Google tool poses privacy risk

Anick Jesdanun
The Australian
OCTOBER 19, 2004

PEOPLE who use public or workplace computers for e-mail and web searching have a new privacy risk to worry about: Google's free new tool that indexes a PC's contents for quickly locating data. If it's installed on computers at libraries and internet cafes, users could unwittingly allow people who follow them on the PCs, for example, to see sensitive information in emails they've exchanged. That could mean revealed passwords, conversations with doctors, or viewed web pages detailing online purchases.

"It's clearly a very powerful tool for locating information on the computer," said Cambridge-based privacy and security consultant Richard M. Smith. "On the flip side of things, it's a perfect spy program."

Google Desktop Search, publicly released last week in a "beta" test phase for computers running the latest Windows operating systems, automatically records e-mail you read through Outlook, Outlook Express or the Internet Explorer browser.

It also saves copies of Web pages you view through IE and chat conversations using America Online's instant-messaging software. And it finds Word, Excel and PowerPoint files stored on the computer.

If you're the computer's only user, the software is helpful "as a photographic memory of everything you've seen on the computer," said Google director of consumer web products Marissa Mayer.

The giant index remains on the computer and isn't shared with Google. The company can't access it remotely even if it gets a subpoena ordering it to do so, Ms Mayer said.

Where the privacy and security concerns arise is when the computer is shared.

Type in "hotmail.com" and you'll get copies, or stored caches, of messages that previous users have seen. Enter an e-mail address and you can read all the messages sent to and from that address. Type "password" and get password reminders that were sent back via e-mail.

Acknowledging the concerns, Ms Mayer said managers of shared computers should think twice about installing the software until Google develops advanced features like password protection and multi-user support.

In the meantime, users of shared PCs can look for telltale signs.

A multicolored swirl in the system tray at the lower right corner of the computer desktop means the software is running. A user can right-click on that to exit the program — thereby preventing it from recording web surfing, email and chat sessions.

Users can also surf on non-IE browsers like Opera and Mozilla, although the software may index web pages already stored before the software gets installed.
Managers of public access terminals can also install software or deny users administrative privileges so they can't install unauthorised programs, such as Google's. In fact, many libraries and cybercafes already do so.

Herb's Cyber Cafe owner Herb Jones tried out the desktop search program on his computer and likes it — but he won't install it on his two public terminals. In fact, he's written software to prevent customers from installing programs like it.

"Otherwise, they can put on their own files if they want, a worm, a virus, anything, and you're shut down," Mr Jones said.

The FedEx Kinko's chain is also taking preventive measures. It's deploying software designed to automatically refresh its public access terminals to a virgin state for each new customer. So any errant software would disappear, as would any personal settings, files or web caches, said Maggie Thill, a spokeswoman with FedEx Kinko's.

But policies do vary, and no precaution is foolproof, warned Carol Brey-Casiano, president of the American Library Association.

"We do our best to protect our patrons and computers and network, but as you can imagine, thousands of people can use public computers in a given week," she said.

The new Google tool would not only aid people in spying on past patrons on public PCs. At home, users could record their kids' instant messaging conversations or view a spouse's email. In the office, employers could index what their workers are up to.

If each user has a separate logon to Windows, Google Desktop Search will be stymied, however. That's because only one person can install and use the software on a given computer.

The power of Google's software relies on centralizing what's already saved on computers; most browsers, for instance, have a built-in cache that keeps copies of web pages recently visited. The difference is that Google's index is permanent, though users can delete items individually. And the software makes all the items easier to find.

The software can also betray users, said Annalee Newitz, policy analyst at the Electronic Frontier Foundation. Delete an e-mail or file, yet a copy remains on Google's index.

Neel Mehta, leader of the X-Force research and development team at Internet Security Systems, said the threats are real, though there are plenty of other products available for spying — ones better at doing the recording secretly.

"It's not designed to be an illicitious tool," Mr Mehta said of the Google software. "It's designed to be a search engine."

The Associated Press

This report appears on australianIT.com.au.