

The Hidden Risk Of File-Sharing

By JOSEPH DE AVILA
November 7, 2007; Page D1

Many of the hundreds of millions of people around the world who swap music, movies and other digital content on their personal computers over the Internet have inadvertently put themselves at risk of identity theft.

Users of popular file-sharing services such as LimeWire have found themselves victims of identity theft when their personal information was inadvertently shared on a so-called peer-to-peer network. And recent high-profile breaches via these networks have put thousands of people's financial information at risk. The problem typically arises when users set up file-sharing software and create a folder for their downloads in the same location as their personal files.



Wesley Bedrosian

Precise data on the incidence are hard to come by, in part because personal information can be accessed many different ways, and victims may not think to blame their file-sharing activities. But identity-theft experts say the problem is real and growing.

The risk from file-sharing "will get worse before it gets better," says Don McGillen, executive director of Carnegie Mellon CyLab, an initiative of the university in Pittsburgh that develops computer-security technology.

In the latest incident, a Seattle man this week pleaded guilty to charges of identity theft for using LimeWire to steal tax forms, credit reports and student-loan applications from the computers of more than 50 people. He used the information to set up phony credit accounts to

buy merchandise online.

[Citigroup](#) in September confirmed that it was looking into a data breach where the names and Social Security numbers from 5,200 customer accounts were inadvertently leaked by an employee using LimeWire. And in June, [Pfizer](#) said the names and Social Security numbers of

17,000 current and former employees were leaked after the spouse of an employee downloaded file-sharing software onto a company laptop. Both companies say they aren't aware of any identity theft linked to the breaches, but they have offered the affected employees or customers free credit monitoring.

In another case involving charges of identity theft, computer crime and racketeering against a group in the Denver area, the final defendant pleaded guilty last week to racketeering. The group had used LimeWire to access several financial records and used the money from their practices to buy methamphetamine, according to the indictment.

"Once the meth addicts have discovered it, it is in widespread use" for identity theft, says Tom Sydnor, director of the Center for the Study of Digital Property with the Progress and Freedom Foundation in Washington, D.C.

Regulators, identity-theft experts and the file-sharing services themselves acknowledge the growing risk and are taking steps to address it. Last month, the House Oversight and Government Reform committee sent a letter to the Federal Trade Commission urging it to expand its focus on file-sharing to protect users from identity theft. At least one company, Tiversa Inc., Cranberry Township, Pa., is offering products to monitor the sharing of files online. And LimeWire and other file-sharing services say they are seeking to limit how files are shared. Many identity-theft experts, however, say the steps are inadequate or confusing.

File-sharing allows users to swap personal files on their hard drives -- from music files and videos to documents and PDFs -- via a peer-to-peer network (often called a P2P). Users download software from one of a number of services that operate on these networks, with names like BearShare, Kazaa, Morpheus and LimeWire. The software then lets users access one of several P2P networks. Once users are connected to the network, they can search for and download copies of files that other users have shared from their hard drives -- even users of other software that use the same network.

P2P networks are often disparaged by critics for enabling users to illegally download copyright material. P2Ps first came to national attention in the late 1990s and early 2000s, when the original version of Napster battled litigation from the music industry. The possibility of identity theft wasn't really on the radar then. But now, the newer applications such as LimeWire -- which unlike Napster don't house a database of files on their own servers, in an attempt to avoid copyright litigation -- have led to a surge in popularity. At any given time, as many as 12 million people world-wide are logged on to P2P networks, according to Tiversa, and 450 million copies of P2P software have been downloaded.

MORE

- [Even the Tech-Savvy Dispute How to Protect Data in File Sharing](#)

With growing use has come growing abuse, say identity-theft experts. But trying to pinpoint when inadvertent disclosure occurred is extremely difficult for law-enforcement agencies, says John Lynch, deputy chief of the Computer Crime and Intellectual Property Section with the U.S. Department of Justice. Identity theft on the Internet can come from several sources, including

leaked files on a P2P network, an online phishing scam or a hacked credit-card company, Mr. Lynch says.

Here's how inadvertent file-sharing often starts: When a user sets up the software for the P2P service, one of the first steps is to create a folder for the files the user will be downloading. Often, the user will place that folder within the computer's "My Documents" folder -- where people also typically put their personal files, including tax returns or other financial documents. Depending on how the user set up the program, all the files in the "my documents" folder or whatever convenient host folder was chosen -- and all of the subfolders -- are then available to others in the network.

Someone who searches a network for, say, "tax return" may be able to download a copy of those personal files off other users' computers. If a user has a company laptop, or has access to company files on their home computer, these files can get leaked, too -- even from the corporate server, Tiversa says.

Even tech-savvy users often don't have a clear understanding of how this works and how to protect select files on their computers, say identity-theft experts. The P2P services' software can be confusing, these experts say, and sometimes users think they have limited the sharing of their files, when in fact, they haven't.

Each service requires different steps. Consumers can try to consult with their software provider, but some are located overseas, identity-theft experts say. And even some experts disagree on the correct steps to use. A recent report from the U.S. Patent and Trademark Office reviewed several online sources that offered instructions on how not to share files on P2P networks, and said most of the instructions were dated and inaccurate.

But for people who do want to use P2Ps, some experts advise reserving a separate computer just for file-sharing.

LimeWire -- one of the most popular P2Ps with an estimated 50 million users -- says confusion is mainly a problem for neophyte users. Mark Gorton, chairman of LimeWire, says the company doesn't track how much inadvertent sharing goes on, but he says the company has been tweaking the software to make it easier for people to avoid inadvertent sharing. For instance, he says that in the latest version of LimeWire, users are no longer able to share their entire C drive. The company has also added a warning icon that tells users how many files they are sharing and will show them a list if they click on it.

Another popular P2P service, BearShare, has had trouble in the past with users inadvertently sharing files. In 2006, BearShare was bought by a unit of [iMesh Inc.](#) as part of a larger settlement between the Recording Industry Association of America and BearShare creator Free Peers Inc. Talmon Marco, president of iMesh, says that the current iteration of BearShare helps to curb inadvertent sharing: Users can swap only media files, such as those for music or movies. Other files, such as PDFs, Word documents or text documents can no longer be shared.

Marty Lafferty, chief executive for the Distributed Computing Industry Association, questions the significance of file-sharing in the total cases of identity theft. Still, he says, the organization is developing best practices for the industry with regards to inadvertent file-sharing. For example, the DCIA is advising its members to rework their programs' warnings to make it clearer when users are sharing files that they might not intend to, says Mr. Lafferty.

Tiversa offers a consumer product that monitors customers' file-sharing, for an annual charge of \$24.95. If a group of files that might contain sensitive information has been designated to be shared, the company will alert the customer and explain how to stop the sharing. Tiversa can also tell the user whether a shared file has been downloaded by another user.

Write to Joseph De Avila at joseph.deavila@wsj.com