



website

MAGAZINE

THE MAGAZINE FOR WEBSITE SUCCESS

WEBSITEMAGAZINE.COM

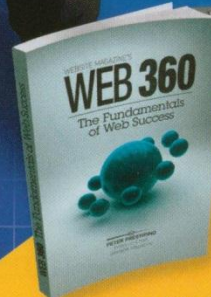
NEW DEMANDS ON

WEB DESIGN

- >> Improve Opt-in Email Lists
- >> Social Media for Merchants?
- >> Data-driven Link Building

PLUS: Top 50 Domain Registrars and Hosting

JUNE 2011/SPECIAL ISSUE
\$6.99 US



FREE BOOK

with Pro Subscription
web360book.com



Trends in E-commerce Fraud Prevention

By Reed Taussig

With the growing prominence of online activities, from e-commerce to online banking, businesses are continually striving to keep up with the latest technologies that combat online fraud. The fraud prevention industry saw a lot of changes in 2010; notably in the rapid growth of e-commerce greatly outpacing the use of fraud prevention technology to protect online transactions.

In light of the persisting issue of fraud prevention, what can brands do to better protect themselves — and the consumers who frequent their sites — against fraudsters? There are a few key trends and predictions in online fraud prevention to be aware of in 2011.

Identifying Visitors without the Use of Cookies

It's a reality that today's fraudsters are becoming savvier, and consumers more concerned with online privacy. Consequently, we're seeing consumers deleting or blocking cookies, or having cookies deleted via their computer security software. This makes it more difficult to detect repeat customers and, by extension, fraudsters that will try to escape re-identification.

Recent upgrades to browsers like Firefox and Internet Explorer reveal further testimony toward moving away from cookie-based fraud detection. The newly released versions of these browsers, Firefox 4, Google Chrome and IE9, allow users to block sites from tracking their activity. This type of private browsing renders cookie-based detection obsolete.

We recommend researching and implementing new cookieless approaches to identifying fraudsters based on the digital fingerprint left by a visitor's computer when they transact with your site. This digital fingerprint includes markers such as the computer's screen resolution, fonts and plug-ins installed on the browser, and can be an effective way of recognizing repeat transactions from the same fraudster even when they change IP addresses and customer details.

Online Privacy Debate

Another pressing topic in the world of fraud prevention is around recent legislation, such as that proposed by the FTC which is designed to protect consumer privacy as it relates to behavioral advertising. As part of this, the fraud prevention industry widely asserts that companies engaged in cyber security should not be included in the suggested framework.

Although some people are concerned about their information being used for advertising purposes, they may be less concerned with their information being used for transaction security purposes. They should, however, be concerned about identity fraud leading to financial and reputational harm against them. In fact, the importance of cyber security, and the nature of the data collected, requires that it be treated differently than consumer data collected for advertising purposes. There may be unintended economic and security consequences for this do-not-track legislation.

For instance, one of the concepts the FTC staff is pushing is one of "transparency", which could be viewed as the need to disclose the manner in which collected information is used. Extensive disclosure would expose to fraudsters the techniques used to discover risk of fraudulent activity and thereby enabling the fraudster to develop workarounds or alternative technologies. There is specific concern regarding deep-packet inspection and data enhancement

ClickStream Web

in this regard, as specific disclosure of the manner in which data is used relative to these techniques could provide fraudsters with important information.

Senators John McCain and John Kerry are currently circulating proposed legislation to create an "online privacy bill of rights", in support of efforts to curb the Internet-tracking industry. As more is done with privacy legislation there will be continued focus on the role of cookies for fraud-prevention purposes.

We recommend that e-commerce retailers educate themselves about these well-intentioned but potentially dangerous proposals so that merchants are not unrealistically burdened with increased implementation, compliance and fraud costs.

Increase in Mobile Transactions and Digital Goods

Mobile has the ability to impact all aspects of fraud prevention. It brings to surface an entirely new set of fraud issues prompted by changing consumer behaviors, new devices and connectivity options.

The first is that IP addresses routing for mobile devices — including smartphones and tablets — is different from PCs or fixed computers. Mobile devices can appear to connect through a Wi-Fi network at a coffee shop in one transaction, and then in the next second appear to come from a mobile 3G gateway located many miles away. This information makes it nearly impossible for online retailers to detect the source of a transaction — an assessment that is imperative in monitoring fraudulent activity.

The second issue is the fact that mobile devices have more limited digital fingerprint attributes to track. For example, the iPhone does not allow the use of Flash, which is sometimes used by advertisers to identify visitors and is frequently used by e-commerce merchants and financial institutions to validate returning customers. Apple's Safari browser also provides less opportunity for digital fingerprinting.

The third issue is that mobile users and casual gaming will also increase the volume of digital goods purchases. Because authorization of digital goods must be instant, there is no opportunity for manual review. In addition, fraudsters can automate digital goods purchases and then resell those items electronically from anywhere in the world. This further exacerbates the problem.

Due to mobile's emerging prevalence, it is important to review its impact on existing device identity and behavior-based fraud filters, as well as centralizing fraud intelligence across all Web, app and mobile transactions in order to improve detection rates and reduce costs.

New fraud prevention solutions will reflect changing consumer behaviors and more practiced and sophisticated fraudsters in 2011. Ever-expanding online fraud techniques demonstrate every evidence that online fraud will expand beyond traditional computer devices into mobile and tablet-based devices in the coming years. Every business that transacts on the Internet needs better fraud prevention solutions as fraudsters become increasingly confident. ■

Reed Taussig, the president and CEO of fraud detection solutions provider ThreatMetrix, has more than 30 years of experience in the computer hardware and software fields. Prior to ThreatMetrix, Mr. Taussig was president and CEO of Vormetric, Inc., a leader in data privacy and protection. Contact Mr. Taussig at rtaussig@threatmetrix.com.



The ONLY professional Do-It-Yourself online video platform that gives you total control!

From one file, deliver video to any OS, browser or mobile device - live, on demand, pay per view or subscription.



On Demand & Live



Mobile



Pay Per View



Live to Mobile



Video Email



Secure & Private Access



html 5



Social



Statistics

Starting at 59⁰⁰/month

www.clickstreamtv.com

877/982/5425

Reseller Opportunities Available:
resellers@clickstreamtv.com