

## 'TIS THE SEASON TO BE WARY

The holidays mark the perfect time to celebrate, give gifts, and take that much-deserved break from work or school. Unfortunately for users, cybercriminals also take this once-a-year chance to proliferate even more of their profiteering schemes.

### Online Holiday Shopping and Security Threats

Internet usage has been integrated into most of our activities because of the convenience and accessibility it offers. Arguably, the most common holiday-related online activity users engage in is shopping. Each year, online shoppers troop online to search for the latest promos, coolest gifts, and biggest bargains or to book flights and reservations to go on their dream vacations during the Christmas season.

In 2009, research firm comScore estimated that around US\$30 billion was spent by holiday online shoppers in the United States alone. The “Green Tuesday” campaign that offered discounts for “green” or environment-friendly products, for instance, accounted for the biggest daily spending amounting to US\$913 million.

	2008 Spending	2009 Spending	Percent Change
November 1–December 31	US\$27,982M	US\$29,084M	4%
Thanksgiving Day (November 26)	US\$288M	US\$318M	10%
Black Friday (November 27)	US\$534M	US\$595M	11%
Cyber Monday (November 30)	US\$834M	US\$887M	5%
Green Monday (December 14)	US\$859M	US\$854M	-1%
Green Tuesday (December 15)	US\$754M	US\$913M	21%
Weekend before Christmas (December 19–20)	US\$677M	US\$767M	13%

Source: comScore Inc., January 2010

Table 1. 2009 E-Commerce Season Versus Year Ago Nontravel (Retail) Spending

This year, the online spending may even outdo last year's figures, as comScore predicts a 7–9 percent increase, reiterating the fact that e-commerce means big business, especially during the holidays.



## Holiday-Inspired Web Threats

Though the holidays usually usher good cheer, they can, unfortunately, also bring about opportunities for cybercriminals to rake in more profit than usual. In a 2009 article, Trend Micro **identified several threats and scams** users may encounter during the most festive of seasons. We expect these threats to continue plaguing users.

### Links to So-Called Great Gifts

Search engines like *Google*, *Yahoo!*, and *Bing* may be very useful tools for shoppers on the hunt for great bargains but they **can also lead to dangerous sites** via various blackhat search engine optimization (SEO) techniques.

SEO is the process of improving a site or a Web page's visibility in search engines. It increases the chances that users will visit a particular site or page for marketing purposes. In the world of cybercrime, however, a similar technique known as blackhat SEO, is used to direct users to malicious sites and pages that serve several FAKEAV variants, among other malware variants.



▶ SEO is the process of improving a site or a Web page's visibility in search engines.

Online shoppers in search of the perfect gifts, travel packages, and other holiday-related items are served poisoned results through their trusted search engines. These results lead to compromised sites or pages that almost always end in FAKEAV system infections. In such an attack, users who click malicious search results see either prompts to download a fake application or codec or fake system scan results informing them that their systems have been infected. Downloading and executing the application or FAKEAV, as the case may be, of course, leads to the same thing—a malware-infected system.

Blackhat-SEO-instigated attacks typically **leverage newsworthy events** like celebrity deaths and scandals and destructive natural calamities to lure in potential victims. As such, cybercriminals **are likely to use search strings** like “holidays,” “gifts,” “decorations,” and “vacation packages” to entrap unsuspecting users this coming Christmas season.

### Social Networks, Not Spared

It seems that cybercriminals are not sparing social networks with *Facebook*, *Twitter*, and other social networking sites proliferating unsolicited holiday promotions as well. In particular, a scam in the guise of a Delta Airlines promo was discovered in *Facebook*, most probably spurred by the fact that the airline recently **gave its customers the option** of booking flights on the social networking site.



Clicking the links embedded in *Facebook* messages promising free tickets led users to a page that required them to “connect” to a page to get the said tickets. This generous offer, however, instead led them to a page that gave a third-party application permission to access their personal information. Giving their permission allowed cybercriminals to access their profiles, to grab their personal information without consent, to spam their email inboxes, and to post messages on their walls that led to a multitude of payloads, including information theft.

Scams are not the only problem that *Facebook* users face, as the site itself has played host to other security-related threats. *Sendible*, a popular marketing tool, for instance, was recently **used to spam malicious links** with the message “Change Your *Facebook* Background Here!” to the followers of several consumer goods giants. Clicking the link directs users to a page that solicits personal information. *Facebook* later admitted that the incident was caused by a temporary bug, which has since then been fixed.

Microblogging site *Twitter* has not been spared either, as a recent scam’s victims repeatedly **re-Tweeted a message** with a link to the site `http://{BLOCKED}voucher.net`. With the promise of free gift vouchers from various online shops, several users were tricked into clicking the malicious link. Affected users found themselves on a site that asked them to complete a survey and to invite their friends to earn points. Looking at the said site’s *WHOIS* information revealed that the domain was only registered in October of this year, suggesting that its creators may just be looking to take advantage of the upcoming holidays. *Twitter* has since suspended the user’s account, rousing even greater suspicion.

## Spammed Surprises

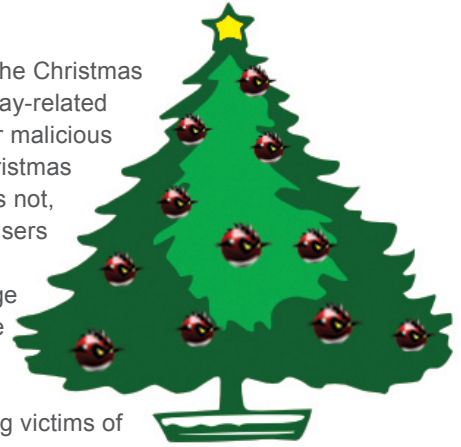
Spammed messages promising huge discounts and bargains are no longer new, especially during the holidays. In fact, spamming should now be considered a cybercrime staple since cybercriminals are known to take advantage of the most opportune events to snare their victims. To them, the most-celebrated occasions worldwide like **Mothers’ Day**, **Valentine’s Day**, and **Christmas** are just another means to profit.

More recently, TrendLabs engineers **found spam campaigns** leveraging the upcoming **Black Friday**, which traditionally marks the beginning of the Christmas shopping season in the United States. Being the biggest sales event in the United States, it seems only natural for cybercriminals to **take advantage of this holiday**. As in previous years, the spammed messages contained links to sites that offered replica watches, bags, and jewelry and sexual-enhancement pills instead of links to legitimate online shops sporting huge discounts and other promotions.

▶ **Black Friday** traditionally marks the beginning of the Christmas shopping season in the United States.

## Be Merry but Be Wary, Too

Just as Black Friday marks the beginning of the Christmas shopping season, however, the first few holiday-related attacks are only the start of bigger and bolder malicious schemes that users should watch out for. Christmas shopping online may be convenient, this does not, however, mean it is always safe. Given that users spend more money during the holidays, cybercriminals also see the holidays as a huge opportunity to increase their profits before the year ends.



Users, however, can readily prevent becoming victims of threats by:

- Immediately deleting dubious-looking email messages, especially those that come from unknown senders
- Avoid downloading file attachments or clicking links embedded in spammed or suspicious-looking email messages
- Scrutinizing promotions, especially those that come from questionable sources
- Keeping in mind that offers that are too good to be true usually are
- Visiting the official sites of vendors instead of relying on links embedded in messages
- Determining the legitimacy of sites and their addresses to avoid becoming victims of phishing attacks
- Ensuring the security of networks and systems, especially those from which they shop online
- Refraining from conducting online transactions in Internet cafes or public places with free Wi-Fi network access
- Making it a habit to keep online transaction records to avoid becoming victims of scams and other forms of fraud

Installing a **security software** that immediately deletes spammed messages from users' inboxes and that verifies the legitimacy of the sites they visit can greatly benefit those who want to have pleasurable holiday online shopping experiences. Users should keep in mind that anyone, whether naughty or nice, can become a victim of cybercrime.

## References:

- Argie Gallego. (February 13, 2009). *TrendLabs Malware Blog*. "WALEDAC Spreads More Malware Love." <http://blog.trendmicro.com/waledac-spreads-more-malware-love/> (Retrieved November 2010).
- Danielle Veluz. (May 5, 2010). *TrendLabs Malware Blog*. "Spammers Celebrate Mothers' Day." <http://blog.trendmicro.com/spammers-celebrate-mothers%E2%80%99-day/> (Retrieved November 2010).
- Delta Air Lines. (August 12, 2010). *Delta*. "Delta Launches First Airline Social Media 'Ticket Window,' Revamps Home Page." <http://news.delta.com/index.php?s=43&item=1098> (Retrieved November 2010).
- Det Caraig. (December 28, 2009). *TrendWatch*. "Don't Let Web Threats Spoil the Ho-Ho-Holidays." [http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/49\\_don\\_\\_\\_t\\_let\\_web\\_threats\\_spoil\\_the\\_ho-ho-holidays\\_\\_december\\_28\\_\\_2009\\_.pdf](http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/49_don___t_let_web_threats_spoil_the_ho-ho-holidays__december_28__2009_.pdf) (Retrieved November 2010).
- Gerald Dillera. (November 19, 2010). *TrendLabs Malware Blog*. "Voucher Scam Spreading via Tweets." <http://blog.trendmicro.com/voucher-scam-spreading-via-tweets/> (Retrieved November 2010).
- Leena Rao. (January 6, 2010). *TechCrunch*. "Shopping Spree: Total Online Holiday Spending Nears \$30 Billion." <http://techcrunch.com/2010/01/06/shopping-spree-total-online-holiday-spending-nears-30-billion/> (Retrieved November 2010).
- Marco Dela Vega. (November 24, 2010). *TrendLabs Malware Blog*. "With Holiday Wishes Come Poisoned Searches." <http://blog.trendmicro.com/with-holiday-wishes-come-poisoned-searches/> (Retrieved November 2010).
- Marco Dela Vega and Norman Ingal. (November 2010). *TrendWatch*. "The Dark Side of Trusting Web Searches: From Blackhat SEO to System Infection." [http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the\\_dark\\_side\\_of\\_trusting\\_web\\_searches\\_-\\_from\\_blackhat\\_seo\\_to\\_system\\_infection\\_\\_nov\\_2010\\_.pdf](http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_dark_side_of_trusting_web_searches_-_from_blackhat_seo_to_system_infection__nov_2010_.pdf) (Retrieved November 2010).
- Mary Bagtas. (December 25, 2009). *TrendLabs Malware Blog*. "Christmas Greetings from Spammers." <http://blog.trendmicro.com/christmas-greetings-from-spammers/> (Retrieved November 2010).
- MG Seigler. (November 9, 2010). *TechCrunch*. "Sendible Flaw Uncovers a Big Facebook Bug; Huge Pages Compromised by Spam." <http://techcrunch.com/2010/11/09/sendible-facebook-hack/> (Retrieved November 2010).
- Niño Penoliar. (November 15, 2010). *TrendLabs Malware Blog*. "Cybercriminals Already in a Festive Mood." <http://blog.trendmicro.com/cybercriminals-already-in-a-festive-mood/> (Retrieved November 2010).

- Phil Wahba. (October 14, 2010). *Reuters*. "comScore Sees Holiday Spending Up 7–9 Percent." <http://www.reuters.com/article/idUSTRE69D5TA20101014> (Retrieved November 2010).
- Ryan Flores. (November 2010). *TrendWatch*. "How Blackhat SEO Became Big." [http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/how\\_blackhat\\_seo\\_became\\_big\\_\\_november\\_2010\\_.pdf](http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/how_blackhat_seo_became_big__november_2010_.pdf) (Retrieved November 2010).
- Trend Micro Incorporated. (November 8, 2010). *Threat Encyclopedia*. "Black Friday Spam." <http://about-threats.trendmicro.com/Spam.aspx?language=us&name=Black+Friday+Spam> (Retrieved November 2010).
- Wikimedia Foundation Inc. (November 23, 2010). *Wikipedia*. "Black Friday (Shopping)." [http://en.wikipedia.org/wiki/Black\\_Friday\\_%28shopping%29](http://en.wikipedia.org/wiki/Black_Friday_%28shopping%29) (Retrieved November 2010).
- Wikimedia Foundation Inc. (November 22, 2010). *Wikipedia*. "Search Engine Optimization." [http://en.wikipedia.org/wiki/Search\\_engine\\_optimization](http://en.wikipedia.org/wiki/Search_engine_optimization) (Retrieved November 2010).