MC³ Newsletter

February 2018

VOLUME 35 NUMBER 2

The February meeting of the McHenry County Computer Club is **February 10, 2018 at Salvation Army Building 290 W. Crystal Lake Ave., in Crystal Lake, IL.**

NOTE: *Enter the building on the parking lot level under the awning.*

Meeting Agenda

- Introductions & Reports
- Protecting Your PC from RansomWare - John Katkus
- Q & A

Upcoming Demos - Subject to Change

- TBD

January Q & A

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

Missing SD Cards

There are 2 missing SD cards for the video recorder. Has anyone seen them? Let Bob or Larry know. Thanks!

Former Execs Team Up to Fight the Tech Addiction Monster - David Jones, TechNewsWorld

A group of former Facebook, Google and Mozilla executives have joined forces with the Time Well Spent advocacy group to establish the Center for Humane Technology (CHT), a new organization dedicated to combating the growing problem of addictive behavior among social media users.

The new center, along with the children's advocacy group Common Sense, on Monday announced a campaign to help change the social media model. Its goal is to lessen the negative impact of automation and other technologies on the development of children and young adults, who are considered highly vulnerable to the most damaging aspects of social

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

media.

“Tech companies are conducting a massive, real time experiment on our kids, and at present, no one is really holding them accountable,” James Steyer, CEO of Common Sense.

Teenagers polled in a 2015 survey used social media for an average of nine hours of per day, Common Sense found. Half of the teens admitted to feeling addicted to their mobile devices, and 60 percent of parents felt that their kids were addicted.

“We desperately need to moderate this behavior, as it is having an adverse impact on virtually everything we see and touch, ranging from personal priorities to who runs our government,” Enderle told TechNewsWorld.

“We are currently largely unable to tell bad actors from good, or fake from real news,” he added, “and the very young and old are most vulnerable.”

The move toward advanced automation and robotics makes addressing this issue even more urgent, Enderle said.

Twitter posts its first quarterly profit as ad sales rise - BBC News 2/7/2018

Twitter has reported its first quarterly net profit helped by a rise in video advertising sales.

The news gave a massive boost to Twitter’s shares which closed 12% up on the day.

That was despite the number of people using the social network coming in below expectations.

Twitter’s previous failure to make a profit had confounded investors given its widespread use and popularity among celebrities and politicians.

Net profit was $91.1m in the fourth quarter of 2017, compared with a loss of $167.1m for the same period a year ago.

Twitter, which has posted consistent losses since it became a public company in 2013, said it expected to be profitable for the full year of 2018 as well.

The company has found success with video and other changes, deepening the experiences on offer, James Erkine, director at marketing firm The Social Circle, told the BBC.

“It’s now about taking that scalable model and using it to reach new user groups to increase their user base,” he said.

“Hopefully now they’ve made a profit once, they should be able to do it next quarter and carry on doing it.”

Jackpotting: hackers are making ATMs give away cash - Samuel Gibbs, The Guardian

Cybercriminals are hacking cash machines to force them to give out money in what is known as "jackpotting", according to two of the world's largest ATM makers and the US Secret Service.

Diebold Nixdorf and NCR sent out an alert to their customers over the weekend, but did not identify victims or specify how much money had been stolen. The US Secret Service started warning financial institutions that jackpotting was now a risk in the US last week, having started in Mexico last year, according to a confidental alert seen by Krebs on Security.

Diebold Nixdorf said that authorities had warned the company that hackers were targeting its Opteva ATM model , which went out of production several years ago.

NCR said: "This should be treated by all ATM deployers as a call to action to take appropriate steps to protect their ATMs against these forms of attack."

Jackpotting has been rising worldwide in recent years, though it is unclear how much cash has been stolen because victims and police often do not disclose details. Hackers require physical access to the cash machine using specialised electronics and malware to take control, including an endoscope.

Once taken over, the machines can be forced to dispense money at a rate of 40 notes every 23 seconds until it is empty, according to the Secret Service. The only way to stop the machine spitting out cash is to press the cancel button on the keypad.

Criminals have been targeting cash machines in pharmacies, retailers and drive-through ATMs, according to the Secret Service.

Attackers in Mexico have been using variants of the Ploutus malware, first spotted in 2013, according to security firm FireEye. It is believed that US cybercriminals are using similar techniques.

In security push, Chrome will soon mark every HTTP page as "non-secure" - Zack Whittaker, 2/8/2018

Google has said starting later this year its Chrome browser will mark all websites that haven't adopted HTTPS encryption as "not secure."

That means any site that doesn't load with a green padlock or a "secure" message in the browser's address bar will be flagged as insecure.

Emily Schechter, Chrome security product manager, confirmed in a blog post that the changes will come into effect with Chrome 68, scheduled for July.

"For the past several years, we've moved toward a more secure web by strongly advocating that sites adopt HTTPS encryption," she said in the blog post published Thursday. "And within the last year, we've also helped users understand that HTTP sites are not secure by gradually marking a larger subset of HTTP pages as 'not secure'."

It's the latest escalation in the search and browser giant's effort to gradually push more webmasters

into adopting HTTPS, a secure encryption standard for data in transit. That means any data sent from your computer or device to that website is transmitted securely and can't be intercepted by an attacker. Because HTTPS wraps a secure tunnel around the site and its user, the encryption also serves as a way to ensure that the content hasn't been modified by an attacker.

The company has employed several other tactics, including ranking sites with HTTPS higher in its search results, as an incentive to drive web developers to adopt the technology.

According to Google, 81 out of the top 100 ranked global websites now use HTTPS by default.

But there are thousands of news and other popular websites that still haven't made the leap (ZDNet included).

For smaller and younger sites, transitioning to HTTPS can be a breeze. Many hosted solutions and servers offer plug-and-play certificates to enable website encryption in a flash. But for larger, sprawling, and legacy sites, HTTPS can be a nightmare. That's because everything on the domain has to be secured -- and a single outlying element can reduce a page to an insecure one.