fasthosts ProActive

Oops-proofing your security

Shared files

Welcome back to our "Avoiding Human Error" blog series. To recap, so far we have covered keeping your eyes peeled for phishing attacks and the importance of strong passwords. Today, we shift our focus to managing shared files.

Shared files are a staple in collaborative environments, but they also pose significant security risks if not handled correctly. Let's dive into how to protect your shared files from human error-induced threats.

Understanding the risks of shared files

When files are shared, especially in a digital workspace, they can become vulnerable to unauthorised access, data breaches, and malicious attacks. Common risks include:

- Unauthorised access – Without proper controls, anyone with the link or basic access can view, edit, or delete sensitive information.
- Data leaks – Shared files can be copied, forwarded, or downloaded by unauthorised users, leading to unintended data exposure.
- Malware infections – Files shared without proper scanning can carry malicious software, compromising the entire network.
- Lost data – File sharing increases the risk of data loss through accidental deletion, overwriting, or corruption.

Common mistakes in managing shared files

To avoid these risks, it's essential to recognise common mistakes people make:

- Too much access – Granting excessive access rights to users who do not need them
- Lack of access monitoring – Failing to track who accesses or modifies shared files
- Poor organisation – Storing shared files in disorganised, hard-to-find locations
- Inadequate training – Not educating users on proper file-sharing protocols and security practices

Best practices for managing access to shared files

- **Implement the principle of least privilege**

Only grant access to the minimum level of information necessary for users to perform their duties. This minimises the risk of unauthorised access and potential data breaches.

- **Use strong authentication methods**

Enhance security by requiring robust authentication measures, such as:

1. Two-factor authentication (2FA) – Adds an extra layer of security by requiring a second form of verification
2. Single sign-on (SSO) – Streamlines the login process while maintaining security across multiple platforms

- **Regularly monitor and audit access**

Keep an eye on who's accessing your shared files and what changes they're making. Regular audits can help identify suspicious activity and keep up compliance with security policies.

- **Educate your team on best practices**

Regular training sessions can help your team understand the importance of secure file sharing. Key topics to cover include:

1. Identifying phishing attempts – Teaching users to recognise and avoid phishing scams that target shared files
2. Secure sharing methods – Instructing on how to use secure sharing options and avoiding insecure channels, like email attachments
3. Version control – Educate on the importance of proper version control, which tracks and manages changes to files and keeps a history of changes, showing who made them and when. This helps you recover previous versions if something goes wrong, preventing data loss.

- **Utilise advanced security tools**

Several tools can help manage and secure shared files effectively:

1. File encryption – Encrypt files before sharing to protect data from unauthorised access. This can be done using built-in tools like BitLocker for Windows, FileVault for macOS, or third-party software such as VeraCrypt and 7-Zip.
2. Cloud storage services – Use reputable cloud services with robust security features and regular backups, like us! Your data is always in safe hands, so why risk it elsewhere? Listen to episode 18 of our podcast, 'Spill the IT', to hear what else we could do for your business.
3. Access management software – Use software to manage user permissions and monitor access

What to do if a shared file is compromised

If you suspect that a shared file has been compromised, take immediate action:

- Revoke access – Immediately remove access for any users who no longer need it.
- Conduct an investigation – Determine how the compromise occurred and which files were affected.
- Notify relevant parties – Inform your IT department and any affected users about the breach.
- Review and update security policies – Enhance your security measures to prevent future incidents.

Managing access to shared files is a critical aspect of maintaining your organisation's security. By implementing these strategies, you can reduce the risk of human error, safeguard your data, and ensure that your collaborative efforts remain secure. In a world full of data, sharing is only caring when it's secure.

Stay tuned for the next post in our "Avoiding Human Error" series, where we'll continue to explore essential tips to keep your data safe and secure.

If you have any questions about security, or think your infrastructure could benefit from a Managed Service Provider like ProActive, get in touch. You can call us on 0333 111 2000 or book a meeting at a time that suits you.