61%

Of Ponemon survey respondents* reported accidentally forwarding files or documents to individuals not authorized to see them.

3 Ways to Make Content Sharing Easy & Secure

If you've ever sent an email to an unintended recipient, you're not alone. In a research study conducted by Ponemon Institute, more than six out of ten people report having accidentally forwarded files to individuals not authorized to see them.

With a single click, your file is out there, for anyone and everyone to access, copy and pass along. If you work in a regulated industry, or deal with IP-centric information and sensitive data, your mistake could cost your firm thousands or millions of dollars in fines and loss of IP. Not to mention bad press and investor angst.

Here are three tips to help you make content sharing easy and secure.

#1: Use the appropriate technology for sharing sensitive information

Email is great, but it is really designed for communication, not file transfer! It's really only appropriate for certain business processes, but in many organizations, it's the default tool for all business processes. The gating factor on email use is often the sharing of large files – and, in many cases, workers are turning to free file-sharing services to do this.

If your company has any security or regulatory concerns, it's likely you have access to secure communications and file-sharing technologies such as encrypted email, or secure file-sharing applications. These technologies are better-suited to support secure file transfer. Look into ways to use them appropriately and you'll avoid making inadvertent email mistakes.

#2: Don't bring your personal productivity and content collaboration tools to work

Consumer-grade productivity and collaboration tools are designed to be used by consumers, not as ad-hoc solutions within the enterprise. They lack the security and oversight that are necessary features of commercial file-sharing and collaboration tools.

Keep in mind, there's no such thing as "free," when it comes to security. Free cloud file-sharing services don't provide the security and auditability that is so important for managing files within regulated environments, which could lead to very costly mistakes.

#3: Maintain control of your content, wherever it goes

With an increasingly mobile workforce, it's important to keep in mind that the security, mobility and collaboration are inextricably linked. Mobile workers need control and oversight over the documents they share beyond their firewall, as they operate from mobile platforms, beyond the reach of corporate security infrastructure. It's important that security provisions be embedded into the content you are sharing, so you can maintain control over documents even when they are outside your organization's IT infrastructure.

Document collaboration technologies that provide integrated information rights management (IRM) capabilities can deliver this kind of control – even when the documents are downloaded and taken offline.

If you keep these three simple tips in mind, and use tools that meet the rigor of regulatory compliance and enterprise security, while being flexible enough to support your daily activities, you can keep your creative mojo going, without creating a security nightmare for your company.

Find out more about Intralinks

Intralinks is here to help. Intralinks VIA is the secure collaboration solution that helps you:

- Manage vendor relationships efficiently
- Flawlessly plan and execute campaigns
- Securely share digital assets
- Track your budget, with appropriate permissions
- Distribute sales enablement tools
- Keep translations on track, with version control

intralinks.com

Reach your closest Intralinks office:
intralinks.com/mylocation

10109