SPRING 2017 E-NEWSLETTER

At Digital Mountain we assist our clients with their cybersecurity, computer forensics and e-discovery needs. For this E-Newsletter, we discuss Internet cookies and the data security, privacy and legal impact it has on organizations and their employees.

Taking a Nibble out of Internet Cookies – Managing Organizational Risk

Marketing dollars on digital advertising will top $335 billion and represent more than 46% of total media advertising by 2020, according to market research firm eMarketer, Inc. Original Internet cookies were a fundamental tool that Web site providers deployed to optimize users' experiences – leveraging user information stealthily gathered from past visits to better ensure a positive browsing experience. Over time, however, organizations developed new flavors of cookies, such as session cookies, persistent cookies, HttpOnly cookies, SameSite cookies, secure cookies, Third-Party cookies, supercookies, and zombie cookies. Newer forms of cookies are valuable in advertising because they enable marketers to track, among other things, websites visited by a particular user enlightening that user's interests, challenges, preferences, and desires. The powers of cookies are such that mismanagement of them can create serious privacy and security vulnerabilities within an organization. This article takes a nibble out of "third-party cookies", which fuel the lofty advertising revenue projections and recommends how an organization can begin to minimize exposure from cookies and other related risks on the horizon.

By default, Internet Explorer, its replacement Microsoft Edge, and many other browsers enable cookies to be exchanged between their browsers and third-party web sites. Users can disable the default sharing setting or create an alert to advise a user about third-party access, prompting for consent to allow a third-party web site to have access. An illustrative example is Facebook: if you visit facebook.com after configuring your browser to send alerts versus block third party websites, you'll notice many third-party websites are seeking to access your cookies. The frequency of the alerts becomes unbearable when surfing the Web, so many users revert to allowing access by default or block cookies entirely. Not all browsers employ this invasive yet optimizing cookies setting by default; Safari actually blocks cookie exchange between your

browser and third-party websites. Thus, when using Internet Explorer or other browsers that have third-party cookies enabled, we recommend turning off this third-party cookie setting which tracks user activity across multiple sites.

Cross-device tracking is an emerging issue, which in a way encapsulates cookies, whereby convergence of communication infrastructure occurs with one provider for Internet access, cable access, and phone access. Convergence enables providers to control, analyze and monetize user traffic patterns and preferences.

New devices also increase the tracking risks. Smartphones can track more information about a user than a desktop or laptop computer depending on how the device is configured. Apple, for example, uses an approach called "identifier for advertisers" (IDFA). With IDFA, a unique identifier is assigned to every user that buys an Apple iOS device. This identifier is used by Apple's advertising network. Some cookies on smartphones are able to track IP address, Unique Device Identifier (UDID), geolocation, and other identifying data to ascertain which ads to deliver to the device. A UDID is specific for each Apple device and is a sequence of 40 letters and numbers that is specific to the device.

We've provided you with just a nibble of the Web-based cookies market. If you're hungry to learn more, there are many other types of cookies to digest. Until then, *an organization should seek to properly configure privacy and security in its employee browser settings based on the organization's risk profile*.

Please direct questions and inquiries about cybersecurity, computer forensics and electronic discovery to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

Internet of Things World
Santa Clara, CA: May 16-18, 2017

ISSA 9th Annual Information Security Summit
Los Angeles, CA: May 18-19, 2017

ENFUSE 2017
Las Vegas, NV: May 22-25, 2017

"The Exchange" Data Privacy and Cybersecurity Forum
New York, NY: May 23-24, 2017

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.

4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: