Stay Safe Online This Holiday Season by Following Proofpoint’s Seven Simple Rules

Cyber Monday and Black Friday Give Rise to Increased Internet Threats: Protect Your Identity and Financial Information With These Helpful Tips

SUNNYVALE, CA -- (Marketwire) -- 11/16/12 -- With the busy holiday shopping season upon us once again, Proofpoint, Inc. (NASDAQ: PFPT), a leading security-as-a-service provider, reminds consumers that as merchants gear up for "Cyber Monday" and "Black Friday" shoppers, spammers and online scammers are also expected to work overtime to exploit the busy holiday season.

For the past several years, Proofpoint email security researchers have observed that the volume of attacks -- including phishing email attacks, social media exploits and other types of malware attacks -- typically increases during the holiday season. Many of these attacks are engineered to take advantage of the consumer mindset during the holidays. Proofpoint once again advises consumers to look out for holiday shopping, charity and package delivery scams that are designed to trick them into giving away personal information, exposing credit card numbers or banking information, or downloading malware that gives criminals remote access to their computers or mobile devices.

In its October 2012 report on email security threats, Proofpoint found that, on any given day, phishing attacks represented 10 percent to more than 30 percent of total unsolicited email volume, and this trend has continued into the first part of November.

Security-as-a-Service vendor Proofpoint (http://www.proofpoint.com) offers the following "Seven Simple Rules" that consumers can follow to help ensure their online safety during the holiday season:

1. Be aware: Always view with suspicion any email with requests for personal IDs, financial information, user names, or passwords. Your bank, online services, government agencies or legitimate online stores are extremely unlikely to ask you for this type of information via email. Consumers should also be suspicious of similar emails that appear to come from an employer or friend. Never send personal financial information such as credit card numbers and social security numbers via email.

Today's malicious emails and phishing attacks are disguised as communications from all sorts of organizations, including banks, money transfer services, government agencies, media outlets, and package delivery services.

2. Don't click: If you receive a suspicious email, don't click the links in the email or open file attachments from anything but 100 percent trusted sources. Links embedded in emails may take you to fraudulent sites that look similar or identical to the legitimate "spoofed" site. In addition to attempting to gather your personal login credentials, these phishing sites may also automatically install malicious software without your knowledge. Increasingly, scammers are using link shortening services to disguise the true destinations of their links. Instead of clicking, open a browser and type the actual Web address for the site into the address bar. Alternatively, call the company using a phone number you already know.

3. Be secure: When you are shopping online, entering important information such as credit card numbers, or updating personal information, make sure you're using a secure Web site. If you are on a secure Web server, the Web address will begin with "https://" instead of the usual "http://". Most Web browsers also show an icon (such as Internet Explorer's "padlock" icon) to indicate that the page you are viewing is secure.

4. Don't fill out email forms: Never fill out forms within an email, especially those asking for personal information. Instead, visit the company's actual Web site (using a Web address you already know) and ensure that the page you are using is secure before entering sensitive information.

5. Keep an eye on your accounts: Check the accuracy of your credit card and bank statements on a regular basis, especially during the busy holiday shopping season. Many scammers count on consumer inattention to get away with fraudulent charges. If you see anything suspicious, contact your financial institution immediately.

6. Get social media savvy: Email isn't the only attack vector used by spammers and scammers. Social media sites like Facebook and Twitter are increasingly used to deliver the same kinds of scams and malicious links to unsuspecting users. Spammers and malware writers continue to distribute malicious, but convincing, emails that masquerade as notifications.
such as friend requests or message notifications. Keep all of the preceding tips in mind when using the latest communication tools.

7. **Make security your first stop:** If your holiday includes giving or receiving a new computer, mobile device or upgraded operating system, install a good anti-virus or Internet security solution before doing anything else online. Reputable vendors include F-Secure, McAfee and Symantec. Be extremely wary of Web pop-ups that offer “free security scans” or that inform you that your machine is infected with a virus. Such offers commonly lead to fraudulent anti-virus solutions that are actually malicious software.

**About Proofpoint, Inc.**
Proofpoint, Inc. (NASDAQ: PFPT) is a leading security-as-a-service provider that focuses on cloud-based solutions for threat protection, compliance, archiving & governance and secure communications. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against phishing, malware and spam, safeguard privacy, encrypt sensitive information, and archive and govern messages and critical enterprise information. More information is available at [www.proofpoint.com](http://www.proofpoint.com).

Proofpoint is a trademark or registered trademark of Proofpoint, Inc. in the U.S. and other countries. All other trademarks contained herein are the property of their respective owners.

**Add to Digg** **Bookmark with del.icio.us** **Add to Newsvine**

**MEDIA CONTACT:**

Orlando DeBruce
Proofpoint, Inc.
408-338-6829
ODEBRUCE@PROOFPOINT.COM

Lisette Paras
Ogilvy Public Relations
415-677-2771
LISETTE.PARAS@OGILVY.COM

Source: Proofpoint

News Provided by Acquire Media