7 Deadly Sins

Magecart/Credit Card Skimming Attacks

THE MEDIA TRUST
We know digital security.

7 Deadly Sins: Magecart and Credit Card Skimming

You may not realize it, but there are several common risk factors that make organizations vulnerable to Magecart and credit card skimming attacks. Take 7 minutes to read this list and gauge your site's risk profile.

1. You don't know who is interacting with your customers and visitors

Many organizations have no idea what code exists in their digital ecosystem at any one point in time, let alone how that code changes from day to day. Digital is dynamic. Unless you have 24/7 monitoring or a team of analysts constantly reviewing each page of your website, there is no way to determine if you are under a Magecart attack.

2. > 90% of your digital ecosystem is outside your control

Websites have become increasingly complex, and as a result, sites are no longer constructed in-house, but leverage third-party vendors to deliver a great customer experience. Data from monitoring top retail, hospitality and media websites reveals that 90% of the digital experience is powered by third parties, further increasing your risk of a breach since Magecart attacks often are launched from third-party code. (Just ask Ticketmaster)

3. Traditional security doesn't protect against Magecart attacks

Traditional security operates from a network perimeter defense approach, focused on protecting the data on systems inside the organization, such as employee computers and corporate servers. Given the growing importance of websites and mobile apps to an organization's success, you need step outside of traditional security and evaluate what renders on your customer's browser when they visit your site.

4. No one group is responsible for preventing Magecart attacks

IT, Information Security, Application Security, Marketing/Ecommerce, Data/Legal Compliance teams play their own part in website and mobile app security. However, these groups are rarely well-connected in their approach to security, and often no one group takes the lead in coordinating efforts to prevent Magecart and credit card skimming attacks.

5. Organizations don't connect the dots between digital, privacy, security

A corollary to #4, different teams have different perspectives regarding the impact of third-party code on the website. Marketing/Ecommerce view it as critical functionality to drive revenue; Legal and Compliance considers it a threat to the regulatory environment and data leakage; Security sees it as a lurking malware threat. This lack of a common view leads to a disjointed approach to protecting against Magecart.

6. Audience extensions and revenue growth lead to risky behavior

Marketing/Ecommerce teams are hyper focused on driving revenue through the website and mobile app, which often translates into using third-party applications to improve customer acquisition and retention, and improve the customer experience (better personalization, advanced metrics, video, online chat, etc.). Revenue is king, and the rush to add functionality using third-party vendors puts the site at significant risk.

7. Magecart continues to evolve in sophistication

Analysis of Magecart attacks over the last several years shows an increasing level of sophistication. As traditional tools and IT teams detected one breach and one attack, the bad actors continue to evolve the code, thereby rending perimeter defense or traditional anti-virus approaches obsolete. Magecart often gains access via third-party code and mirrors the payment page and checkout process functionality so that website visitors do not recognize the attack, allowing them to continue for many months.