COMPUTER NEWS from the

MAY 2014 Volume 2 NO. 5

As found on the web and other sources

Are Social Networks Committing Suicide?

FROM: “askbobrankin.com”.

Lots of people are finding that the popular social networking sites (Facebook, Twitter, LinkedIn) are becoming more annoying, more expensive, and less useful. Here's how I see the problem, and my take on what the future of true social networking should look like.

Will Social Networks Collapse?

Recently, I wrote about LinkedIn’s underhanded attempts to pry money out of job seekers, employers, and even people it invites to congratulate their colleagues on promotions or new jobs. In my RankinFile.com article Is LinkedIn Trustworthy? I mentioned that other social networks are also guilty of deviously milking members.

This article goes into more detail on that subject and why I believe the social networking bubble is going to collapse under the weight of its own avarice.

All of today’s major social networks – Facebook, Twitter, LinkedIn – were founded on the same business strategy. Give away services for free to gather lots of members as fast as possible, in an effort to corner the market on eyeballs. “Whoever gets biggest first, wins” is the simplest explanation of the network effect.

Facebook has over a billion members now; it will be very difficult for any challenger to overtake and surpass Facebook's lead and attract significant numbers of members. Even people who loathe Facebook stick with it because "that's where everyone is."

Once you are too big to leave, you can stop depending on ad revenues alone and start charging members to use what was once free.

LinkedIn invited me to congratulate a colleague who'd landed a new job, but when I tried to do so I learned the price was giving LinkedIn the password to all of my email contacts. I've also been hit up for $30 a month just to say "hello" to someone who appeared interesting. No, thank you, to both.

Facebook gave every member two inboxes for private messages. The main inbox alerts you when new mail lands in it. The "other" inbox is more like a spam folder; messages that land in there often lie unnoticed for months. When you attempt to send a message to someone you are not "friends" with, Facebook flat-out tells you that it probably won't be seen – unless you pay Facebook to put your message in the recipient's main inbox. Usually, the fee is only a dollar, but on a few occasions I've been asked for five; the person I was trying to message wasn't anyone special, as far as I could tell.

More Pay to Play

Businesses and organizations that maintain Pages on Facebook are getting socked hard these days. The owners of these Pages worked hard to build fan bases, creating and posting engaging content that was liked and shared widely, bringing in new fans.

But now, Facebook is deliberately limiting the exposure that a Page's post gets to 1 or 2 per cent of the Page's total fan base. So if you have 1,000 fans, perhaps only 100 of them will see what you post in their Newsfeeds. That's down from 16 per cent two years ago, before Facebook began the slow, subtle throttling of this free marketing channel.

The solution that Facebook offers is to pay for greater exposure. Some huge brands, like Nike, may be willing and able to do so. But many small businesses and nonprofit organizations are watching their interactions with fans dwindle by 80 per cent or more. A lot of hard work is being wasted.

Twitter recently introduced "sponsored tweets" that sponsors pay to have inserted into your timeline even though you are not following the sponsors. They're not re-tweets from someone you follow, but unsolicited and unrecommended advertisements… spam, by any other name.

You know who else gives away free samples and then, when people are hooked, charges through the nose for the same product? Heroin dealers. It's a very effective business strategy – and a widely despised one.

Video Killed the Radio Star

In olden days, like the 1980s, social networks were called "online services." CompuServe, Prodigy, America Online (now just AOL), and some of the largest dial-up Bulletin Board Systems (BBSes) were the Facebook and LinkedIn and Twitter of today.

They were more honest in their business strategy, telling everyone up front, "We'll give you a month's free trial, but after that it's going to cost you to stay here." You might not like the price, but at least you had fair notice of what you were getting into. Not so with heroin dealers, who pretend to be your generous buddy until you're dependent upon them, then nickel and dime you to death.

The Internet killed the old-school online services by enabling people to connect with whomever they wished, and do whatever they liked with their connections. The intermediary's role became superfluous, so the intermediaries could not charge enough to survive.

The Decentralization of Social Media

I believe the same thing will begin happening to today's social networks as they attempt to get more money from members, by charging for more and more popular features that once were free.

People will simply go build their own Web sites, with forums and private message systems and e-commerce stores and whatever else they want. It's already happening with the surging popularity of services like Blogger, WordPress, and Tumblr. If folks don't trust or prefer not to use an established service provider, even the cheapest web hosting accounts have drop-in components for those who want to roll their own blogs, forums, photo sharing or even online stores. Isn't that the beauty of the Internet... leveling the playing field, and putting the power to publish in the hands of Everyman, instead of the Elite Few?

They'll spread the word about their sites by email, instant messaging, Skype, and maybe newsgroups will make a comeback. They may entice some of their friends on current social platforms to escape those walled gardens. But they won't need Facebook, LinkedIn or Twitter

badly enough to pay for access or “privileges.” It the process, they'll take back ownership of their data and their privacy.

And something interesting will happen, I think... The Web will look more like a (social) network of inter-connected individuals, rather than a few large herds of cattle. You think I'm wrong? You may be right, I may be crazy. But wouldn't it be a nice change?

Read more:
http://askbobrankin.com/are_social_networks_committing_suicide.html#ixzz2yKmQ77fr

---

Is Using Windows XP Really That Dangerous?

By Brandon Dimmel on April, 14 2014 in “Infopackets.com.”

Is it really that dangerous to continue using Windows XP?

Microsoft's **Windows XP has officially been decommissioned** as of April 8, 2014, meaning that Microsoft will no longer support the software insofar as **security updates** are concerned.

Without any security updates, Windows XP is extremely vulnerable to attack if and when an **operating system exploit** is discovered. And, even if one is discovered, it may or may not make headlines - which means most users running Windows XP simply won't be aware their system has been compromised. It's these types of attacks that are most dangerous, and are often referred to as **zero-day exploits**.

Security expert Andrew Storms at CloudPassage questioned the notion put forward by many security experts. They suggest that hackers have been waiting anxiously for the April 8, 2013 deadline in order to launch a series of attacks on Windows XP users - but, so far, that hasn't happened.

Dangers Wait Down the Road, Security Experts Say

TK Keanini, chief technology officer at Georgia-based data analysis firm Lancope, agrees that it's unlikely hackers are about to launch a doomsday attack on XP machines any time soon. But Keanini says the real dangers will be found in the future, perhaps when Windows XP users suspect them the least.

"It is important to note that ... [it] is not like [**the year 2000 bug**] where something will break or suddenly have a vulnerability," Keanini said. "It is the fact that any new vulnerability discovery cannot be fixed." (Source: **pcworld.com**)

Storms agrees that it's likely a serious attack will come someday down the road. In fact, Storms recommends isolating a Windows XP machine from a network, ensuring that any infection afflicting that system won't spread to others.

If a Windows XP machine is isolated from a network (both the Internet and public networks), it's reasonable to expect that the machine could function infection-free for quite some time. However, that is not true if the machine comes in contact with an **infected CD, DVD, or USB device**. That's exactly how the **conficker worm** spread back in 2008, which quickly spread to well over **9 million PCs** in a very short amount of time.

Windows XP Users Should 'Upgrade As Soon As Possible'

In the long run, Keanini says most Windows XP users should plan to **upgrade to a new operating system** as soon as possible.

"If you have an XP [system] ... you need to treat it as if it were already dead and move quickly to get it replaced," Keanini said. "Pretend it caught fire, and you will be moving with the right amount of urgency."

Regardless, all security experts agree that Windows XP users should take extra special caution when storing their most sensitive information on their PCs -- such as banking and credit card data. At the very most, do not store sensitive information in documents or plain text files. This type of information should always be encrypted in order to help mitigate risk. Programs like **Roboform** are able to encrypt website passwords, including documents known as 'safe notes'.

Online Banking with Windows XP "Incredibly Dangerous"

"Skyrocketing online banking malware combined with a coming slew of never-to-be-patched vulnerabilities means that online banking on Windows XP is going to become incredibly dangerous soon," noted Christopher Budd, Trend Micro's threat communications manager.

"While that is a risk to the users of those Windows XP systems, in aggregate and in the end, it's those users' banks and financial institutions that face the greatest risks." (Source: **cbc.ca**)

What's Your Opinion?

Are you still using Windows XP and do you plan to update your system to another operating system any time soon? If you plan to stay with Windows XP, what precautions are you taking to help protect your system? Lastly, do you believe a major attack on Windows XP systems is coming, or do you think this is simply fear mongering designed to sell newer PCs and/or promote other operating systems?

XP UPDATE
Malwarebytes last week announced a security service that will continue to protect users of the XP operating system.

Want to try Computer Russian roulette!

Beware of Key Generators

FROM: askbobrankin.com.
Twenty years ago, a key generator was a machine in the hardware store that made duplicates of your house keys. Today, a key generator (or keygen) is a tool that software pirates use to illegally activate or unlock commercial software. Aside from the obvious ethical issues, there's another reason why you should steer clear of these things. Read on to learn about the hazards of keygens…

What is a Key Generator?

"You can't cheat an honest man" is an old proverb, and it has its complement: it's pretty easy to cheat dishonest people. That's why malware distributors love to target people who steal software, music, movies, games, and other intellectual property. One of the favorite traps set for pirates is the key generator.

Sure, you could plant a virus or Trojan in a complete software package. But why bother uploading hundreds of megabytes to various sites, or making such a large package available to downloaders, when a small file of a few thousand bytes will catch just as many fish?

Trial versions of programs are available from the developers' sites. What pirates often want is a license key that transforms a trial version into a full-featured version that never expires. Programs that generate illicit license keys are called "key generators" or "keygens" for short.

Keygens don't have to be very big. All they need to do is prompt the user for the same registration data that the software does and then use the same algorithm that the software uses to generate a license key. A few dozen kilobytes of code are ample for these simple tasks. The small keygen packages are often spread more widely and quickly than gigabyte-sized packages containing pre-cracked software.

Now Playing on YouTube…

If you visit The Pirate Bay Bittorrent mega-site and search for the word, "keygen," you'll be rewarded with many hits. (It's safe to go and look, but don't download anything if you wish to avoid a malware infection or a warning from your ISP.) But malware distributors are also using YouTube to spread their poisoned programs.

Many pirates are also music and video junkies. Keygen videos provide entertainment bait as well as the promise of free software. The video portion is usually of low production value, and the "music" that accompanies many keygens is ripped from 1970s video games. (There are even libraries of tunes known as "keygen music" or "chiptunes" for the convenience of miscreants who post these links.)

On the keygen video page, you'll find a link to download the actual keygen program. It's like playing Russian Roulette, only the odds are a lot worse. The most likely outcome of clicking that link is that you'll get a nasty malware infection, or become ensnared in a botnet. (See BOTNET ALERT: Are You Vulnerable?)

An acquaintance of mine who works for a software development company says that keygen videos targeting the company's products pop up daily on YouTube. The company swiftly reports

the illicit content and YouTube is responsive in taking it down. But not all firms are as diligent in protecting their intellectual property, he says. Many keygen videos have remained on YouTube for years, gathering thousands of views and an undeserved reputation for legitimacy.

The reason for the longevity of some of these keygen videos may be a form of counter-terrorism. It's entirely possible that some bogus keygen videos are posted by the very companies whose software the keygen program is supposed to steal. “Poisoning the well” of keygen Torrents and videos with malware-infected keygens is one way to discourage piracy.

You might think that Google, owner of YouTube, would proactively police its video site for any sign of keygens and remove such content without waiting to be asked. But that would take an army of keygen cops, so the removal process relies on user reports of keygen videos.

False Flags

The comments left on Torrent pages and YouTube pages are not reliable indicators of a keygen’s safety. Positive comments (“It works, no infections!”) are often left by the malware distributor and/or his co-conspirators. Negative comments (“Hey, my antivirus software says this file is infected with…”) are either removed by a page’s owner or explained away by the owner’s shills.

“Don’t worry about the anti-virus alert, it’s a false positive” is the usual advice. There isn’t any reason why an uninfected keygen program would trigger a false positive in an anti-virus program. All a keygen does is accept input, generate a string of letters and numbers, and display it to the user. So if your anti-virus warns you not to run a keygen, something else buried in the keygen is causing the alert.

In almost all cases, a key generator is a tool that's designed to help people do something illegal. Think of it as the digital equivalent of a lock picking kit. Honest people have no need for either. The irony is that there are so many bogus key generators now, that even the dishonest have reason to avoid them.

Your thoughts on this topic are welcome. Post your comment or question below...

Read more: http://askbobrankin.com/beware_of_key_generators.html#ixzz2yc46BVPt

---

The U.S. has created an atomic clock that will not lose or gain a second in 300 million years, making it three times more accurate than previous clocks. Now you have no excuse for being late to work.

I WENT TO A BOOKSTORE AND ASKED THE SALESWOMAN, "WHERE'S THE SELF- HELP SECTION?" SHE SAID IF SHE TOLD ME, IT WOULD DEFEAT THE PURPOSE.