

**IN THIS STORY**

1. [Wireless attacks: Wave a white flag?](#)
2. [Neighborhood watch](#)
3. [Courts to set expectation](#)

**RESOURCES**

[IT Product Finder](#)

[Special Reports](#)

[Downloads](#)

[Tech Jobs](#)

[White Papers](#)

[RFP Center](#)

[Letters to the Editor](#)

[Subscribe to Newsletters](#)

[Events Calendar](#)

[Register for Classes](#)

[Online Book Library](#)

[Contact the Editors](#)

[E-mail Publishing](#)

[Managed Hosting](#)

Search:

Wireless attacks: Wave a white flag?  
**Neighborhood watch**

By Robert Lemos  
Special to ZDNet  
July 1, 2002

[TalkBack](#)

[E-mail this](#)

[Print this](#)

Residential neighborhoods are rife with unprotected networks as well. From the top of an office building in a mainly residential area of Seattle, several students learning hacking and security from IOActive's Pennell were able to find more than 30 wireless access points, most with no security.

David Pollino, managing security architect for digital security firm @Stake, is concerned that few people are taking the wireless problems seriously. "Too many people are buying access points, taking them out of the box, and plugging them in," he said.

Moreover, because those who use wireless networks at home typically don't keep access logs, the threat goes beyond legal responsibility for damages because they could easily be fingered as the perpetrator, Pollino warned.

When the notorious Melissa virus struck in March 1999, law enforcement officials quickly tracked its release to an America Online account that had been hacked. AOL's logs indicated that the person who released the virus dialed in with a telephone number that didn't belong to the account owner.

"Right now, the account owner has a good story to tell over a beer," Pollino said. "But what would have happened today if the person who released the virus got into AOL through a home (wireless) network? The trail would have gone cold at the victim's house, and they would likely be arrested."

In addition, if an attack does a great deal of damage, the individual or company whose account was used in the hacking could face enormous liability charges, said Joseph Burton, a lawyer with Duane Morris who focuses on information security issues.

Until now, Burton said, companies have been afraid to sue others for their security problems. "Companies are reluctant to bring the cases, because it's like living in a glass house and throwing the stone. Everyone is at risk."

advertisement

**@BUSINESS INFRASTRUCTURE**

---

**INTEGRATED  
INFRASTRUCTURE**

**NOW YOU'RE TALKING  
E-BUSINESS.**

>> Click for IBM's latest integration white paper.

[← Previous page](#) | [1 2 3](#) | [Next page →](#)

**RELATED INFO**

**ARTICLES**

- ▶ [Where wireless is most vulnerable](#)
- ▶ [Warchalking marks Wi-Fi 'hot spots'](#)
- ▶ [Microsoft tightens security for Wi-Fi](#)
- ▶ [Visit the Security Update Center](#)

**PRODUCTS**

- ▶ [Cisco Aironet 340 wireless bridge](#)
- ▶ [Vernier Networks AM 5400 Access Manager](#)
- ▶ [ReefEdge Connect Server 100](#)

Tech Update Today

Linux Update

eBusiness Update

Security Update

Tech Update Weekly

Windows 2000/XP Update

- ▶ [All newsletters](#)
- ▶ [FAQ](#)
- ▶ [Manage my newsletters](#)

 [E-mail this](#)

 [Print this](#)

## TELL US YOUR OPINION

TalkBack: [Post your comment here](#)

Comments? Questions? [Tell us](#) what you think.

 **Services:** [IT Jobs](#) | [Wireless ISP Info](#) | [BizTech Library](#) | [2GHz Notebooks](#) | [Bluetooth](#) | [Clearance Sale](#)

CNET Networks: [Builder](#) | [CNET](#) | [GameSpot](#) | [mySimon](#) | [TechRepublic](#) | [ZDNet](#)

[About CNET Networks](#)

[About Us](#) | [Support](#) | [Your Privacy](#) | [Service Terms](#) | [How to Advertise](#) | [ZDNet Jobs](#)

Copyright © 2002 CNET Networks, Inc. All rights reserved. ZDNet is a registered service mark of CNET Networks, Inc. ZDNet Logo is service mark of CNET Networks, Inc.