proofpoint

October 28, 2010

Proofpoint Identifies Top 10 Email Horror Stories of 2010

Email gaffes, data loss, botnets and worms continue to plague companies and cost millions

Sunnyvale, Calif. – October 28, 2010 – Email continues to be a major channel for data loss blunders in 2010, according to Proofpoint, Inc., the leading provider of SaaS email security, email archiving and data loss prevention solutions. Just in time for Halloween, Proofpoint has identified some of the most frightening email-related incidents in 2010 that were not only embarrassing to individuals and their companies, but in some cases cost hundreds of thousands of dollars.

In no particular order, Proofpoint highlights some of this year's mishaps below:

eDiscovery nightmare: Investment firm fined for not saving emails
Brokerage firm Piper Jaffray & Co. was fined $700,000 by FINRA for alleged "shoddy email practices." The law firm apparently failed to save over 4 million emails between 2002 and 2008. The firm attributed the failure to disclose "intermittent trouble with email retention and retrieval during the relevant period."

Rise of the zombies: Millions of PCs hijacked, Stuxnet botnet targets real-world infrastructure
Microsoft researchers revealed that millions of computers worldwide (more than 2 million of them in the US) had been compromised and made part of botnets in just the first 6 months of the year. In October, Microsoft issued its largest ever list of fixes for flaws in Windows, Internet Explorer and a range of other software. This included a security patch to plug a hole exploited by Stuxnet, the first-known worm designed to target real-world infrastructure such as power stations, water plants and industrial units.

Indecent exposure: Aussie banker (almost) gets fired for televised email blunder
No place is safe, not even your desk. A banker at Macquarie Private Wealth in Sydney opened not-safe-for-work photos of a model, unaware a colleague behind him was doing a live television interview about the Australian economy.

Creepy overshare: Security Breach at Shell Reveals Personal Employee Information
The situation is particularly difficult for the infamous oil corporation- the database of names and personal contact details of 170,000 employees had been e-mailed to several non-governmental organizations, including Greenpeace, Friends of Earth and Shell Guilty.

Giant worm attacks: 'Here You Have' marks return of old school threats
A mass-mailing worm masked as a PDF marked the return of an old spam tactic by spreading via infected computers and email address books. To make matters worse, it also had an Autorun feature that spread the worm via remote machines, mapped network drives, and removable media. Companies across North America were widely affected by the worm.

Style Weekly reporter gets the axe
A reporter at Style Weekly thought he was sending an email to his editor on Wednesday, in which he called a blind motivational speaker a "blind [expletive]." However, it turns out the reporter sent the note to the blind man's PR person. This is a good reminder to always check the to:, cc:, and bcc: fields… and don't put anything in email that you wouldn't want the whole world to see.

Credit card chaos: Retailer's email confirmations expose private financial information
After a probe by PC Pro Magazine, it was discovered that UK retailer Argos was sending out the credit card numbers of their online customers in emails confirming purchases. What's worse, the emails also included a link that contains the recipient's name, address and credit card details, which could be stored in the browser's history unbeknownst to the customer.

You've been accepted… for a discounted laptop!
UCAS, the UK organization responsible for managing applications for higher education courses, sent a misleading email to students anxiously waiting for their A-level results, with the subject line, "you have been accepted." Unfortunately, it was not university they were accepted to, but rather a discounted HP laptop.

Silence of the spams: Producer almost loses tickets to the Oscars
In an overzealous moment, a film producer spammed Academy of Motion Picture Arts and Sciences members with a message that practically begged voting members to support his film over its Best Picture competition. Unfortunately, the

Academy explicitly bans directly campaigning to voters, and the producer had to immediately send an apology email in order to attend the award ceremony.

Prime suspect: Data loss affects nearly one-third of enterprises, email the main culprit
Proofpoint's 2010 research on outbound email and data loss risks showed that enterprises continue to suffer from data loss at a shocking rate. The most common source of exposures of confidential or proprietary information remained email, with 35% of large companies investigating an email-based breach in the previous 12 months. Lost and stolen mobile devices and social media channels were also exposed as serious sources of risk.

To learn more about email security and how to minimize email risks, visit http://www.proofpoint.com.

About Proofpoint, Inc.
Proofpoint focuses on the art and science of cloud-based email security, eDiscovery and compliance solutions. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against spam and viruses, safeguard privacy, encrypt sensitive information, and archive messages for easier management and discovery. Proofpoint's enterprise email solutions mitigate the challenges and amplify the benefits of enterprise messaging. Learn more at www.proofpoint.com.

# # #