduced risk of infecting visitors and eliminating malware removal by inexperienced users.

###