NJCCIC

NJ CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL

THE WEEKLY BULLETIN | December 30, 2015

NJCCIC Blog: Onward to 2016...

2015 has been quite a year for New Jersey's cybersecurity. As it comes to an end, it's worth noting a few highlights from the last year and foreshadowing what lies ahead in the new year.

Read full blog post here

Breach Notification

Hyatt Notifies Customers of Malware Activity

On December 23, Hyatt Hotels Corporation announced it was investigating a point-of-sale malware breach that may have compromised payment card transactions at an unknown number of Hyatt-managed properties. Hyatt customers can visit www.hyatt.com or call 1-877-218-3036 for more information. ***NJCCIC comment: This incident underscores a notable trend in PoS breaches targeting the hospitality industry, as Hyatt joins a number of other large hotel chains that announced data breaches this year, including Hilton, Starwood, Mandarin Oriental, and the Trump Collection.***

LiveStream

On December 23, the Brooklyn, N.Y.-based streaming service, LiveStream, warned customers that an unauthorized individual

Latest Cyber Alerts

Vulnerabilities in Joomla

Vulnerabilities in Adobe Flash Player and AIR

Vulnerabilities in Google Chrome

AVG Anti Virus Chrome Extension Vulnerability Alert

Vulnerabilities in Google Android

Cyber News

191 million voters' personal info was exposed by misconfigured database
via Databreaches.net

Former Morgan Stanley Financial Advisor Sentenced for Illegally Accessing Confidential Client Information
via FBI New York

may have accessed a database containing users' names, email addresses, encrypted passwords, and if provided, date of birth and/or phone numbers. Users are advised to change their LiveStream passwords, and any other online accounts that shared the same credentials.

[2016 Reality: Lazy Authentication Still the Norm]
via KrebsOnSecurity

[The Fraud Tsunami Heads To The Sharing Economy]
via Dark Reading

Tip of the Week

"Recognizing Fake Antiviruses"

Fake antivirus is malicious software (malware) designed to steal information from unsuspecting users by mimicking legitimate security software. The malware makes numerous system modifications making it extremely difficult to terminate unauthorized activities and remove the program. It also causes realistic, interactive security warnings to be displayed to the computer user.

Get cyber tips like this and more from US-CERT

Questions?

Email a Cyber Liaison Officer at
njccic@cyber.nj.gov.

---

cyber.nj.gov

New Jersey Cybersecurity & Communications Integration Cell

information about TLP, see https://www.us-cert.gov/tlp/.

Share this email:

communications@njohsp.gov
Trenton, NJ | 08625 US