# Proofpoint highlights top 10 tips for businesses and their staff to avoid email disasters

Submitted by: Six Degrees Limited
Thursday, 4 December 2008

---

Oxford, UK – December 3rd 2008 – 2008 has been a year of high profile and embarrassing email data loss blunders from Government ministers, utilities companies and even the Student Union. Just last month, Alistair Campbell found himself at the centre of a row after an obscene email outburst aimed at BBC journalists(1).

According to Proofpoint, an email security specialist, email is already the primary outlet of data leakage and we are only just seeing the tip of the iceberg. Identification of data leakage, either deliberate or unintentional, will continue to grow.

A recent Forrester Research study(2) revealed that 66 per cent of UK companies are “concerned” or “very concerned” about ensuring that email cannot be used to disseminate company trade secrets or valuable intellectual property. And 63 per cent of UK companies are “concerned” or “very concerned” about protecting the confidentiality of personal identity and financial information in outbound email.

To help companies protect both themselves and their staff from data loss mishaps, Proofpoint has come up with following “Safer Email” top tips for businesses and employees:

Email tips for businesses

1.Select your filtering solution wisely. Insist on a gateway-based solution that’s easy to use, highly accurate, quick to deploy and scalable.

2.Act fast to minimise loss. Implement effective processes will help identify, track and resolve any rogue emails through a variety of options including quarantine, deletion, and re-routing back to the original sender for clarification.

3.Focus on your data. Know the value as there are clear differences between a customer’s private information (National Insurance numbers; bank account numbers etc) and company sensitive content (financial accounts; sensitive memos and press releases; blueprints etc)

4.Encrypt. Businesses should ensure that they have an enforcement mechanism in place to prevent sensitive information falling into the wrong hands.

5.Review & Audit. Continually review the information leaving your organisation and make sure it adheres to your outbound security policies. Educate users and continually assessing effectiveness of the policies, updating where necessary.

Email tips for employees

1.Expect to be unlucky! Don’t rely on luck, take care to follow the company guidelines and do your

best to be practical. If you are not sure about the value of information – ask. It is always better safe than sorry.

2.Manage your email accounts.  A good rule of thumb for the average email user is to keep a minimum of three email accounts. Your work account should be used exclusively for work-related conversations. Your second email account should be used for personal conversations and contacts, and your third email account should be used as a general catch-all for less secure interactions e.g. signing up for newsletters, entering online competitions etc.

3.Avoid fraudulent email.  Never respond to an email stating that you've won the lottery.  If it looks too good to be true, it probably is.

4.Insure your financial information via email.  Banks and online stores provide, almost without exception, a secured section on their website where you can input your personal and financial information. They do this precisely because email, no matter how well protected, is more easily hacked than well secured sites. Using your credit card wisely insures you against theft and fraud.

5.Look at your policy. There's an old saying that it's better to seek forgiveness than permission. Not in the case of your employer's sensitive information.  If in doubt, don't send it.  Make sure you are up to date on your employer's email policy, especially when it comes to sensitive or confidential documents.

About Proofpoint
Proofpoint secures and improves enterprize email infrastructure with solutions for email archiving, encryption and data loss prevention.  Proofpoint solutions defend against spam and viruses, prevent leaks of confidential and private information, encrypt sensitive emails and archive messages for retention, e-discovery and easier mailbox management.  Proofpoint solutions can be deployed on-premises (appliance); on-demand (SaaS) or in a hybrid architecture for maximum flexibility and scalability.  For more information, visit www.proofpoint.com

1. http://www.thisislondon.co.uk/news/article-16446130-details/Labour+email+blunder/article.do
2.Forrester Consulting fielded an online survey of email decision makers from companies with 1,000 + employees including 301 US, 32 UK, 30 German, 31 French and 30 Australian companies.  The full report is available at: www.proofpoint.com/outbound

For additional information:

Six Degrees PR
+ 44 (0) 1628 480280
proofpoint@sixdegreespr.com