MC^3 Newsletter

December 2017

VOLUME 34 NUMBER 11

The December meeting of the McHenry County Computer Club is **December 9th**, at the Senior Services Associates 110 W. Woodstock Street, Crystal Lake, IL.

NOTE: *Park across the street and enter at the south door, or enter at the west side and park along the side or rear of the building.*

Meeting Agenda

- Introductions & Reports
- 2018 Elections
- Latest W10 & it's Good Things - Al Edlund
- Q & A

Upcoming Demos - Subject to Change

- Backing Up to an External HD - Bob Wagner

November Q & A

The editor has not received any questions and answers from November.

US Airlines to limit smart luggage - CNET

New rules require removal of lithium ion batteries from luggage before being checked -- a task impossible for some bags.

Many major US airlines have announced restrictions on so-called smart luggage out of concern their lithium ion batteries may pose a fire risk.

Smart luggage tends to contain a USB port for charging devices, GPS to track the bag's location, remote locking and built-in weight sensors. Some even sport a motor to propel the bag for ease of movement through an airport.

These features require power that is often supplied by built-in lithium ion batteries, which contain highly flammable liquid. Worried the batteries could cause a fire in the cargo hold that

continued on next page

McHenry County Computer Club
Established 1982
MC^3

Our membership is $26.00 a year.

NOTE: This fee offsets the running of the club; membership benefits include help with computer problems. Please pay Lyle Giese, our treasurer, or the designated Board Member in his absence.

MC^3 OFFICIALS

President:
Larry Freeman
lpfreeman@hotmail.com

Vice President:
Bob Wagner
rmwagner@ameritech.net

Secretary:
Bruce Eckersberg

Treasurer:
Lyle Giese
lyle@lcrcomputer.com

Database Manager:
Lem Erita

Newsletter:
info@Mc3ComputerClub.org
(for articles & suggestions)

Past President:
John Katkus

Webmaster:
Cindi Carrigan

Board Members:
Jack Luff, Dave Lutes,
Jim Beierle, Al Edlund,
Ken Schuring

would go undetected, airlines are instituting new rules that require fliers remove the batteries when they check their luggage and carry them into the passenger cabin.

“Beginning Jan. 15, customers who travel with a smart bag must be able to remove the battery in case the bag has to be checked at any point in the customer’s journey. If the battery cannot be removed, the bag will not be allowed,” American Airlines said in a statement on Friday. Delta and Alaska soon followed suit with similar policies on their flights.

In the past couple of years, the use of lithium ion batteries has been linked to fires and spewing smoke in a slew of products, including Samsung’s now-canceled Galaxy Note 7, hoverboards, and Boeing’s 787 Dreamliner.

The Federal Aviation Administration issued a warning about the batteries last year, urging airlines to examine the risks associated with transporting lithium batteries as cargo, including “the potential risk for a catastrophic hull loss.” The alert covered batteries being transported as components and not those already inside devices such as laptops, tablets, phones or hoverboards.

However, many bags have batteries that can’t be removed, and that has smart luggage makers like Bluesmart worried.

“We are saddened by these latest changes to some airline regulations and feel it is a step back not only for travel technology, but that it also presents an obstacle to streamlining and improving the way we all travel,” Bluesmart told CNN.

Risky Scripts Pose Threat to Web Surfers, Say Researchers - TECHNEWSWORLD

A popular technique used by website operators to observe the keystrokes, mouse movements and scrolling behavior of visitors on Web pages is fraught with risk, according to researchers at Princeton’s Center for Information Technology Policy.

The technique offered by a number of service providers uses scripts to capture the activity of a visitor on a Web page, store it on the provider’s servers, and play it back on demand for a website’s operators.

The idea behind the practice is to give operators insights into how users are interacting with their websites and to identify broken and confusing pages.

“You use session replay scripts to find out where all the dead zones are on your website,” said Tod Beardsley, director of research at Rapid 7.

“If you have a space for a ‘click here for 10 percent off’ and no one clicks there, there may be a problem with that page,” he told TechNewsWorld.

The scripts also can be used for support and to troubleshoot user problems, Beardsley added.

Peeping Scripts

However, the extent of data collected by the scripts far exceeds user expectations, according to researchers Steven Englehardt, Gunes Acar and Arvind Narayanan.

Text typed into forms is collected before a user submits the form, and precise mouse movements are saved -- all without any visual indication to the user, they noted in an online post.

What's more, the data can't be reasonably expected to be kept anonymous.

"In fact, some companies allow publishers to explicitly link recordings to a user's real identity," wrote the team. "Unlike typical analytics services that provide aggregate statistics, these scripts are intended for the recording and playback of individual browsing sessions, as if someone is looking over your shoulder."

That means that whether a visitor completes a form and submits it to the website or not, any information keyed in at the website can be seen by the operator.

"Even if you deleted the data you entered into a form, it would be exposed and visible to the website owner," said Abine CTO Andrew Sudbury.

"You're being recorded when you think you aren't, so you might reveal things you wouldn't reveal if you knew you were being recorded," he told TechNewsWorld.

read more