fasthosts ProActive

Oops-proofing your security

Shared calendars

Welcome back to our "Avoiding Human Error" blog series. To recap, so far we've covered phishing attacks, the importance of strong password and staying safe while sharing files. Today, we shift our focus to managing shared calendars.

Shared calendars 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 calendars from human error-induced threats.

Understanding the risks of shared calendars

When calendars are shared, especially in a digital workspace, they can become vulnerable to unauthorised access, data breaches, and malicious attacks.

1. Unauthorised access

- Internal threats – Employees or internal stakeholders who shouldn't have access might view or edit sensitive calendar entries.
- External threats – If the calendar is shared too broadly, or accidently shared with clients or partners, external parties could gain access to confidential information.

2. Data leakage

- Meeting details – Information about meetings, including attendees, locations, and topics, could be exposed leading to potential breaches of confidentiality.
- Event descriptions – Descriptions of calendar events might contain sensitive information about projects, deadlines, or business strategies.

3. Phishing attacks

- Malicious invites – Attackers could send malicious calendar invites that contain phishing links, leading to compromised accounts or systems.

4. Operational disruption

- Unauthorised changes – Changes to calendar events or accidental deletion by unauthorised users can cause confusion and scheduling conflicts, leading to business disruption.

5. Privacy concerns

- Personal information – Shared calendars can inadvertently expose personal information about employees, such as medical appointments, or personal meetings.

Common human errors in managing shared calendars

- Too much access – Granting excessive access rights to users who don't need them and not updating permissions frequently
- Lack of access monitoring – Failing to track who accesses or modifies the calendar
- Weak authentication practices – Sharing login credentials and using weak passwords
- Poor organisation – Having disorganised calendar entries that are hard to find and manage
- Inadequate training – Not educating users on proper calendar-sharing protocols and security practices

What to do

- Implement and monitor proper access controls – Only grant access to those who need it and monitor and update this regularly
- Enhance authentication practices – Set up a two-factor authentication system (2FA) and ensure passwords are complex and changed regularly
- Educate employees – Teach employees about phishing, secure sharing practices, and calendar management
- Maintain software updates – Ensure all applications are up-to-date with the latest security patches

Immediate actions if your shared calendar is compromised

- If you suspect that a shared calendar has been compromised, take these immediate actions:
- Revoke access – Immediately remove access for any users who no longer need it
- Conduct an investigation – Determine how the compromise occurred and which calendar events 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

Ensuring secure access to shared calendars is essential for maintaining your organisation's overall security. By adopting these strategies, you can minimise the risk of human error, protect your data, and keep your collaborative activities safe. In today's data-driven world, sharing responsibly means sharing securely.

If you need advice on keeping your infrastructure secure, or you'd like to chat about managing your IT, get in touch! Give us a call on 0333 111 2000 or book a meeting at a time that suits you.