



## **Latest Email Attacks Prey on People's Familiarity with the Web**

*Scammers continue to expose the weakest link in email security by spoofing trusted brands in order to generate clicks and steal identities*

**Rohnert Park, Calif. – June 28, 2010** – Email security companies and their customers continue to battle the weakest link in email security as the latest email attacks prey on people's trust in popular brands. These new attacks have the look and feel of trusted brands, increasing the likelihood that recipients will respond. Once easily identified as scams by way of poor design, multiple misspellings and grammatical errors, today's spam and phishing attacks are so sophisticated and detailed that even experienced computer users fall victim to the scams.

In the past year, [Red Condor](#) has blocked and [warned](#) the public about phishing, spear phishing and blended threat campaigns spoofing eBay, Adobe, YouTube, Amazon, Apple, BlueMountain eCards, craigslist, Facebook and Twitter--among other popular brands.

In addition to the installation of malware on unsuspecting users' computers, these campaigns can have more insidious results, such as violation of social trust. For example, a [Adobe malware campaign](#), a fake security alert that targeted users of Adobe Software, also spoofed email addresses of managers and other employees within a bogus email thread. This technique made the email appear to come from a trusted person in the organization, thus increasing the likelihood the recipient would follow the instructions in the email.

["Today's threats](#) are more sophisticated, with the intent to steal personal and corporate information by any means necessary," said Dr. Tom Steding, CEO of Red Condor and co-author of *Built on Trust*. "When people see emails that appear to come from Apple, eBay, Facebook or other brands they know and trust, they tend to react. Even more damaging is the erosion of trust that can result from a campaign that spoofs the email addresses of people in the users' professional network or social circle."

The good news is that people can protect themselves if these new nefarious campaigns make it into their personal or work inboxes. Red Condor recommends the following:

- **Trust no one:** Today's scams are coming from trusted brands and in some cases from hijacked email addresses. Before you click on anything, read the entire email.
- **When in doubt, throw it out:** If the email is important, the sender will resend it or follow up in another way.
- **Ask your IT expert:** For a consumer, call your Internet Service Provider and for businesses, ask your IT staff if there are new spam campaigns or threats making their way around the Internet.
- **Make security the top priority:** Frequently change passwords and make sure your security solutions are up-to-date. Create passwords with a combination of numbers, letters and characters.

Among the many spam, virus and phishing campaigns blocked and reported by Red Condor in the past year are the following:

- **June 9, 2010** - [Red Condor](#) issues warning of new, highly sophisticated email malware threat that spoofed YouTube and used a redirect on a compromised website to a common Canadian Pharmacy web site to distribute malicious PDFs.
- **May 4, 2010** - Red Condor issues warning for malware threat crafted to appear as an email thread discussing vulnerabilities in Adobe software.
- **April 2, 2010** – Red Condor stops spear phishing attack spoofing a security warning from AT&T Internet Services.
- **April 1, 2010** – Red Condor warns public of fake eBay security alert recommending eBay users download “security shield” that installs a Trojan virus.
- **March 12, 2010** – Red Condor blocks phishing campaign targeting users of ADP's RUN online payroll processing services.
- **January 7, 2010** – Red Condor blocks aggressive spear phishing email campaign that includes link to a web site that appears to be a Microsoft® Office Outlook® Web Access page.
- **December 8, 2009** – Red Condor captures an e-Card spam campaign that appears to come from American Greetings' BlueMountain.com.
- **December 2, 2009** – Red Condor issues warning about spam campaign claiming to be from the Centers for Disease Control and Prevention.
- **November 29, 2009** - Red Condor issues warning about a phishing ploy and malware threat posed as an update to Macromedia Flash Player.
- **October 28, 2009** – Red Condor identifies blended email threat posing as a message from Facebook administrators. Users prompted to download “updatetool.exe,” a Zbot Trojan variant.

- **August 13, 2009** – Red Condor issues warning about virus embedded in an email that appears to be a response to a craigslist advertisement.
- **August 4, 2009** – Red Condor issues warning about email security scams preying on people looking for employment. Emails include fake jobs from reputable companies such as Pepsi and Starbucks, or messages from job sites such as CareerBuilder or Monster.com.
- **May 22, 2009** – Red Condor warn of Twitter invitation virus that includes the subject line, “Your friend invited you to twitter!”

“While most of the anti-spam solutions on the market do a decent job stopping the widespread spam campaigns, they fail to block targeted, sophisticated campaigns that are spoofing major brands,” added Steding.

The company’s Zero Minute Defense™ System allows Red Condor to respond in real-time to new spam, viruses and phishing attacks. Other anti-spam products rely on statistical methods, Bayesian filters and trust metrics to react to new threats. These traditional methods are not designed to recognize the threats embedded in well-written, well-designed messages used by today’s scammers. Red Condor’s multi-layered defenses and proprietary and precision filtering techniques use between 30 and 60,000 rules at any one time to ensure accuracy and speed of response. In addition, Red Condor’s email security experts monitor incoming spam around the clock for changes in spammers’ tactics, allowing the company to quickly analyze and adapt to new threats.

### **About Red Condor**

Red Condor is revolutionizing spam fighting with its next-generation technology. Red Condor’s highly accurate email filter, [hybrid](#) architecture Vx Technology™, and fully [managed appliances](#) lead to a dramatic reduction in the cost of owning a premium [spam filter](#). With solutions for [small businesses](#), as well as ISPs with millions of email inboxes, Red Condor has a cost-effective, timesaving solution that is rapidly gaining market share. The system’s design has built-in zero tolerance for lost email, and a near zero false positive rate while achieving long-term spam block rates greater than 99%. Red Condor *Archive* is a secure [message archiving service](#) with lifetime retention and unlimited storage. The company’s next-generation technology is backed by a 24x7 customer care center staffed by email security experts at Red Condor’s headquarters.