

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

around the globe. It was an interesting conversation, not because there was any real news in the current trends but because the state of cybercrime makes it clear we have to re-think our entire approach to security.

Oct. 26, 2011

I had the opportunity to spend some time with Don Codling, unit head for the FBI's CyberCrime Division, talking about the state of computer and network security around the globe. It was an interesting conversation, not because there was any real news in the current trends but because the state of cybercrime makes it clear we have to re-think our entire approach to security.

To be honest, I've always treated computer security lightly. If you take a few sensible precautions, don't cruise the porn sites on the Internet and use a good email filter, security software for a PC seemed more a way to separate fools from their money than anything else. To prove the point, a few years ago I ran a server wide open on the Internet without any protection at all for more than two years ... without a single problem.

But things are different now.

It's not just that organized crime and terrorist organizations have turned to online crimes to fund their operations. It is not even that a legion of hacker wannabees tries to find and exploit weaknesses in just about every piece of software released today. And it is not that computers are in some way more vulnerable than they used to be. The biggest problem is that there are more than two billion people online today. And by definition, at least half of these have subnormal tech skills. Or intelligence, for that matter.

Two billion people means that there are more people who will open any email attachment that features hearts or nude pictures of Brittany Spears, no matter who

the email is from. More people who just have to play games on Facebook, no matter

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

simple information pipeline and let you choose what you wanted to look at. Today, competition in the broadband marketplace means you can also choose an ISP that has a higher level of security. So the first step is to actually interview your service providers — not only the primary ISP, but your email and web hosting services if these are separate. While you're at it, the accounting software vendor that provides you with your portal or online access should be interviewed for their security measures, as well.

**2. Get some filtering software.** The days when protection cost an arm and a leg are over. From Microsoft to AVG, there are free options for computers. In addition, there are other products we have discussed here in the past — like Lavasoft's Ad-Aware and Spybot's Search and Destroy — that are free and should be run on a weekly basis.

**3. Turn off your computers at night.** Old-think said that there was no need to turn off computers when you left for the day; that it was actually better to let them run. But “botnet trojans” that install on your machines and use them for criminal purposes generally do so in the middle of the night, when no one is using the machine and might notice the unusual level of activity. A machine that is turned off can't be infected as easily.

**4. Separate work and play.** It may seem churlish to tell employees that they can't check their Facebook page during work hours, or do a little shopping. But it's the only way to stay safe. Make the policies, and make them stick. No software installed on any office machine unless approved. No visits to websites that are unnecessary for work. No kids using business machines ... not even in the home office.

**5. Check your computers regularly.** Small businesses are favorite places for criminals to stick their data — credit card numbers, child pornography and other malware. They like small businesses because security is more lax and they can move their data in and out with ease. Do a sweep of every computer on a regular basis,

looking for anything that does not belong, including personal files of employees that

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

## Reality Check

*A compendium of ideas, products, rants and raves from the viewpoint of the author. Note that the author has no financial interests in any of the products mentioned. Feel free to disagree, or to share your ideas by sending them to [davemcclure@cpata.com](mailto:davemcclure@cpata.com).*

**Internet Site of the Month: Market America (<http://www.marketamerica.com>).**

One of the fastest-growing e-commerce sites on the planet, a “trusted partner” of the better business bureau, and shoppers get cash back when they shop at such major sites as Walmart.com and Amazon.com. It's also a more secure way to shop, since you know that the website has been vetted properly. Nope, I am not affiliated with them, but I do like their model for safe shopping online.

[Thumbs Up] – **The Blackpad.** Here's competition for the iPad (and Samsung's Galaxy) tablet computer from BlackBerry. Dubbed the Blackpad, it gives the “crackberry” addicts a pad of their own. An estimated 25 million units are in production, featuring a 7-inch display, two cameras (including one that can be used for video conferencing), Bluetooth and wi-fi capabilities. The down side? No 3G or 4G capability so far.

[Thumbs Down] – **Email Retention Policies.** Chances are good you don't have any, and that can be a costly mistake. If you are sued, you will be compelled to produce ALL documents, including email, that may pertain to the case. Don't have them, or can't easily search them? You'll pay dearly for this oversight.

[Thumbs Sideways] – **Wiretapping Your Cell Phone.** Legislation expected to be introduced into Congress next year would extend the wiretapping laws to computing devices and cell phones, as well as social networks. As with most security laws, this is both good news and bad. Do we protect terrorists and criminals or do we protect the privacy of consumers. Law enforcement agencies generally have a poor record when

it comes to abusing wiretap laws, but it makes sense to update the laws we have for

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

[Thumbs Up] – **Comcast's Xfinity Online**. While I am an old DirecTV guy, I am following with interest the moves being made by cable giant Comcast. The latest is an effort to update the company's "TV Anywhere" strategy by offering cable content where you want to watch it — on TV, online or on a cell phone. It's a good use of emerging technologies and will be interesting to watch as television services evolve.

Technology

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.

© 2024 Firmworks, LLC. All rights reserved