



Business » News

Monday, April 12, 2006


Security matters

Unprepared computer users face shaky future



By **CAROLINE LYNCH**
 clynch@courier-journal.com
 The Courier-Journal

Subscribe!
 Click [here](#) to get the C-J delivered to your door each morning.



First the computers slowed down.

Then the e-mails stopped making sense.

By the time the Louisville company sought help from Network Advocates, it was less than 24 hours from time to prepare payroll.



One virus wasn't to blame; thousands were. And a hacker was likely tracking keystrokes via an overseas computer, which could have provided access to bank account numbers, passwords and other private company data.

The labor bill alone was \$4,400. About \$900 in protections could have prevented the whole mess, said Tom Troutman, president of Network Advocates.

"The good thing about the Internet is that we're all connected," Troutman said. "And the bad thing about the Internet is that we're all connected."



PHOTO ILLUSTRATION BY HYANGSOOK LEE, THE COURIER-JOURNAL

Clinical Research Coordinator

Engineering
 Willing to consider a new career...

Drivers
 WERNER ENTERPRISES SPECIALIZED...

Physical Therapy
 Physical Therapy Staff &...

Retail
 JOBS AVAILABLE! SALES ASSOCIATES I...

[All Top Jobs](#)

About Top Jobs



GET GROCERY COUPONS HERE!



» **FREE!** «
PRINT YOUR OWN COUPONS!



Click here

[to print coupons.](#)

Tips and help

The Better Business Bureau, Federal Trade Commission and the National Cyber Security Alliance suggest small-business owners take these and other precautions to protect their data:

- Keep updated anti-virus software running on all computers.
- Back up data weekly.
- Install firewalls.
- Check software vendors' Web sites regularly for security patches.
- Develop a security policy to let employees know how to handle e-mail, Internet usage, backup procedures and computer infections.
- Turn off the file-sharing function unless absolutely necessary. Forbid employees from

As the Internet brings millions of users uncomfortably close, information is a hot item and scam artists are targeting the unaware and unprepared.

Computer security issues happen just as often to small businesses as they do to large. An increasing number of complaints have spurred both local and national agencies to address the subject.

For the first time last week, the Better Business Bureau issued a checklist for business owners on how to secure their servers, said Sarah Rolfingsmeier, communications director for the local bureau. The list was issued jointly with the Federal Trade Commission

downloading file-sharing programs.

- Use passwords that include numbers and upper and lowercase letters and require changing every 90 days. Systems should lock out users who get a password wrong three times.

- For a full list of recommendations, go to: www.ftc.gov/opa/2006/04/cybersecure.htm.

For more help:

- The Information Resource Technology Center is launching the state-funded Kentucky Regional Information Security Testing Lab to evaluate businesses' IT security for a low cost. Call director Jim Graham at 852-0900.

- Network Advocates lists best practices at networkadvocates.com/press/techtips/.

- Suspect an e-mail or Internet scam? Call the Better Business Bureau at 583-6546.

and the National Cyber Security Alliance.

"The reason we've done this is because there's an increase in scam artists targeting consumers and small businesses," she said, adding that the bureau is trying to tie the reminder to the time change, hoping businesses will remember to update twice yearly.

Louisville's Information Resource Technology Center (iTRC) is spending \$250,000 to launch the Kentucky Regional Information Security Testing Lab, a program that will evaluate companies' security systems — from policy to firewall — and produce a low-cost vulnerability assessment.

"We'll hack in and tell them where their weaknesses are," said Jim Graham, director of the technology center.

Graham said the need is critical because of the devastating effects of having information stolen and

the high costs of cleanup. He said small businesses often don't devote the resources to protecting their network because they don't have the time or the know-how, and don't see an immediate impact on their bottom line.

"It's like insurance — you don't think about it unless you have an accident," he said.

Graham and other experts said it's best for small-business owners to outsource their technology needs. However, there are still some basics they need to know.

Firewalls vital

Firewalls, the first line of defense, keep the bad guys out and the good guys corralled in the right space. Troutman says they are essential and recommends getting a good one.

"As the malicious community gets smarter and better, the firewall has to stay smart too," he said, adding that high-speed Internet connections leave computers constantly online, making them more available to hackers.

Firewalls, available where software is sold, should be put at every point where the computer system is connected to networks, says the Better Business Bureau. Even small, home-based businesses need them, Troutman said.

'All but shut us down'

Darrin Jenkins, network administrator for nonprofit Kentucky Baptist Homes, got hit hard last year by the Lovesan virus, which came while the agency was changing its network layout and had fewer precautions. "One of the viruses created so much traffic on our network, it all but shut us down," he said. "The good data couldn't move. That one took us a couple of days."

Troutman said business owners can equip one computer with an anti-virus program for under \$50, and most update themselves.

Back up, educate

From client lists to accounting records, some small businesses would be out of business without their records, but many don't properly back them up.

Joe Sykora, owner of Fortress Network Security and InterSpace Computers, said even when businesses back up their information, they rarely double-check the system. He's seen enough blank tapes to know.

Another problem he sees is small-business owners buying wireless Internet kits without understanding the increased risks. Ask a professional before you delve into wireless, he said.

But education is one of the biggest defenses against compromising your data, experts agree.

Graham acknowledges that keeping up to date can be a challenge when Microsoft and other companies are updating "patches," or corrections to weak spots, almost daily. That's why he suggests outsourcing.

As privacy laws have popped up to govern what information must stay hidden, companies get themselves in legal trouble if they have slips. Hackers can get owners in legal trouble too.

Troutman recently helped a company whose server a hacker used to store movies. That situation could have caused copyright lawsuits, he said.

He's also seen financial and image problems.

"I wouldn't connect a business to the Internet for three seconds without a firewall, anti-virus software and security patches," he said. "It's like building a building, putting in gates and guards and passkeys and fences, without realizing you'd built a west wing you didn't protect."

[^^ Back to top](#)

[Home](#) · [News](#) · [Sports](#) · [Business](#) · [Features](#) · [Scene](#) · [Velocity](#) · [Classifieds](#) · [Jobs](#) · [Cars](#) · [Homes](#) · [Marketplace](#) · [Contact Us](#) · [Search](#)