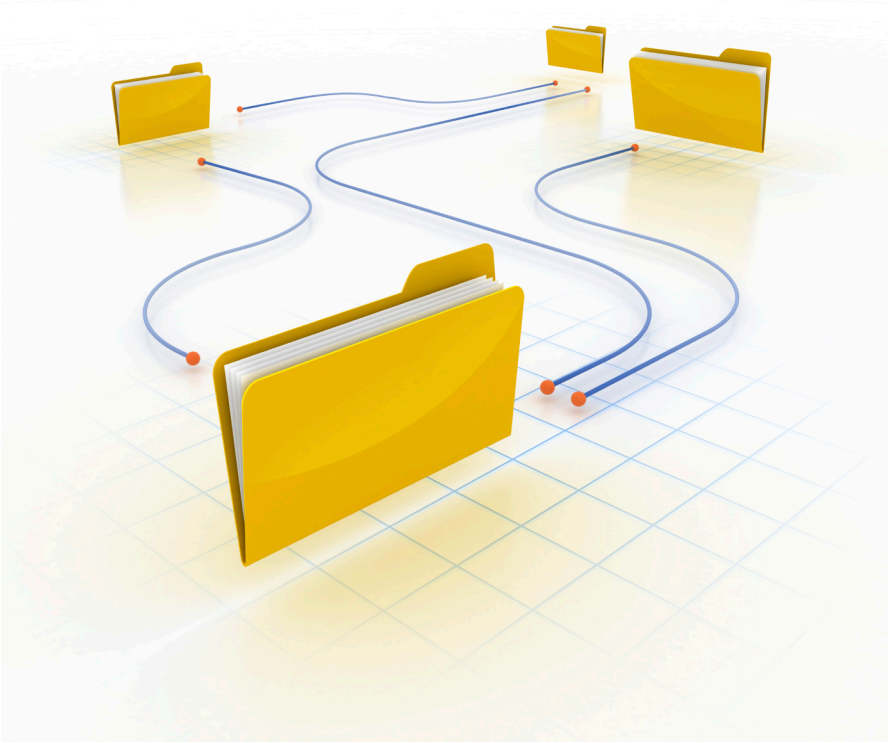
PEER-TO-PEER FILE SHARING:

A GUIDE FOR BUSINESS



FEDERAL TRADE COMMISSION | FTC.GOV

Most businesses collect and store sensitive information about their employees and customers, like Social Security numbers, credit card and account information, and medical and other personal data. Many of them have a legal obligation to protect this information. If it gets into the wrong hands, it could lead to fraud and identity theft. That's why any company that collects and stores sensitive information must consider the security implications of using Peer-to-Peer (P2P) file sharing software and minimize the risks associated with it.

WHAT IS PEER-TO-PEER FILE SHARING SOFTWARE?

Peer-to-Peer (P2P) technology is a way to share music, video and documents, play games, and facilitate online telephone conversations. The technology enables computers using the same or compatible P2P programs to form a network and share digital files directly with other computers on the network. Because virtually anyone can join a P2P network just by installing particular software, millions of computers could be connected at one time. BearShare, LimeWire, KaZaa, eMule, Vuze, uTorrent and BitTorrent are examples of P2P file sharing programs.

When P2P file sharing software is not configured properly, files not intended for sharing may be accessible to anyone on the P2P network. The Federal Trade Commission (FTC), the nation's consumer protection agency, has written this guide to highlight the security problems that can result when organizations allow their employees – and others with access to their networks – to use P2P file sharing software. The guide also notes measures network administrators or security professionals can use to address these problems.

SECURITY RISKS

P2P file sharing programs allow computers to download files and make them available to other users on the network. P2P users can designate the drives and folders from which files can be shared. In turn, other users can download and view *any* files stored in these designated areas.

People who use P2P file sharing software can inadvertently share files. They might accidentally choose to share drives or folders that contain sensitive information, or they could save a private file to a shared drive or folder by mistake, making that private file available to others. In addition, viruses and other malware can change the drives or folders designated for sharing, putting private files at risk. As a result, instead of just sharing music, a user's personal tax returns, private medical records or work documents could end up in general circulation on P2P networks. Once a user on a P2P network downloads someone else's files, the files can't be retrieved or deleted. What's more, files can be shared among computers long after they have been deleted from the original source computer. And if there are security flaws or vulnerabilities in the P2P file sharing software or on an organization's network, the P2P program could open the door to attacks on other computers on the network.

The decision to ban or allow P2P file sharing programs on your organization's network involves a number of factors. For example, what are the types and locations of sensitive information on your network? Which computers have access to files with sensitive information? What security measures are already in place to protect those files?

If your network has sensitive information that isn't necessary to conduct business, your best bet is to delete it – securely and permanently. To help you determine the kinds of files that might be deleted, read *Protecting Personal Information: A Guide for Business* (**www.ftc.gov/infosecurity**).

But if your network has sensitive information that is necessary to conduct business, weigh the benefits of using P2P file sharing programs against the security risks associated with the programs. Is there a business need to share files outside your organization? If so, are there more secure ways for your employees to share files?

Whether you decide to ban P2P file sharing programs on your network or allow them, it's important to create a policy and take the appropriate steps to implement and enforce it. That will reduce the risk that any sensitive information will be shared unintentionally. Among the questions to consider:

- If you decide to **ban** P2P file sharing programs, how will you prevent these programs from being installed and used?
- If you decide to **allow** P2P file sharing programs, how will you protect the sensitive information stored on your organization's network?
- If you allow employees, contractors, or vendors to use non-network computers for remote access, what additional steps will you take to protect sensitive files from being shared through P2P file sharing programs installed on those computers?
- How will you train your employees about the risks of using P2P file sharing programs? Will you impose sanctions if your policies are not followed?
- How will you determine if your policies are effective?

PROTECTING SENSITIVE INFORMATION ON YOUR NETWORK

There's no shortcut when it comes to dealing with P2P file sharing security concerns. Regardless of whether you choose to allow P2P file sharing programs, take these steps to ensure that the sensitive information on your network is secure:

- Delete sensitive information you don't need, and restrict where files with sensitive information can be saved.
- Minimize or eliminate the use of P2P file sharing programs on computers used to store or access sensitive information.
- Use appropriate file-naming conventions.
- Monitor your network to detect unapproved P2P file sharing programs.
- Block traffic associated with unapproved P2P file sharing programs at the network perimeter or network firewalls.
- Train employees and others who access your network about the security risks inherent in using P2P file sharing programs.

IF YOU DECIDE TO BAN THE USE OF P2P FILE SHARING PROGRAMS...

A decision to ban P2P file sharing programs altogether requires policies and procedures to prevent these programs from being installed on computers on your network, and to detect any P2P programs that have been installed – and block traffic associated with them.

To prevent P2P file sharing programs from being installed:

- Use administrative security controls to block access from your network to sites used to download P2P file sharing programs. You can filter sites based on URL, IP address, filename and content, or you can use commercial products designed to do the job. The controls also should block access to sites that offer free software downloads; these sites often are sources of P2P file sharing programs.
- Use administrative security controls to prevent employees from installing unapproved programs on your organization's computers.

To detect P2P file sharing programs already installed – and block traffic associated with them:

- Use scanning tools on individual computers and networks often to find P2P file sharing programs and remove them. Commercially available scanning tools can identify many P2P programs.

- Install tools that allow network administrators to restrict, monitor and otherwise manage access to P2P file sharing networks from your corporate network, including intrusion detection systems (IDS), intrusion prevention systems (IPS) or firewalls that detect P2P traffic and restrict appropriate inbound and outbound connections to the Internet. Configuring these tools may require research because different P2P file sharing programs use different protocols. Commercial hardware and software providers may be helpful.
- Install tools that create records of file transfers based on the configuration of IDS, IPS and firewalls to detect and control P2P traffic.
- Use network monitoring tools and techniques like flow reconstruction to identify whether your network has P2P traffic and to determine the nature – and maybe the names and contents – of files that have been sent to and from your network using P2P file sharing programs.
- Review records and activity logs on your network to identify traffic volume spikes that may indicate big files or a large number of small files are being shared.
- Install data loss prevention tools that inspect files flowing from your network to determine whether they contain certain types of sensitive information, like Social Security numbers. Regularly review the records these tools create to determine whether sensitive information is being exported.

To protect sensitive information:

- Restrict the locations to which work files containing sensitive information can be saved or copied. For example, you can create designated, well-defended network servers to house these files or use a file management program. These kinds of tools and techniques isolate sensitive information and may limit the extent to which P2P file sharing programs need to be banned.
- If possible, use application-level encryption to protect the information in your files. This type of encryption can help protect files that are shared inadvertently on P2P networks. If you use encryption, keep the passwords and encryption keys safe: make sure they are not available in drives or folders designated for sharing.
- Use file-naming conventions that are less likely to disclose the types of information a file contains. For example, it's easy to spot terms like "ssn," "tax," or "medical" within a filename.
- If you find an unauthorized P2P program on your network, monitor it for sensitive information, either directly or by using a third-party service provider. Because search terms can be viewed by others on P2P networks, be careful about the terms you use. Some search terms (such as those that include "ssn") may increase the risk to sensitive information, while others (such as company or product name) likely will not. To help manage these risks, consult a security professional.

IF YOU DECIDE TO ALLOW P2P FILE SHARING PROGRAMS...

If you decide to allow P2P file sharing programs on your organization's computers, it's smart to control their use to try to prevent unauthorized file sharing.

First, review various P2P file sharing programs, and select one that is appropriate for your organization. Next, permit only the approved program and configuration.

To control the installation of approved P2P file sharing programs:

- Provide the approved program directly to authorized users from an internal server rather than from a public download site. That can reduce the chance that the program will contain viruses or other malware.

To control the use of approved P2P file sharing programs:

- Update the approved P2P program often from an authorized and verified source to incorporate the latest security patches.
- Block outbound traffic through the approved P2P file sharing program to prevent sharing the types of files that most often contain sensitive information, including files that have the suffixes .doc, .docx, .xls, .xlsx, .mda, .mdb, .txt and .pdf. If these are the types of files your business needs to share, consider using a program other than a P2P file sharing program.
- Use the tools and techniques already cited to detect unapproved P2P file sharing programs (or unauthorized versions of approved P2P programs) on your network and to block traffic associated with them.

To protect sensitive information:

- Restrict the locations to which work files containing sensitive information can be saved or copied. For example, you can create designated, well-defended network servers to house these files or use a file management program. These kinds of tools and techniques isolate sensitive information and may limit the extent to which P2P file sharing programs need to be banned.
- If possible, use application-level encryption to protect the information in your files. This type of encryption can help protect files that are shared inadvertently on P2P networks. If you use encryption, keep the passwords and encryption keys safe: make sure they are not available in drives or folders designated for sharing.
- Use file-naming conventions that are less likely to disclose the types of information a file contains. For example, it's easy to spot terms like "ssn," "tax," or "medical" within a filename.
- Monitor P2P networks for sensitive information, either directly or by using a third-party service provider. Because search terms can be viewed by others on P2P networks, be careful about the terms you use. Some search terms (such as those that include "ssn") may increase the risk to sensitive information, while others (such as company or product name) likely will not. To help manage these risks, consult a security professional.

IF YOU ALLOW REMOTE ACCESS TO YOUR NETWORK...

Whether you ban P2P file sharing programs or allow them, additional measures may be appropriate when employees, contractors, vendors, service providers or others can access sensitive information on your network remotely.

To protect sensitive information while allowing remote access:

- Provide dedicated company computers to employees who access your network remotely, rather than allowing them to use their own personal computers. The computers you provide should have the same security measures and protections you use at work to prevent, detect and block unauthorized file sharing to P2P networks.
- Require remote access to proceed only through secure connections to your organization's network, like Virtual Private Network (VPN) software or Secure Sockets Layer (SSL). This is appropriate for employees who telework – or for customers or suppliers who need regular access to your system.
- Restrict the locations to which work files containing sensitive information can be saved or copied, and permit remote users to access, use or modify the files – but not to download them. If you allow people to use their personal computers to download files from your organization's network, consider requiring them to securely delete your files from their computers when they are not using the files.
- Exercise due diligence to ensure that customers, suppliers, contractors, vendors, service providers and other third parties that access your network use appropriate security policies and procedures to address risks associated with P2P file sharing programs.

TRAINING EMPLOYEES AND OTHERS ABOUT P2P FILE SHARING PROGRAMS

These days, keeping sensitive information secure really is every employee's responsibility. Regardless of whether you ban the use of P2P file sharing programs or allow it, everyone who has access to sensitive information on your network should be trained about the security risks associated with these programs. If you allow the use of P2P file sharing programs, effective training should demonstrate how to restrict drives or folders to limit what other P2P users can view. It should emphasize the importance of keeping files with sensitive information out of P2P shared drives and folders and minimizing the amount of sensitive information on computers using P2P file sharing programs. For more information, read *P2P File-Sharing: Evaluate the Risks* (**www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt128.shtm**). Consider what sanctions might be appropriate if your organization's policies about using P2P file sharing programs are not followed or if files containing sensitive information are shared on P2P networks contrary to those policies. Training your employees about securing sensitive information sends the message that your organization believes in keeping personal information private.

EVALUATING YOUR POLICIES

Evaluate your security measures regularly to be sure they are doing the job. Circumstances change, equipment and software become outdated, and people make mistakes. As a result, effective security is dynamic, and requires monitoring and updating.

ADDITIONAL RESOURCES

- **www.ftc.gov/infosecurity**
- **www.OnGuardOnline.gov**
- **www.sans.org/top20**
- **www.us-cert.gov**

The FTC works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them. To file a complaint or to get free information on consumer issues, visit **ftc.gov** or call toll-free 1–877–FTC-HELP (1–877–382–4357); TTY: 1–866–653–4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.