

# Cyberstalking rears its head in the workplace

MSNBC

Published on [ZDNet News](#): April 24, 2001, 5:00 PM PT

**She was a young, attractive, friendly single clerk. He was an obsessive network administrator with access to the entire company's computer systems. She turned him down; he wouldn't take no for an answer. The side comments, e-mails and creepy looks never stopped. Eventually, he was fired, and that's when the trouble really started.**

Armed with full knowledge of the company's network, he had little trouble breaking into its computer system from the outside. He assumed several identities and started firing off embarrassing e-mails about her around the firm. He took secret documents and, posing as other company employees, made veiled threats to release the secrets to the public. Meanwhile, he continued to try to get a rise out of the clerk. At one point, he "gave" her a \$130,000-a-year raise.

Fortunately, he did most of his dirty work sitting behind a computer at his new employer--and with one e-mail, he made a mistake.

"He sent it from his work account rather than an assumed account," said Eric Friedberg, a former prosecutor for the U.S. attorney's office in New York. Friedberg now operates a private computer crimes consulting business called Stroz Associates. Armed with that single e-mail, Friedberg went to the suspect's new employer and got the firm's cooperation. Computer logs there provided plenty of evidence, and the suspect has now been indicted.

The Internet's annals are full of horrible, it-could-never-happen-to-me stalking cases.

There's the California woman whose home address was published in Usenet groups by an ex-boyfriend, along with a message indicating she fantasized about being raped. Six volunteers arrived within days. And there's Amy Boyer, murdered by a stalker who tracked her using an online database.

But cyberstalking doesn't have to come in such fanatical flavors, and it doesn't happen only in the far corners of the Internet, on bulletin boards or in chat rooms.

Stalking is going mainstream, some say. The gender gap is slipping; by some measures, women are the harassers in nearly one-third of cyberstalking cases. And stalking has made its way into the workplace, where jilted lovers follow the object of their obsessions virtually as they head to the office. Thanks to stalking's terrorizing cousin identity theft, interoffice stalking incidents may even be increasing, said Parry Aftab, who runs Cyberangels.org, an online stalking victims resource.

"It's moving back into the workplace in a very serious way now," Aftab said. Of the 600 or so cases of stalking reported each day to Cyberangels, she says about one-fourth involve office problems.

And it's not just jilted lovers. In one recent case, an employee who felt he had been passed over for a promotion to CEO launched into a calculated fury of identity theft-based harassment. Slowly but surely, the middle-aged middle manager started generating interoffice e-mails among co-workers, noting every time the CEO was late for a meeting or left work early. He'd drop notes making it clear that the CEO was being watched, commenting on the particular tie he had on that day or something that was said in a meeting. Eventually, the notes escalated and the stalker threatened to manufacture a fictitious pedophilia addiction in the CEO and expose it before the company.

"He did it all from a cybercafe near the office," Aftab said. "He thought he was anonymous. But we figured out that the e-mails were coming from that cafe, and they only showed up when he wasn't in the office."

## **What makes a cyberstalker?**

There is some disagreement among experts about whether the Internet has led to a rise in stalking cases or simply shifted the way stalkers do their thing. Mark Zwillinger of Kirkland and Ellis, a legal team of computer crime experts, thinks sending a nasty e-mail is so quick and easy that it sends some folks over the edge who might not otherwise be stalkers.

"Technology is an enabler that changes the risk-benefit calculations of a person who commits the crime," he said. His firm recently investigated a case in which a co-worker stole another worker's identity and started sending racially inflammatory e-mails to the firm in the victim's name. "When you're really pissed off and have a real grip, it's simple, it only takes a minute, and that's why it's a problem," Zwillinger said.

Perceived anonymity plays a role, too, said Jayne Hitchcock, a former cyberstalking victim who now runs Working to Halt Online Abuse.

"A person who wouldn't normally do it in real life thinks, 'I can do it online. I'm going to e-mail her and tell her off. They'll never know it's me,'" she said. In most cases, stalkers fail to cover their tracks and their trails are easily discovered, Hitchcock added. "They're not necessarily technically savvy people."

### **When stalkers are smart**

But some are, and that can make things even worse. Former CIA psychologist Eric Shaw helps investigators profile stalkers, and he thinks the world of information technology sometimes provides an unhealthy outlet for socially challenged people.

"They latch on to the IT world as a way of belonging. The IT world is often everything to them. It's a way they can be important, meaningful and have power," Shaw said.

When a firm's internal IT people are involved in harassment, it creates a dangerous combination of skills and access, one Friedberg says he's seen repeatedly-- in large part because many firms give little thought to the tremendous access computer experts have to company information.

"They are in a position where large numbers of both internal and IT consultants have access to key corporate assets, and they aren't willing to spend the money for thorough background checks," he said. "All companies need to give serious thought to checks and balances they're going to bring to bear on people that have that access."

### **The company in the middle**

Companies embroiled in a harassment or stalking case suddenly find they face a bevy of difficult decisions. No firm wants the bad publicity associated with such a case, particularly if it involves both harassment and a breach of computer security.

That's why companies sometimes avoid turning to law enforcement, and one reason boutique computer crimes firms like Stroz are becoming an attractive alternative.

Still, even with private investigators on the scene, there are tough choices. Friedberg said the company and the victim in the jilted lover case were willing to let the situation play out a little while investigators hunted for clues and evidence that would stand up in court; but that's risky. At any moment, the suspect could do something terribly embarrassing for the company or divulge critical secrets.

Victim companies sometimes just decide to cut their losses, secure the network and hope the harasser just goes away. Of course, there's a long-term risk that he or she might return if not caught.

"Companies are in a box regarding how much risk they are willing to tolerate," he said. "Generally in a workplace violence situation, you don't know it's workplace violence while it's brewing. You have to make a difficult judgment as to how quickly you act, whether speed or more serious proof is your priority."

Complicating that choice is the potential liability of the company if an employee suffers real harm. The threat of potential lawsuits means most companies act quickly, Hitchcock said.

"Most victims go to their employer and it gets taken care of," she said. Simple advice she gives companies is to immediately change the victim's e-mail address and phone number and have all e-mail sent to the old address directed to a network administrator for safe-keeping, in case it's needed later by law enforcement.

"We have seen a handful of cases where the employer said, 'Just ignore it.' But they have to understand that if a person who is harassing using their e-mail system, they are attacking the company, too."

### **What to do**

Organizations like WHOA.org and Cyberangels also offer 24-hour-a-day, 7-day-a-week advice to victims and corporations. Hitchcock says most of the time, stalkers retreat immediately when they find out they can be arrested or sued.

"We can resolve over 80 percent of reports quickly," she said. "Most online stalkers think they are anonymous, but when they find out they aren't, they usually back off."

Of course, the other 20 percent require much more careful tactics. Among the advice both Aftab and Hitchcock give victims is to be sensitive to the possibility of harassment right away. Don't engage in back-and-forth dialogues over e-mail that feel uncomfortable; just simply say, "Stop contacting me," and resist the temptation to respond to further inquiries. The harasser wants reaction, so many situations can be diffused before they get out of hand by not responding. Meanwhile, save all e-mails or voicemails and report them to the company.