MC³ Newsletter

March 2018

VOLUME 35 NUMBER 3

The March meeting of the McHenry County Computer Club is **March 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
- Demo: A Sampling of APCUG Content by Larry Freeman and Ken Schuring
- Q & A

Upcoming Demos - Subject to Change

- We need demos for April and May - Please submit ideas to any MC3 board member

February Q & A

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

Three Questions to Ask Before Downloading an App - Ron Yokubaitis, Stay Safe Online

Data collection is a brave new world for consumers and companies alike. There is no escaping it, nor is there the ability to avoid it at some level. That is why many privacy conscious consumers seek out virtual privacy networks (VPNs) in order to attain some shred of discretion. This conundrum begs the question, “How do you scrutinize before downloading?”

Generally, consumers should be more skeptical when selecting their apps. There are pitfalls when choosing something about which you’re not completely educated. Ironically, the internet isn’t the best place to help, as reviews are often designed to push you toward a particular product more than help you make an informed decision.

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

That's why in today's app-happy climate recent headlines should have you questioning the way we choose applications for ourselves as well as our children. Life was simpler when the con artists used known buzzwords like "Nigerian Prince" in their email to coax you for information. Before that, golden-agers like myself would use the term "Trojan Horse." Today's phrase seems to be "app of the day."

The first question you need to ask before downloading an app is, what is the company's privacy policy? These policies can be long and burdensome to read, and that is how they are intended to be perceived. The lack of time in your busy life is what some companies rely on to make money. Try to scan the policy to find out how they intend to use your personal information and data they collect through the app; this will give you an idea of what they do with your info.

Second, if the app is free, you should ask yourself how this company makes money. The company is obviously spending thousands of dollars on PR and marketing efforts to get its "free service" in front of you. You have to wonder who would finance this kind of operation. If a business is not charging for their services, there are several ways it can make money – it can allow other companies to advertise to you through the app, or it can sell your data – such as tracking your regular location stops, shopping habits or frequent searches – to third parties. Some companies make money doing a combination of both, and oftentimes, this information is not easy to find because it would make you reconsider downloading.

Finally, you should ask, who is behind this company? Too many bad actors rely on the consumer instinct to leap before they look to simply hide who is behind the business by not revealing any information. The absence of a company history or contact information should raise red flags aplenty. If there are no photos, no bios of the company executives and no way to contact a business, then how can you decide whether you can trust this company with your data?

Another word of caution for consumers is that even a genuine company that has the latest and greatest app should not automatically justify downloading. Take the recent mess from Strava, for example. Strava is an exercise app designed to "enhance" your sports activity by sharing your workout paths and allowing you to see other popular trails to get your fit on. When the company published a global map of users' cool paths, a detailed trail some military personnel use to exercise was revealed to the world, along with a layout for a few secret facilities. Strava is not trying to be the Edward Snowden of the app world, but the company has made its way into being the latest parable for the privacy conscious.

On its website, Strava clearly describes its intention to users and how collected data will be used. Every user should have asked themselves the three questions. If certain military personnel had, they would have realized quickly that maybe sharing the geolocation of paths along secure facilities isn't the best app for me.

So before you download that next app, do exactly what you do when a prince shoots you an email asking for your bank account. Ask questions before sharing your personal information.

Tips for Using Peer-to-Peer Payment Systems and Apps - Alvaro Puig, FTC

Online peer-to-peer, or P2P, payment systems let you send money to people quickly. I've used them to collect money from the parents on my daughter's soccer team and to send money to my brothers when we've bought a gift for a friend. Personally, I almost always know where my phone is, but I can't say the same for my checkbook.

The use of these services is a growing trend—I just read an article that estimates there will be more than $700 billion in peer-to-peer payments in the U.S. in 2018. There are several mobile peer-to-peer apps out there already and banks are also getting into the game. If you use a peer-to-peer payment system, here are some tips to keep in mind.peer to peer payments

- In many apps, when you receive a payment, the money is added to your P2P system balance. It'll remain there until you transfer it to your bank account or use it for another transaction within the system. If you transfer the balance to your bank account, confirm that the deposit went through. The transfer could take a few days or even longer if it's flagged for additional review.

- Scammers try to get you to pay them in many different ways—including by sending money online—so make sure you know who you're sending money to. If you use the service to receive money from someone you don't know personally—maybe as payment for tickets to a concert or a game, or for an item you're selling—transfer the money to your bank account and make sure the money is there before you send any goods. Read the terms of service if you're not sure if these kinds of transactions are permitted on the service you use.

- Peer-to-peer payment systems require access to your financial information, so check your account settings to see if you can enable additional security measures that aren't on by default. Consider turning on multi-factor authentication, requiring a PIN, or using fingerprint recognition like Touch ID.

- Some systems or apps might share information about your transactions on social media. Check social media permissions or settings—some may be set to share your information with everyone by default. Adjust your settings based on what you're comfortable sharing.

Venmo, one of the players in this space, just reached a settlement with the FTC for some of its alleged practices. You can read more about it on our business blog.

It's True: False News Spreads Faster and Wider. And Humans Are to Blame - Steve Lohr, NY Times

What if the scourge of false news on the internet is not the result of Russian operatives or partisan zealots or computer-controlled bots? What if the main problem is us?

People are the principal culprits, according to a new study examining the flow of stories on Twitter. And people, the study's authors also say, prefer false news.

As a result, false news travels faster, farther and deeper through the social network than true news.

The researchers, from the Massachusetts Institute of Technology, found that those patterns applied

to every subject they studied, not only politics and urban legends, but also business, science and technology.

False claims were 70 percent more likely than the truth to be shared on Twitter. True stories were rarely retweeted by more than 1,000 people, but the top 1 percent of false stories were routinely shared by 1,000 to 100,000 people. And it took true stories about six times as long as false ones to reach 1,500 people.

Software robots can accelerate the spread of false stories. But the M.I.T. researchers, using software to identify and weed out bots, found that with or without the bots, the results were essentially the same.

“It’s sort of disheartening at first to realize how much we humans are responsible,” said Sinan Aral, a professor at the M.I.T. Sloan School of Management and an author of the study. “It’s not really the robots that are to blame.”

Here are other findings from the research.

Covering the history of Twitter

The research, published on Thursday in Science magazine, examined true and false news stories posted on Twitter from the social network’s founding in 2006 through 2017. The study’s authors tracked 126,000 stories tweeted by roughly three million people more than 4.5 million times. “News” and “stories” were defined broadly — as claims of fact — regardless of the source. And the study explicitly avoided the term “fake news,” which, the authors write, has become “irredeemably polarized in our current political and media climate.”

The stories were classified as true or false, using information from six independent fact-checking organizations including Snopes, PolitiFact and FactCheck.org. To ensure that their analysis held up in general — not just on claims that drew the attention of fact-checking groups — the researchers enlisted students to annotate as true or false more than 13,000 other stories that circulated on Twitter. Again, a tilt toward falsehood was clear.

The way information flows online — and, occasionally, spreads rapidly like a virus — has been studied for decades. There have also been smaller studies examining how true and false news and rumors propagate across social networks. But experts in network analysis said the M.I.T. study was larger in scale and well designed.

“The comprehensiveness is important here, spanning the entire history of Twitter,” said Jon Kleinberg, a computer scientist at Cornell University. “And this study shines a spotlight on the open question of the success of false information online.”

Novelty wins retweets

The M.I.T. researchers pointed to factors that contribute to the appeal of false news. Applying standard text-analysis tools, they found that false claims were significantly more novel than true ones — maybe not a surprise, since falsehoods are made up.

The study’s authors also explored the emotions evoked by false and true stories. The goal, said Soroush Vosoughi, a postdoctoral researcher at the M.I.T. Media Lab and the lead author, was to find

clues about what is “in the nature of humans that makes them like to share false news.”
The study analyzed the sentiment expressed by users in replies to claims posted on Twitter. As a measurement tool, the researchers used a system created by Canada’s National Research Council that associates English words with eight emotions. False claims elicited replies expressing greater surprise and disgust. True news inspired more anticipation, sadness and joy, depending on the nature of the stories.
Two stories: one true, one false

The researchers provided an example of two business stories, and how much more time it took the true one to reach 200 retweets. The example also shows the judgment calls made by fact-checking organizations.

- In 2014, the fashion chain Zara introduced children’s pajamas with horizontal stripes and a gold star. The company said the design was inspired by what a cowboy sheriff would wear. But Twitter users posted messages saying the pajamas resembled Nazi concentration camp uniforms. Snopes: True. Time to reach 200 retweets: 7.3 hours.

- In 2016, a website republished a portion of a satirical article about how the Chick-fil-A restaurant chain had decided to begin a “We don’t like blacks either” marketing campaign to stir up controversy and boost sales. It came after the company’s president did say he opposed gay marriage. Snopes: False. Time to 200 retweets: 4.2 hours.

What can be done?

The M.I.T. researchers said that understanding how false news spreads is a first step toward curbing it. They concluded that human behavior plays a large role in explaining the phenomenon, and mention possible interventions, like better labeling, to alter behavior.

For all the concern about false news, there is little certainty about its influence on people’s beliefs and actions. A recent study of the browsing histories of thousands of American adults in the months before the 2016 election found that false news accounted for only a small portion of the total news people consumed. “We have to be very careful about making the inference that fake news has a big impact,” said Duncan Watts, a principal researcher at Microsoft Research.

Another author of the M.I.T. study, Deb Roy, former chief media scientist at Twitter, is engaged in a project to improve the health of the information ecosystem. In fall 2016, Mr. Roy, an associate professor at the M.I.T. Media Lab, became a founder and the chairman of Cortico, a nonprofit that is developing tools to measure public conversations online to gauge attributes like shared attention, variety of opinion and receptivity. The idea is that improving the ability to measure such attributes would lead to better decision-making that would counteract misinformation.

Mr. Roy acknowledged the challenge in trying to not only alter individual behavior but also in enlisting the support of big internet platforms like Facebook, Google, YouTube and Twitter, and media companies.

“Polarization,” he said, “has turned out to be a great business model.”