COMPUTER NEWS from the

Nov. 2013 Volume 1 NO. 11

As found on the web and other sources

PRIVACY BE DAMNED!

Facebook Kills Privacy Protection Feature

By Brandon Dimmel on 20131016 in "infopackets.com".

Facebook is killing a privacy feature designed to restrict who can find users through the social networking site's search tool. The firm defended the move by saying only a small percentage of its members actually used the feature.

The feature, which is called "Who can look up my Timeline by name?" allowed Facebook users to customize who could find their profile through a search of the social network's database. For people who wanted to keep their profile information off-limits to employers, strangers, and enemies, it was deemed a highly useful feature.

'Small Percentage' Could Include Millions of Users

But Facebook says only a small percentage of its user base -- which includes well over one billion people -- actually employed the feature.

It's not yet clear how many users were fans of the feature, though reports indicate the percentage was in the single digits. (Source: washingtonpost.com)

Because it found most users did not employ the feature, Facebook began a slow process of phasing it out last year. That process is now just about complete, according to reports. The change doesn't mean users have lost all control over who can see their information. Facebook is reminding users that they can control who can see each comment and photograph posted to the site.

Facebook Suggests Feature Gave Users a False Sense of Security

Facebook even went so far as to suggest that the feature it's eliminating gave too many of its users a false sense of security because people could still find a picture or comment through names and tags. "Our concern, quite frankly, is that people think it provides a level of security, but it actually doesn't," noted Facebook Privacy Team member Nicky Jackson. (Source: cbsnews.com)

Still, many users are upset about the change, which is hardly the first policy adjustment to arouse the indignation of Facebook members.

The United States' Federal Trade Commission (FTC) is currently investigating a Facebook policy that allows the company to use its members 'pictures in advertisements ***on the site*.**

Privacy be DAMNED! PART 2

Google to Place User Photos, Info in Ads
By Brandon Dimmel on 20131014 in "infopackets.com"

Facebook recently took heat from users upset with the company's claim that it could use members' photographs for advertising purposes without asking permission. Despite that outrage, Google is now implementing a similar policy.

According to reports, users of Google's own social networking service, Google+, could soon see their pictures placed in advertisements. Those same users will not be consulted before these ads are made or compensated once the ads are placed online.

Google Puts Positive Spin on New Terms of Service

In a recent statement Google said that, through a new terms of service being released November 11, 2013, it maintains the right to use Google+ members' user names and profile pictures for "reviews, advertising," and other commercial purposes.

In effect, the policy means that a user (over the age of 18) unknowingly consents to become brand ambassador for the goods and services they recommend via Google+.

Google believes it's a positive step because these "shared endorsements" purportedly help Google+ users "save time" when searching for new goods and services. After all, what's better than a recommendation by an actual friend, family member, or colleague?

"We want to give you -- and your friends and connections -- the most useful information," Google announced on its website. "Recommendations from people you know can really help."

Internet Privacy Advocates Slam New Policy

Of course, not everyone shares Google's opinion on the matter.

Internet privacy and social media lawyer Bradley Shear recently told ABC News that he believes Google's policy "demonstrates that Google does not care about their user's privacy," and that "This is an absolute abuse of the trust of [Google] customers."

"We're all essentially now a product," Shear added. "I really think that goes against the grain of what we are as a society." (Source: go.com)

Opt-Out Possible, But Discouraged by Google

There is good news, however: unlike Facebook, Google is giving Google+ members the ability to opt out of the program.

However, the firm isn't exactly encouraging people to make the change; in fact, when a user decides to opt out they're presented with an "Are you sure?" message followed by the warning "your friends will be less likely to benefit from your recommendations."

The U.S. Federal Trade Commission is currently investigating Facebook's new policy but because of the government shutdown it's not yet clear if the Google+ policy will also undergo review. (Source: washingtonpost.com.)

Download of the month.

WinPatrol 28.9.2013.1

WinPatrol is designed to monitor your system and alert you any time a program makes unwanted changes to your PC settings. This program, which is partly designed to help you detect zero-day attacks, is available for Windows XP, Windows Vista, Windows 7, and Windows 8.

http://www.winpatrol.com/

Can a Virus Really Destroy Your Hard Drive?

From “askbobrankin.com

Occasionally, I hear from readers who say a virus 'destroyed' their hard drive and they had to buy a new one. But are there actually viruses that can physically damage a hard drive? Is it even possible for a virus to damage hardware, or is this an urban legend? Read on to find out the truth...

Beware the Horrible, Terrible, Evil, Hard Drive Destructo Virus!

I can't tell you how many times I've heard a reader say "A virus wiped out my hard drive, so I had to buy a new one and re-install everything." When I ask what exactly they mean, the victim sometimes claim that a virus 'fried the electronics,' 'crashed the head,' or otherwise physically damaged the drive. In other cases, people were told by a repair technician that a virus had permanently damaged the hard drive, and they needed to purchase a new one.

My short and simple answer to the question is "no". To the best of my knowledge, no antivirus researcher has ever discovered a virus that causes physical damage to hardware. You can be sure that such a discovery would have made headlines all over the world. It just hasn’t happened.

People who claim it has happened are wrong, or are being disingenuous. Or it could be what I call "Cousin Vinny Syndrome" -- a modern day version of "I heard it from a friend who knows a guy who lives near the police department in a major city, and he knows about this stuff."

It’s not unheard-of for an unscrupulous repair technician to tell a naïve customer that a virus has “destroyed” a hardware component, usually a hard drive. Then the technician gets to sell the victim a new hard drive, memory stick, motherboard or power supply. They'll also charge for the “service” of re-installing the operating system and apps, in addition to the hours of labor that

went into “diagnosing” the bad news. The customer leaves thinking that viruses can damage hardware, and blames viruses for any future hardware problems.

Then there are the amateurs who, upon failing to fix their own hardware, conclude that “it must have been a virus because I couldn’t possibly have done anything wrong.” There are various computer glitches (which may include a virus, a power spike, or just poorly written software) that can wipe out critical sectors of a hard drive. When this happens, you'll be greeted by a startup screen that says "Disk Boot Failure", "No Fixed Disk Found", "Missing Operating System" or some other ominous error message that *seems* to indicate that the hard drive is physically damaged. But in almost every case, it's not really a hardware problem.

See my article Help, My Hard Drive Died! to learn about various tools that can help you recover from these situations. In many cases, you won't even have to re-install Windows or restore files from a backup.

Viruses can and have turned hard drives into seemingly useless bricks. But the only thing they can damage is the data stored there. A virus that overwrites the drive’s boot sector renders it inoperable. But a corrupted boot sector is fixable; only the data written to that sector has been damaged, not the magnetic media that stores the data. Reformat the drive, or reconstruct the boot sector, and the drive will work again. If a virus wipes out files, you can restore from a backup, and you're back in action.

Hard Drives, Head Games and Semantics

Getting back to the original point, is it possible to write a virus that destroys hard drives? A hard drive (like many other PC components) is controlled by embedded chips that contain low-level “microcode.” This microcode can be replaced in what’s called a “flash update.” So why couldn’t a virus replace the legitimate microcode? In a Computer World magazine column published in 2005, columnist Robert Mitchell got a Western Digital VP to admit that it is possible, in theory. Mitchell claimed this admission proves that a virus could “essentially destroy” a drive.

But Mitchell was playing a semantics game. “Essentially” does not mean “physically.” In his context, “destroy” means “render unusable.” A virus could make it impossible for the system’s BIOS to communicate with a drive, but it could not damage the drive’s hardware. If the virus could be flushed out with a new legitimate flash upgrade, the drive would work again. Again, there's no physical damage -- only the DATA on the device is affected. And data can be replaced.

I've also heard about theoretical viruses that write data so frantically to the hard drive, that it just eventually crashes the head or wears out the surface of the drive. I just can't buy this theory, because that virus would have to be running non-stop for months or even years before anything bad happened. I struggled to find an analogy for this, and I thought of the Etch-a-Sketch. Its surface is kind of like a hard drive platter, and the little "pen" you control with the dials is the read/write head. You can scribble all you want, but you're not going to damage the device. And anything you write on the surface of the Etch-a-Sketch screen can be wiped away by shaking it

and starting over. That's similar to reformatting a hard drive, which will wipe out the virus and anything that it did.

And then there's the Chernobyl Virus, which appeared in the late 1990s. Some have said that it could cause actual physical damage to the BIOS chip, but that appears to be the stuff of legend and rumor. It might have been able to erase data on a hard drive, or over-write the data on the BIOS, but that's not permanent physical damage. Oh, and I have to mention StuxNet, the virus that targeted computers controlling uranium enrichment equipment in Iran. In this case, the virus tried to affect the functioning of centrifuges and other equipment being controlled by the infected computers. There was no physical damage to the computers, and it's not even clear if the centifuges were damaged.

Let Me Be Perfectly Clear..

I am NOT trying to say that a computer virus can't damage files or destroy data. Of course it can. And 15 or 20 years ago, old-school hackers might have been interested in doing that type of thing. **But today, viruses are not created to destroy hardware or data.** Viruses are created to steal data and money, to send spam, or to disrupt other users with denial of service attacks. And they're written so as to do their dirty work in secret. Virus creators WANT your hard drive to last a long time, so they can continue to use your computer to do their bidding.

Of course, computer components such as hard drives, motherboards, RAM, graphics cards and power supplies can wear out, or burn out. But those things are caused by defects in manufacturing, poor quality materials, overheating, or power surges. If a computer repair tech tells you a virus caused it, take your computer somewhere else.

If you (or your Cousin Vinny) disagree with my opinion that a virus cannot physically damage a hard drive, please let me know! And please, cite a credible source when you do. Your comments and questions are welcome below...

Read more:
http://askbobrankin.com/can_a_virus_really_destroy_your_hard_drive.html#ixzz2hRfvjW8g

---

What is More Dangerous Than Malware?

From “askbobrankin.com.”

Most computer and Internet security articles focus on threats found 'out there' in the online sphere, or in the form of bad people with malevolent intentions. The danger is that they will get to you or your computer, and steal or damage. Most security measures focus on preventing such intrusions. But the greatest threat is not 'out there.' It is in you…

The Biggest Online Threat?

It IS you, in fact. You are human (no matter what your ex says), and have a human Mind (or enough of one to get by). Nothing is more capable of causing, or is more likely to cause you trouble. Yet the Mind is seldom the subject of information security articles. This is one of those rare reads.

"It ain't what you don't know that gets you into trouble," wrote Mark Twain. "it's what you know for sure that just ain't so." Almost every activity that a human performs, including most of what is supposed to be "knowledge work," is done unconsciously; motions are gone through with blind faith that they will produce the same results they did last time. No attention is paid to what is right in front of you, in your hands.

That is why people click on links in emails that generally look like they're from their bank; follow the instructions on what generally looks like their banks' Web sites; and have their accounts emptied by bandits in Ukraine. Had you been paying attention, you would have noticed that your bank's emails address you by name, not as "Dear Customer…" You would have remembered that your bank has told you, at the time you opened your account and many times since, that it will never ask you for your account password via email, and that you should always use a bookmark or type in the bank's web address. But people do not pay attention.

It's why people believe the "Nigerian prince" who promises that if you send him $5000 by wire transfer, he'll give you half of the $15 million lying dormant in a secret bank account. It's why lonely women send money to "international businessmen" they've never met, thinking they are helping to save the life of a dying son who desperately needs an operation. Kind-hearted people, especially the naive, the emotionally vulnerable, or the financially stressed ones, want to believe the best about others, even if it's not rational.

It's why people click into the dark corners of the Internet, or on flashing banners that say "You just won an iPad!" They believe that because they have McAfee or Norton AntiVirus, it will protect them from all possible cyber-threats. Of course, they don't know that viruses can morph and propagate in minutes, but it takes days for antivirus companies to update their malware signature databases. They haven't applied critical Windows security patches, or updated their Java software or Adobe Reader in years. Maybe they're just lazy, or too busy. More likely, they've simply decided to trust the claims of the company that sold them the Internet security suite, and pay $49 a year for "peace of mind."

"You Can Trust Me..."

Trust is the belief that you can predict behavior with an acceptable degree of confidence. It might be the behavior of a person, a computer program, a pet, or a website such as LinkedIn.com. Innumerable people have overestimated their prediction abilities with regard to people, programs, cars, pit bulls, “trusted service providers” and “trusted partners.”

Recently, a group of LinkedIn members filed a petition for a class action lawsuit against the company, attempting to convince a judge that savvy professionals such as themselves (just look at those glowing recommendations!) could not possibly have known that giving any website access to one’s email contacts is the same as handing over one’s family and friends over to multi-level marketers. Good luck with that, folks; like LinkedIn’s legal department says, “We believe the lawsuit is without merit.”

And there's also a new obnoxious thing appearing on Facebook. When I click to accept a friend request, I am asked: “Do you know so-and-so outside of Facebook? YES or NO!” That’s not a friend asking if you know somebody with whom you just exchanged passing fistbumps. It’s a computer asking and then DEMANDING an answer. (Psst, you can click outside that popup, and it will slink away.)

When you answer questions like that; when you willingly tell Facebook about the books and music you like, the movies you've watched, and your favorite TV shows; when you link your profile to all of your family, friends and business acquaintances; it's Facebook using you for free to fill in the blanks of their highly marketable dossiers on over a billion people.

Why believe that? Because that is how Facebook has behaved from the beginning, if you have paid attention. Mark Zuckerberg started Facebook by stealing copyrighted information and publishing people’s personal information without their permission. Of course, he and his official biographer don’t see it that way, but that is what history shows. Do not trust a person or a corporation to do other than what it has done in the past, despite what the legalese in the Privacy Policy says.

The three “A’s” of security are: Attention, Adaptation, and Action. Pay attention to what is right in front of you. Adapt your Action to new or changed external behavior. Don't blindly trust your antivirus software, click anywhere except where Zuckerberg tells you to, don’t click when you see “Dear Customer…", or when you know in your gut that something smells fishy. Are you paying Attention to me?

Read more:
http://askbobrankin.com/what_is_more_dangerous_than_malware.html#ixzz2hQVZAI54

QUOTE of the month!
Lawyers believe that a man is innocent until proven broke.
~ Robin Hall
*****