proofpoint

October 26, 2009

"Hallowee-mail Horrors": Proofpoint Identifies Top 10 Terrifying Email Blunders of 2009

Recession Fears, Banking Scams, and Healthcare Debate Create Frightening Fiascos

SUNNYVALE, Calif. – October 26, 2009 –It is no surprise that the biggest email horror stories this year capitalized on consumer and business fears during the height of the recession, according to Proofpoint (http://www.proofpoint.com), the leading provider of unified email security, archiving and data loss prevention solutions. With Halloween creeping around the corner, Proofpoint has identified some of the scarier email incidents of 2009 that not only haunted individuals, but businesses as well.

These blunders, attacks and mishaps have wreaked havoc on email systems and caused financial stress for consumers, corporate executives, politicians, and, of course, email administrators.

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

1.) Trojan Horse Empties Bank Accounts
In September, it was reported that a banking Trojan horse, dubbed URLZone, had thwarted fraud detection systems, to enable software to actually steal money while users are logged in to their accounts and display a fake balance. Victims' computers were infected either by clicking on a malicious link in an email or visiting a Website that has been compromised with hidden malware. The Trojan also kept a log of the victim's bank account login credentials, took screenshots, and snooped on the user's other Web accounts, such as PayPal, Facebook, and Gmail.

Article here »

2.) FBI Forgery
The wife of FBI Director Robert Mueller banned him from online banking after he nearly fell for a phishing scam. Mueller received a seemingly legitimate email from what he thought was his bank, which prompted him to verify some information. He even went as far as filling out some of his personal information before realizing it might not be a great idea. He said he barely caught himself in time before falling victim to the scam. As a result, he changed his passwords and tried to pass the incident off to his wife as a "teachable moment." However, that did not stop Mrs. Mueller from sanctioning Mr. Mueller's online activities.

Article here »

3.) White House Adopts Spammer Tactics
In August, the White House emailed thousands of messages to Americans detailing its stance on the contentious issue of healthcare reform from an email account created to gather and dispel rumors, but some recipients claimed the messages were unsolicited. The White House acknowledged the unsolicited email and blamed third-party groups for the mass email.

Unfortunately, the damage was already done. Critics questioned whether the White House used address-gathering tactics similar to those employed by spammers.

Article here »

4.) Hotmail Phishing
Most recently, more than 10,000 Hotmail accounts were compromised in October and passwords were posted on several Websites where developers typically share programming code. News site Neowin reported it had seen part of the list, which has since been removed, and notified Microsoft of the issue. In this phishing scam, hackers sent out legitimate-looking emails under the letterhead of banks, eBay and other institutions, telling consumers they needed to reset online passwords to their Web sites for security purposes.

Article here »

It seems that many of the affected account holders could have used a password reset. Security researchers with copies of the exposed passwords reported that "123456" was the most commonly used among them.

Article here »

5.) Start-up Suicide
Back in September, social media advertising and applications start-up RockYou, sent out a mass email to their customers and associates announcing their new site redesign, but instead of using BCC:, they displayed the entire mailing list of over 200 email addresses in the CC: field. Not surprisingly, many of those addresses ended up on a spammer's list.

Two months later, the start-up sent out another mass email using a mailing list. Unfortunately, the email asked contractors to provide information for their W9 tax forms. This resulted in people inadvertently sending personal information to the entire mailing list.

Email may not be as trendy as social networks, but companies still need to use both properly.

Article here »

6.) Judge Orders Gmail Account Deactivated
In August, Wyoming-based Rocky Mountain Bank mistakenly sent names, addresses, social security numbers and loan information of more than 1,300 customers to a Gmail address. When the bank realized the problem, it sent a message to that same address asking the recipient to contact the bank and destroy the file without opening it.

No one responded, so the bank contacted Google to ask for information about the account holder. U.S. District Court Judge James Ware in the northern district of California ordered Google to deactivate the email account and also disclose the Gmail account holder's identity and contact information. The Gmail user hasn't been accused of any wrongdoing, but someone at the Bank should be a little more careful when typing in the TO: field in an email.

Article here »

7.) Payroll Panic

Payroll processor PayChoice was the victim of a Website breach in which customers received targeted emails purporting to be from the company, but were designed to trick people into downloading malware. Workers received emails that directed them to download a browser plug-in or visit a Website to continue accessing the Onlineemployer.com PayChoice portal.

Clients were notified within hours and the site was shut down. It was later learned that the emails were sent from a Yahoo! email account and the links were hosted from servers in Poland.

Article here »

8.) UK Tax Terror

Britain's tax authority, HM Revenue & Customs, issued a warning about a rash of scam emails that used convincing (but fake) government email address in an attempt to lure recipients into divulging their personal information to receive a tax refund. The scam messages claimed that recipients were entitled to a tax refund and asked for bank or credit card details, so that the fictitious refund could be paid out.

Like most legitimate businesses and government organizations, the HMRC stressed that it would not inform citizens of a tax rebate via email, nor would it invite them to complete an online form to receive a tax rebate.

Article here »

9.) Death, Taxes and Phish

In September, a fake email notice that purports to come from the Internal Revenue Service continued to make the rounds, widely ramping up attacks against businesses and individuals. The attacks were concealed in a bogus email containing a subject line of "Notice of Underreported Income," according to US-CERT. The emails contained a link or an attachment that, if opened, will infect users with the Zbot/Zeus Trojan, a nasty credentials-stealing program that seeks to compromise banking login information.

Proofpoint reports that these phishing emails continued to be widely circulated as the October 15th deadline for filing extended tax returns approached.

Article here »

10.) UCSD Fake-Out

28,000 students were turned away from UC San Diego in one of the toughest college entrance seasons on record after a particularly cruel twist in the perils of instant communications. All 46,000 students in the entire freshman applicant pool received the same misfired message of acceptance, which could have led to the largest freshman class at any university globally.

The 18,000 students who were actually accepted breathed a sigh of relief. Unfortunately, the rest of the applicant pool had to march on in the grueling college application process.

Article here »

To learn how to avoid these security issues and more, visit http://www.proofpoint.com.

About Proofpoint, Inc.
Proofpoint secures and improves enterprise email infrastructure with solutions for email security, 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-demand (SaaS) on-premises (appliance), or in a hybrid architecture for maximum flexibility and scalability. For more information, please visit http://www.proofpoint.com.

# # #