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

Consumers Can Protect Their Identity and Financial Information with These Helpful Tips

SUNNYVALE, Calif. – November 16, 2009 – While online merchants gear up for the holiday shopping season and “Cyber Monday” shoppers await dollar-stretching deals, spammers and scammers will once again turn up the volume on their attacks and look to take advantage of increased email and Internet use during the busy holiday season.

As in previous years, security experts at the Proofpoint Attack Response Center expect to see a significant increase in attacks—including spam and phishing emails, social media exploits and malware attacks—designed to take advantage of the consumer mindset during the holidays. Proofpoint warns consumers to look out for holiday shopping, charity, online banking and tax scams that are designed to trick them into giving away personal information or downloading malware that gives criminals remote access to their computers.

Email security vendor Proofpoint (http://www.proofpoint.com) offers the following “Seven Simple Rules” that consumers can follow to make sure their cyber-holiday season is a safe one:

1. Be aware: 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 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 government agencies, software vendors and money transfer services, as these examples from the Proofpoint Email Security Blog show.

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. 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 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 this time of continued economic unease and during the holiday shopping season. If you see anything suspicious, contact the 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 are riding the social media wave, commonly using 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, netbook or upgraded operating system, install a good desktop 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 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.

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