MC³ Newsletter

September 2017

VOLUME 34 NUMBER 8

The September meeting of the McHenry County Computer Club is **September 9th**, at the Salvation Army Building, 290 W. Crystal Lake Ave., in Crystal Lake.

Meeting Agenda

- Introductions & Reports
- Q & A
- Anniversary Party

Upcoming Demos - Subject to Change

- October 2017: "Team Viewer" - John Katkus

August Q & A

There are no questions and answers this month.

IMPORTANT NOTE!!

The November and December 2017 meetings will be held at **Senior Services Associates**
110 W. Woodstock Street
Crystal Lake, IL

This is due to the Salvation Army's holiday Red Kettle program.

From USA Today - Elizabeth Weise: September 7, 2017

What to do if you're one of the 44% of Americans hit by the Equifax breach

An estimated 143 million U.S. consumers could be affected by a cybersecurity attack carried out against Equifax, one of the nation's three largest credit-reporting companies.

Normally one of the first things victims are told to do is to go to a credit-reporting company and request their records to make sure that there are no unauthorized accounts or charges on their existing accounts.

This time around, experts suggest checking with Equifax ri*vals, Experian and TransUnion.*

continued on next page

McHenry County Computer Club
Established 1982
MC³

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.

MC³ 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

While there is no evidence of unauthorized activity in the Equifax credit reporting databases, the company said that there was potential unauthorized access to information it had stored from mid-May through July 2017. The information included names, Social Security numbers, birth dates, addresses and, in some cases, driver's license numbers.

The hackers also got access to credit card numbers for roughly 209,000 consumers, plus certain dispute documents with personal identifying information for approximately 182,000 consumers, Equifax said.

In the wake of this breach, experts counsel several immediate actions:

BE EXTRA CAREFUL ABOUT EMAILS AND LINKS

Users should avoid clicking on links or downloading attachments from suspicious emails that claim to be updates from Equifax or connected to the breach.

Equifax will send paper mail to consumers whose credit card numbers or dispute documents with personally identifying information were impacted. It has also created a dedicated website for consumers to see if they were affected at www.equifaxsecurity2017.com. They can also call the Equifax call center at 866-447-7559.

Hackers often use news of big breaches to conduct "phishing" campaigns, sending official-looking emails that make it seem as if the affected company or other legitimate services are asking them to supply information or click through to a link to repair any damage.

When in doubt, call or email the company that appears to be sending the message separately, don't go through the email you've been sent.

CHANGE PASSWORDS

Especially if you typically use similar passwords and security questions on multiple accounts, do this. Once hackers have access to ID and password information for one system, they routinely try the same combination against multiple other platforms to see which ones work, an easily automated process.

ENABLE TWO-FACTOR AUTHENTICATION

For the vast majority of victims who didn't have credit information compromised, the biggest risk here is that a criminal uses this information to answer your "security questions" and reset your password.

That usually sends a password reset to your email account, so making sure that email account is secure should be your primary concern, said Nathaniel Gleicher, head of cybersecurity strategy for Illumio, and former director of cybersecurity policy for the White House under President Obama.

Two-factor authentication keeps them from doing that by sending a text message or call to the user's phone with a code as a second verification step. The code which must be typed in before the account can be opened.

CHECK YOUR CREDIT CARD AND OTHER ACCOUNTS

Review your online accounts for suspicious activity. That includes banks, credit card companies and hotel and airline loyalty programs. Hackers frequently slice and dice information from large data breaches, selling groups of user information for specific companies on the dark web. Even the smallest accounts can be bundled together into a large group to be sold.

Read more at https://www.usatoday.com/story/tech/news/2017/09/07/what-do-if-youre-one-44-americans-hit-equifax-breach/644406001/

From Talking Tech - Brett Molina: September 7, 2017

Hurricane Irma boosts downloads of walkie-talkie app Zello
The go-to app during rescue efforts in Houston following Hurricane Harvey is rising in popularity as Hurricane Irma speeds toward Florida.

Zello, a walkie-talkie app where users can push a button to talk to any one through a cellular or Wi-Fi connection, is the most popular free app on both Android and iOS app stores.

According to mobile app research firm App Annie, Zello moved to the top spot on Apple's store Tuesday, then reached the top of Google Play on Wednesday.

Zello was among the key tools used by rescuers to help victims of Hurricane Harvey in Houston. Last week, Zello CEO Bill Moore said 20 times as many new users in Houston were on the app compared to the previous week.

"It's centered on live voice," said Moore. "Our voice is how we most naturally communicate. A few seconds of voice has so much information on emotion, education, gender, what part of the country are they from.

How it works

Once users create an account, they explore a variety of channels to join and chat. In the case of Harvey rescue efforts, channels such as the Cajun Navy Dispatch and Harvey Animal Rescue appeared where users could quickly push a button to talk and seek help.

There is some potential for confusion as users parse which channels are linked to official rescue groups. Recently, a channel for Texas Search and Rescue was pulled after the official group claimed their logo and name were misused, said Moore.

The technology for Zello dates back to 2007, and saw boosts in use during global uprisings, including ones in Egypt and the Ukraine, as well as protests in Venezuela. Zello was blocked during several of these events, most recently in Russia in April.