At work, all e-mail can be public

By DAN RICHMAN
P-I REPORTER

By now, most employees have gotten the message: It's both technically possible and legally permissible for your employer to read e-mail you send or receive at work.

That seems logical. If you're using an e-mail address ending with your company's name -- a type of e-mail known as POP3 (Post Office Protocol) -- the address makes it clear that the company owns the domain name and the server on which the e-mail system resides.

But what about Web-based e-mail, such as Gmail, Hotmail and Yahoo Mail?

Sure, you write and read it on your employer's computer, but it somehow seems like it's more private. You can access it from anywhere, and the company's name isn't part of your address.

"Web-based e-mail is absolutely perceived to be more secure by many employees, but I think employers can monitor it," said Virginia Culler, 26, a freelance writer who lives in Capitol Hill.

Right on both accounts, experts say. They warn workers to curb their tendencies toward unfettered personal expression, whistle-blowing and any other activity on the Internet that they'd rather the world not know about.

"There really isn't any difference between POP mail and Web mail," said Bruce Schneier, chief technology officer for BT Counterpane, a security-services company in Mountain View, Calif.

"There's nothing less secure about Web-based e-mail -- it's all insecure."

Monitoring software, easily found on the Internet and available for as little as $50, claims to record all programs used, keystrokes typed and Web sites visited, and can capture each user's screen hundreds of times per hour. With this software, employers can know what you've written even before you send it.

Even if e-mails aren't read as they're being typed, they can be intercepted while in transit. Employers can install filters on traffic moving onto and off of their servers, scanning for keywords or phrases that would alert them to breached confidences or unlawful behavior.

One piece of software, located in seconds through an Internet search, offers e-mail activity-recording features and specifically says that it records Hotmail, Yahoo and Gmail.

"Even when they delete their e-mail," the product "will keep a copy for you to review," its ad claims.
At work, all e-mail can be public

In the alternative, a company's information technology department can browse the temporary Internet files that are created each time a Web-based e-mail message is received, said Ira Winkler, a computer-security expert based in Annapolis, Md.

In his view, "you are a little bit, and I mean a little bit, safer using Web browsers than POP3," because POP3 e-mails are probably stored longer and are more likely to be examined than temporary Internet files.

"Still," he said, "if you are intermingling your personal and business e-mail, you are in trouble."

Even if you're telecommuting, your employer can monitor your home computer, said Lewis Maltby, president of the National Workrights Institute in Princeton, N.J.

"If the company has software that's monitoring computers in the company network, when you log on from home, you're at risk," Maltby said.

Computers using a wireless Internet connection are inherently insecure, because that connection is subject to interception through widely available software. Such software can display not only the contents of e-mails but also the owner's login and password, unless encryption is used.

OK, so employers have the ability to read pretty much all unencrypted e-mails. Do they also have the legal right?

In general, yes, though perhaps somewhat less so in Washington state.

In most of the nation, it's lawful to monitor computers, even without notice, the Privacy Rights Clearinghouse says in an online bulletin. More broadly, "the state of the law as to the private sector is there is no right to privacy in the workplace, provided the employer has negated any expectation of privacy, either in handbooks, manuals or postings," said Evan Spelfogel, a New York labor lawyer.

Public-sector employees or workers living in California may have slightly more rights against such monitoring. But even if an employer has a stated policy ensuring privacy in e-mails, it may disregard that policy in cases of wrongdoing, the clearinghouse says.

Washington employees have been protected in some at-work communications since the 1970s by the state's privacy act, said Ivan Orton, a senior deputy prosecutor with the King County Prosecutor's Office.

He said that under that law, an employer is vulnerable to criminal prosecution and a civil suit if it intercepts e-mails sent to or from work, unless there is a labor-management agreement in place allowing such behavior, or the employer has announced a policy of monitoring e-mail.

Still, to be completely safe, "People should have no expectation of privacy on the Internet," Winkler, the computer-security expert, said. "It's natural to express yourself fully in e-mail -- but before it reaches me, it goes through about a dozen computers. The reality is, it's available not only to your employer but to anyone along the way."

**HOW TO SECURE YOUR E-MAIL**

- Russian carrier flies 747-400ER
- Its U.S. traffic slowing, Starbucks to run first national TV campaign
- SEC drops rule on overseas accounting
- Need holiday cash? Dell helps grease the wheels
- Business Briefing
Encryption is one way e-mail can be made more secure. Even if encrypted e-mail is intercepted, it can't be understood without a major cracking effort. Secure e-mail certificates, offered at no charge on several Internet sites, both encrypt e-mail and prove to recipients that you are who you say you are. But not all of them work for all browsers, and at least in some instances, recipients must use the same service. Employers may also forbid loading encryption software on employee PCs.

P-I reporter Dan Richman can be reached at 206-448-8032 or danrichman@seattlepi.com.