

## p2p File Sharing:

Your private information, now available for download.

“A search of one p2p network found at least 2,500 Microsoft Money backup files, which stores the users’ personal financial records, available for download.”

–“File-Sharing Programs and Peer-to-Peer Networks – Privacy and Security Risks”  
2003 Government Reform Committee Report

### What is p2p?

p2p (peer-to-peer) is a method of sharing files over networks (like the Internet) directly between users. The decentralized nature of p2p systems removes the need for central servers, and removes the possibility of centralized control.

### Why is p2p dangerous?

Forgo the fact that p2p software disrupts Internet and email access. Ignore the reality that much of content on p2p networks is pirated and illegal. Are your confidential documents ending up online for everyone to download? A 2003 report by the Government Reform Committee entitled “File-Sharing Programs and Peer-to-Peer Networks – Privacy and Security Risks” states that users of p2p software are inadvertently and unknowingly making their personal information available to others. “A search of one p2p network found at least 2,500 Microsoft Money backup files, which stores the user’s personal financial records, available for download.”

Even companies like Pfizer are not immune, having exposed the personal records of employees when an employee’s spouse installed p2p software on a company-owned laptop.

### How can I prevent my files from leaking?

Because of the decentralized nature of p2p, once a file leaks out, there is no getting it back. So the easiest way to stay secure is not to use p2p software and remove

any that you may have installed.

If you must use p2p software, be careful when installing to decline any automated scan of files to share. Make certain that only files in a specified folder can be shared and turn off any automated scanning options. Additionally, never use p2p software on your PC where sensitive data is stored, such as the machine you use for financial software or human resource record keeping.

### Fighting Back

If you are using p2p, one way to keep aware of what you might be leaking is to run searches on yourself. Create a list of keywords, these can be anything that is meaningful to your business but not so broad that you’re trying to find a needle in a haystack. Use words that are product names, process names, even vendor and supplier names. You might just find that your vendors might be leaking your information.

Another method is to search p2p networks for your own documents. Several companies have sprung up over the past few years specializing in testing the p2p waters for you. For a fee, these companies will maintain searches for keywords and proprietary names that you define. They will then alert you when results are found matching your keywords. If you are interested, contact a BCC Consulting representative for more information, and we can put you in touch with the appropriate vendor.