

# tools of the trade

## Easy Note-taking

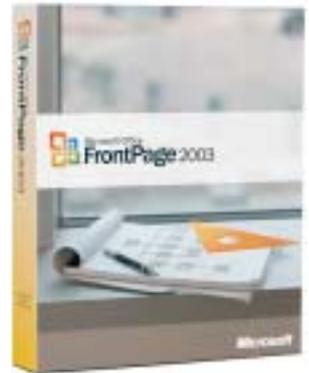
The WizCom Technologies' **Infoscan** looks like a marking pen, and you sweep it across printed text in the same way you would to leave a yellow highlight. But nothing appears on the page. Instead, the highlighted text appears on a screen on the pen, and there are seven very small buttons to direct the words or numbers you have captured. The Infoscan is a scanner, an electronic note-taker, that fits in your pocket. It will store an



amazing 500 pages of printed data, and you transfer those "notes" to your PC with a USB or serial cable connection or to your laptop or PDA via the infrared connection. The notes are fully editable MS Word documents. You can work with the Infoscan connected to your computer (tethered mode) or disconnected (mobile mode). You don't mark the documents—you capture them with a device that weighs less than three ounces. There's also a WizCom SuperPen model that can store and transfer data (including tables for Excel with cells that retain their original format) and say the line or word aloud with built-in Text-to-Speech technology. The SuperPen can be loaded with any of 30 free dictio-

naries so that it can translate text into English or just define using medical, computer, scientific, or Wall Street specific dictionaries from the Houghton Mifflin collection. Read about both pens at [www.wizcomtech.com](http://www.wizcomtech.com).

**Microsoft's FrontPage 2003** is the latest version of its website creation software. FrontPage lets you create and manage a website without learning HTML code. Using a WYSIWYG (What You See Is What You Get) environment, the pages are built using wizards and drag-and-drop elements and styles. On each page you can click between different views. Page view shows an editable view in Normal, HTML Code, and Preview modes. You can directly edit the page coding in the second of these views or use familiar MS Office tools and menus without bothering with code. Folders view opens a familiar Explorer style list-



Microsoft FrontPage 2003

ing of files and folders. A Reports view offers a variety of information from which pages load slowly to where broken hyperlinks appear. A Navigation view maps the pages of the entire site, and a Hyperlinks view charts the linked connections on the pages. A final Tasks view registers where and when scheduled tasks are to be completed. New with the 2003 edition are interactive buttons for rollover images with hyperlinks, a split view of the Design and Code views on the same page, and dynamic Web templates that let you create multiple templates. You can add Macromedia Flash content, use a smart Find-and-Replace function, utilize XML support, and much more. A list of



WizCom Infoscan pen

## Spam Wars—The Litigation Begins

◆ Michael Castelluccio, Editor

■ FIRST IT WAS A PING-PONG MATCH limited to just the players. You got spam, you put a spam filter in place. The spammers adjusted their subject lines and hid their addresses to get over that net, so you downloaded a heavy-duty spam blocker. They made their adjustments, and you spent even longer emptying out your e-mail inbox. Herbal supplements, low-cost loans, porno, mortgage advice, your aunt telling you to forward some message to 10 others or the world as you know it will end. Next up, perhaps, are all those marketers who are being shoved off phone queues because of the national no-call legislation.

Dave Farber, one of the original pioneers of the Internet, said in a recent interview in *Salon*, "Over the last six months the amount of spam has gone up phenomenally. This last virus or worm that started generating huge volumes of e-mail sort of broke the back. It's not too late, but I think it's getting to be close to too late. If you believe in the old atomic scientist's clock, it's five minutes to midnight."

And when the clock strikes 12—what happens then? A complete collapse of the whole e-mail system? Will people just abandon their e-mail addresses as the mail servers fill and spill over at ISPs all over the world?

*continued on next page*



Fingerprint Cards System

all the new features are on the Microsoft site at <http://www.microsoft.com/office/preview/frontpage/default.asp>.

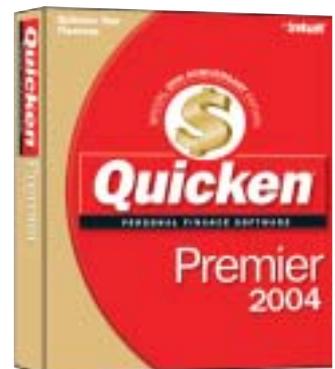
**Fingerprint Cards AB**, based in Sweden, offers several versions of its fingerprint scan technology, including an area sensor system and swipe sensor system. Both read an individual's fingerprint and match it against its stored database for verification. The technology can be used to secure computers

by directly connecting the scanner to the computer, or it can be embedded in devices that lock passageways, containers, or cabinets. Partners working with Fingerprint Cards are developing markets for physical access control and time and attendance applications, both of which operate without cards and badges. AcciMetrix has created a gun holster that locks a gun in the holster with a mechanical clip and fingerprint-activated releaser.

Information on the two versions of the technology is available at [www.fingerprints.com](http://www.fingerprints.com).

Intuit's **Quicken 2004** is available in four versions: Deluxe, Premier, Premier Home and Business, and Quicken for Mac. The program still maintains its lead in personal finance software with 15 million active individual Quicken users. For anyone not familiar with the basic functions, there are online demos at the Quicken website. An added advantage of the Premier edition for Windows is a new Express Account Setup that instantly connects Quicken to your financial institutions and then downloads your transactions and balances while setting up your account so you start with updated

information. There are a number of personal investment functions, such as Capital Gains Estimator, Mutual Funds Insight, and tax reports for Schedules A, B, and D. The Premier Home and Business program has Detailed Net Worth Monitoring, Flexible Investment Tracking, and Market Performance Comparisons. For side-by-side comparison of the versions, go to [www.quicken2004.com](http://www.quicken2004.com).



The New Quicken

## Fighting Back

As the horizon darkens, there are those hauling the first big guns that will soon be in place on a number of fronts around the world. Rather than defend against the assault with filters and blockers, these spam warriors are setting up cannons to answer the next serve launched over the 'Net at them.

Maybe it wasn't heard 'round the world, but one of the first loud volleys was fired in the U.K. Britain established a law that imposed a £5,000 (\$8,057) fine for spammers convicted in a magistrates court. If the offending sender loses in a jury trial, the fine would be unlimited, and a prison term could be attached. The law will go into effect December 11.

Italy had preceded England with its own anti-spam law. There the fine can go as high as 90,000 (\$101,600) with jail time not to exceed three years.

Here in the U.S., some states have also joined the counterattack. California leads with the toughest legislation. A law was signed by Governor Davis in September that would punish unsolicited commercial e-mail sent or received within the state with fines of up to \$1 million per incident. It will take effect January 1. The law, like most other anti-spam legislation, exempts e-mail that is sent to a recipient who has an existing business relationship with the sender. But in that case it requires that the sender include an opt-out message with the mailing.

Washington state has an older law (1998) that's not as severe. Washington will fine an e-mail offender \$500 per message for spam with misleading subject lines, fake reply addresses, or hidden transmission routes.

Actually, 36 of the 50 states have active legislation of one sort or

another against spam, but as Scott Perry, head of Postini Inc., was quoted in Informationweek.com, "[state legislation] doesn't seem to have affected the spam issue that much."

The problem is enforcement—a problem with two sides. First, there's the cost of enforcement. Some states encourage the e-mail-blitzed citizen to sue. Realistically, that's not much of an option. How is the average person going to track down the mailer when the addresses and routes are faked? The states that take on the pursuit themselves are likely to be in the midst of draconian cuts in every department, so the question becomes, "Where does e-mail fit on their priorities list?" Dave Crocker, a Farber student, calls the state initiatives "research activity for a future federal law." His teacher adds, "You need somebody out there with the bank account, like the Federal Trade Commission or the Federal Communications Commission. The FCC did a good job with fax spam."

There's a Criminal Spam Act of 2003 wandering around Congress, but it's likely to undergo a name change with little chance of passing this year. There's also a bill sponsored by Orrin Hatch (R.-Utah) and Patrick Leahy (D.-Vt.) that was passed by the Senate Commerce Committee, and the two pieces of legislation need to be combined. But probably not this year.

The second problem with anti-spam legislation concerns jurisdiction. As copyright and tax lawyers have discovered, the Internet can be somewhere, anywhere, and nowhere at the same time. A domain online is not the same as what we normally think of as a domain on terra firma. Do the spammed in Massachusetts get to sue somebody in Martinique? How?

All the legal considerations might

be moot if the technical challenge of locating the perpetrator overwhelms your resources. When a hacker shuts down businesses across the globe, costing economies millions of dollars, euros, pounds, and yen, you can understand every country loosing the hounds. And the FBI or some other agency often locates the hacker because the search is given such high priority. But would the same effort be expended to track down junk mail processors?

## Counterattack

An ominous report from the front hit the airways in late September. On September 25, Reuters reported that three websites that provide spam blocking lists were hit and shut down by denial of service attacks—massive mailings that overwhelmed their systems. The Spamcon Foundation, Osirusoft, and Monkeys.com were hit in what some experts theorized was the next level in the war on spam. Andrew Barrett of Spamcon was quoted as saying, "There seems to be a methodical, well-planned attempt to use preassembled networks of zombie machines to create sustained denial of service attacks on servers where these block lists run."

When you combine the September assault with the theory that the SoBig virus earlier this year was nothing more than an attempt to take over thousands of computers worldwide to be used as forwarding mailers for spam, you might be drawn to an unnerving conclusion. Perhaps the other side is also rolling up and loading their own heavy artillery, and the ping-pong game is about to escalate to trench warfare well beyond our current, maddening cycle of open-delete/open-delete/open-delete/open-delete. ■