

# 12 things computer users should fear in 2010

About once a year, computer security news leaps out of the technology section and onto the front page and the top of network news broadcasts. This year, the day was April Fools' Day, as the Conficker worm became the latest malicious program with the power to eat the Internet. Somehow, we soldiered on, most of us without ever having to kick on the emergency power generators or dig into that can of spam in the basement shelter.

But Conficker, while no dramatic outbreak, was also no laughing matter to the hundreds of thousands of Web users who were infected. The problem with the hype cycle in computer security news is that it can have an incremental "cry wolf" effect on computer users. The odds that the Internet will topple over in 2010 are, once again, quite low. But serious threats abound and bad guys are mostly still outpacing good guys in our virtual world, which will be slightly more dangerous than this year. Here are 12 reasons why:

## 1. E-mail attachments are back

The LoveBug and Melissa virus, which did bring the Web to its knees 10 years ago, both used the simplest of delivery mechanisms -- an e-mail attachment. Sure enough, that method stopped working after companies banned attachments and users wised up. Attachment viruses nearly dried up. Then, a new generation of users came online who hadn't learned the Melissa lesson and older users forgot. So this year, virus writers began dusting off their old methods and -- surprise! -- they worked again. Next year, be on guard for unexpected attachments, says Carl Leonard, head of the Websense threat lab.

"Sometimes you think this stuff has gone away and then it comes back," he said. "We're definitely seeing an uptick in Trojans that come through e-mail."

## 2. Anti-virus products less effective

Old-fashioned virus screening tools now catch only about three out of every four viruses through what's called "signature-based" detection, says Martin Lee of Symantec. Basic anti-virus tools scan all programs using a list of known malicious programs, looking for electronic "signatures." Virus writers now generate so much malicious software that the good guys just can't keep up. To make matters worse, virus writers are employing a technique known as "polymorphism," so the virus can electronically mutate and evade detection. That means about 25 percent of viruses can evade detection by scanners. New "heuristic" antivirus software detects malicious programs by watching what they do rather than inspecting what they are, but these products are far from perfect.

Making matters worse, viruses are now more stealthy after infections. Once upon a time, an infection was obvious, thanks to a dramatic slowdown in performance or some other obvious symptom. Not true today.

"It's become increasingly difficult for people to be aware they've become infected," Lee said. "Often, end users just will not realize something has happened."

With few guarantees for protection, it's more important than ever to keep the kids off music piracy sites and for you to avoid other unsavory Web places -- and you know the ones I mean.

## 3. Fake anti-virus software

Knowing that your antivirus product might not be doing the job, you might be tempted to look online for an alternative, or to try one that surprisingly pops up on your desktop. That's a bad idea: It's probably a criminal trying to extort you for money. The art of selling rogue anti-virus software was perfected in 2009. Leonard says consumers shelled out \$150 million for fake antivirus programs last year.

"People are selling malicious software and dressing it up as an antivirus product," he said. "It surprises me the volume that they are selling. You would think people have become used to seeing these things."

Obviously not. [The Federal Trade Commission did shut down two rogue sellers last year](#), but not until they allegedly tricked nearly 1 million consumers into downloading their software.

The technique, which works like a charm, will expand next year.

## 4. Social networking

Facebook-based attacks grew dramatically in 2009, and will continue to increase in the coming year.

There are basically two flavors -- viruses that take advantage of the platform's liberal rules for information sharing among applications; and impersonation/identity theft, where a criminal hijacks an innocent user's account and tricks trusted friends and family. But other variations are certain to appear. Criminals can use publicly available information to personalize attacks ("Hey, check out these pictures from Paramus Catholic's Class of 1986!"). Facebook is easily farmed for password-generating information such as "What was your high school mascot?" And all those "click here" e-mails from Facebook are a Christmas present for would-be phishers, who can easily imitate them.

"People are getting comfortable in social networking situations and I think that they should really re-examine their level of trust and interaction," said Mary Landesman, senior security researcher at ScanSafe.

And remember, even if Facebook old-timers are too smart for all these tricks, the service is teeming with older newbies. If you've been friended by mom (or grandma) you know what I mean. They'll have to endure the Facebook privacy learning curve, too. Be generous. Spend a few minutes with older relatives this holiday getting them to tighten up their privacy settings.

## 5. Botnets

The bane of the Internet for the past five years -- botnets, or armies of compromised home computers -- will remain a problem this year. And they it may be even worse: botnets have become much more resilient. Once upon a time, botnets could be disrupted by "cutting off their head," or disabling their command and control computers. But now, criminals are "building disaster recovery" into the networks, Symantec's Lee said. That makes them even more difficult to knock off line.

"You must have grudging respect for them and their techniques," Lee said.

## 6. Spam

Spammers took a body blow during 2009 when the notorious McColo Internet Service Provider was kicked off-line. The volume of spam plummeted from around 80 percent of all e-mail to 20 percent. Temporarily. By year's end, nine out of 10 e-mails were spam, and the number keeps climbing.

"Can it get to 95 percent?," Lee asked, rhetorically. "It never ceases to amaze me how much we put up with this."

## **7. Finally, Apple gets respect - from cybercriminals**

For years, the worst-kept secret in the computer security world was the safety of using Macintosh computers. It seemed that criminals didn't bother trying to attack Macs. This was no political statement, however. It was merely pragmatism: Apple products were a small target. But with the uptick in Mac market share, the increasingly popularity of Apple's Safari Web browser and the ubiquity of the iPhone, expect criminals to target Steve Jobs' products, says Leonard. Already, he says, there have been a handful of iPhone attacks.

"Malware authors know where people are going," he said. "It's more worthwhile for them to go after these platforms."

## **8. Cell phones**

Speaking of iPhones, 2010 might be the year that we see a significant attack against cell phone or smart phone users. Such an attack has been predicted for years, and has not yet materialized. But each year, cell phones become more powerful, contain more personal information and are used for more financial transactions. In other words, they become "juicier targets" for criminals, says Lee. An obvious attack -- like something that wipes out phone books -- might not be the breakthrough cell phone virus. Lee says consumers should be on the lookout for a simple automated way to use mobile phones to steal cash. One possibility: some TV shows urge consumers to send text messages at \$1 a piece. What happens when a criminal figures out how to redirect such messages, or initiate them?

## **9. SEO poisoning**

You have probably noticed that companies can "game" Google and other search engines, puffing up their search engine results using a series of tricks such as creating fake pages that link heavily to each other. Annoying, but relatively harmless. Unfortunately, bad guys have perfected this method and use it to mercilessly attack information seekers every time a large news event occurs. Perhaps hundreds of thousands of users were infected after the death of Michael Jackson through this technique -- getting a booby-trapped Web page to rank 5th or 6th on a Google "Michael Jackson" search, even for just a few minutes, is probably the most effective malicious program attack used today.

"We see this sort of attack daily and especially when a signature event occurs, like Michael Jackson's death," said Leonard. Expect much more next year. When the next big news hits -- however self-serving this may sound -- stick with news Web sites you trust.

## **10. WINDOWS 7**

Naturally, as the year progresses, criminals will set their sights on the increasing install base of Windows 7. Microsoft has continued to improve security and delivery of updates to its flagship operating system. But there will be problems, no doubt. And then there's this troubling notion: Eight out of 10 existing Windows viruses will run on Windows 7, says Leonard. Impressive forward-compatibility from the bad guys. For consumers, it means there's no time to be complacent.

## **11. URL shorteners**

Services like bit.ly make sending links through Twitter and e-mail infinitely easier. Unfortunately, it also means criminals can turn obvious troublesome URLs, like [https://RomanianDarkLords.Ro/\\$\\$\\$eBay.com](https://RomanianDarkLords.Ro/$$$eBay.com) into friendly-sounding links like <http://bit.ly/5uuWwo>.

That makes life easier for criminals, and harder for you, as it takes away one possible hint that a link is trouble.

Websense recently partnered with Bit.ly to help make the process safer. But you should stick with the old rule: Never click on a link you didn't expect, and always manually type URLs into your browser's address bar.

## **12. Gumblar**

Last but not least, Landesman says the most troublesome development of 2009 could be the breakout security problem of 2010. The so-called Gumblar worm used an advanced technique to build a new kind of botnet. Rather than target thousands of home computers, Gumblar attacked Web hosts (Web sites) and turned them into "carriers." The program managed to download a Web site's code, inject a hidden malicious program, then-reload the now booby-trapped site.

Because Web sites act as a kind of hub online, they have the potential to spread a serious attack much more quickly. And 10,000 compromised Web sites are much harder to shut down than 10,000 compromised home computers, Landesman said.

Worse yet, a seriously successful Gumblar-style attack could undermine Web users' trust in the Internet. Sites that are one day safe and trustworthy may the next day be dangerous. That would severely hamper security systems that are based on "trusted" sites.

"When you have compromised sites acting as the host itself, the notion of good vs. bad is completely gone," Landesman said. "Users will find that fewer and fewer sites that they can trust whatever trust they do have could be very fleeting."

Already, Gumblar-infected sites have transmitted code to visiting PCs that redirected all Google searches to pay-per-click Web sites, netting a tidy sum for creators.

Gumblar was declared a bigger problem than Conficker in May by Scansafe, and even though its network of compromised Web sites was eventually tamed during the year, Landesman is convinced that the technique will see many copycats.

"It's one of the attacks we are assured of seeing in large quantities in 2010," she said