Leading Conversion Platform, Picreel, Releases Response To Security Breach: Zero Data Compromised

All client and company data, including payment data, personal data, passwords, company or customer data, is safe, and no data has been compromised.

RENO, NV, USA, May 22, 2019 /EINPresswire.com/ -- Picreel, the leading conversion rate optimization platform that uses popup offers and onsite retargeting to help website owners convert more visitors into buyers and subscribers, releases official response to recent attempted security breach. All client and company data, including payment data, personal data, passwords, company or customer data, is safe, and no data has been compromised.

> “In addition to the built-in security system that automatically detected and prevented the attack, Picreel customer data is maintained outside of the company's front end servers.”
>
> *Kevin Petersen*

On May 12, 2019, the JavaScript code that Picreel clients install on their websites was targeted by a malware program out of Panama. The hack attempt on Picreel servers triggered a security switch that temporarily halted access and paused all customer ad campaigns. For a brief moment, the Picreel code was prevented from running and any Picreel functionality would have been disabled.

Because the malware was immediately identified and security measures were automatically initiated to prevent the Picreel code from running, no client or company data was impacted, stolen, viewed, or otherwise affected.

"Hackers with servers out of Panama are regularly trying to access various sites around the world - which is why we had that safety system built into our script. When the hacker code tried to attack Picreel, the script that Picreel clients install on their websites was automatically deactivated. Although this prevented popup offers from launching when a visitor came to a site - it also prevented the hacker from capturing any information," said Kevin Petersen, General Manager at Picreel.

Data security has always been a top priority for Picreel. In addition to the built-in security system that automatically detected and prevented the attack, Picreel customer data - including account

and payment profiles - is maintained outside of the company's front end servers. Any hack attempt on the Picreel website, while possibly disruptive to customers' advertising campaigns, is not connected to any sensitive data. Furthermore, Picreel customers' marketing leads are secured in a separate database.

Since the attempted hack, Picreel has added additional security measures to defend against future attacks. The company has also assigned a dedicated resource to ensure the security of all client installed JavaScript code, and is currently running a validation script to verify that the code on customers' sites has not been corrupted. The company will notify only those customers whose code has been altered, regardless of whether it was related to this incident.

"When we see issues like this, including ransomware, we routinely collect hackers' IP addresses and send them to the cyber crimes unit of the FBI. However, it is not practical, useful, nor actionable to notify our entire customer base every time we receive a ransomware email or other threat. Our policy is to notify customers affected by any level of breach or data loss, and to date, Picreel has never experienced a loss of data," concluded Petersen.

Customers can view Picreel's complete Privacy Policy here.

The company encourages customers to check Google's Transparency Report to view Picreel's "safe status" in real-time. It also recommends Picreel customers maintain their own website security protocols to keep hackers and malware from propagating malicious code on their servers.

About Picreel: Picreel is a conversion rate optimization software company with more than 10 years' experience helping website owners get more customers with fully customizable popup overlays, surveys and links that capture website visitors before they leave a site.

Chris Browne
Picreel
+1 888-891-5782
email us here
Visit us on social media:
Facebook