Issue # 12 Volume #15 December 2014

AaSys Solutions

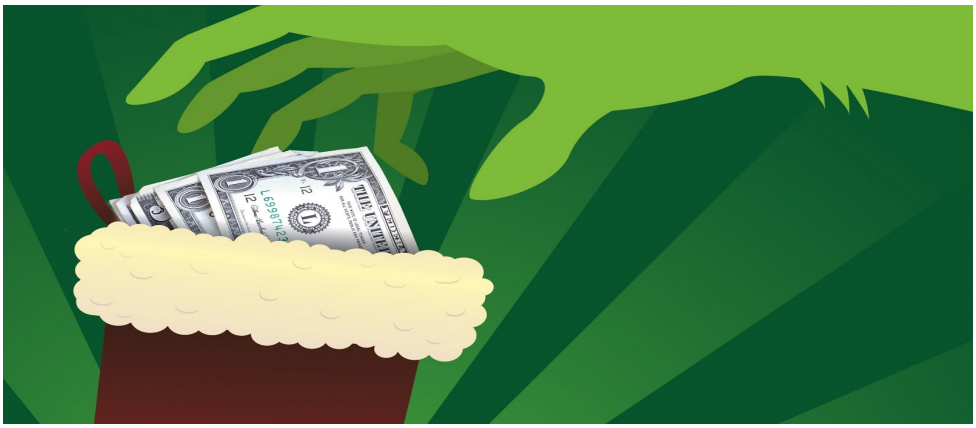
Solutions are our Business

"Bah humbug!" - Avoid holiday scams

The holidays are a time for eggnog, family and festive meals, but there's also a dark side to the season: the scammers and hackers who are ready to pounce on the unaware. Financial scams tend to pop up more around the holidays. Consumers are busy, buying lots of goods and more than willing to shell out extra cash for those in need. While generosity is the theme of the season, it's vital consumers exhibit caution when making any purchase or donating to a charity.

Shopping online helps you avoid the crowds and hassles of stores during the holidays and can reveal some great bargains. But surfing for gifts in cyberspace can be risky, courtesy of copycat websites that shoppers sometimes visit inadvertently after typing the name of that sought-after item into a search engine. Although legitimate online retailers pop up on the screen, so do "cybersquatters," bogus businesses that steal or alter the Internet addresses of well-known companies to launch copycat sites.

And this season may turn into a free-for-all for fraudsters thanks to a few trends that are prompting criminals to set their traps for unmindful consumers. The bad guys have a wide variety of tricks up their sleeves, from fake charities to "phishing" schemes aimed at tricking holiday shoppers.



One difference this year is that this holiday season may be the last for magnetic-strip credit cards, which are easier to hack. A new security standard going into effect next October will introduce the "chip and PIN" cards favored in Europe.

"This is like the last hurrah for hackers to go after retailers who are using magnetic-strip credit cards. If you are a holiday shopper, go into holiday shopping season assuming your card will be compromised in a credit breach and act accordingly," says Yaron Samid of BillGuard. On top of continued data breaches, the year's past data attacks on retailers such as Target, Home Depot and Michael's means that criminals also have access to millions of stolen emails. Those emails can be used in phishing scams to target unwary retailers this holiday season. The phishing attempts can appear to come from either a retail or a shipping company, such as UPS or Fedex, but actually are fake emails that are trying to get consumers to disclose their emails.

Continue Page 2

Are there subjects that you would like to have covered in future newsletters? We are always looking for topics of interest and we welcome all suggestions! To submit a topic, subscribe, or unsubscribe to our distribution list, please send an email to newsletter@aasysgroup.com

11301 N. US Highway 301, Suite 106
Thonotosassa, FL 33592
(800) 799-8699
www.aasysgroup.com

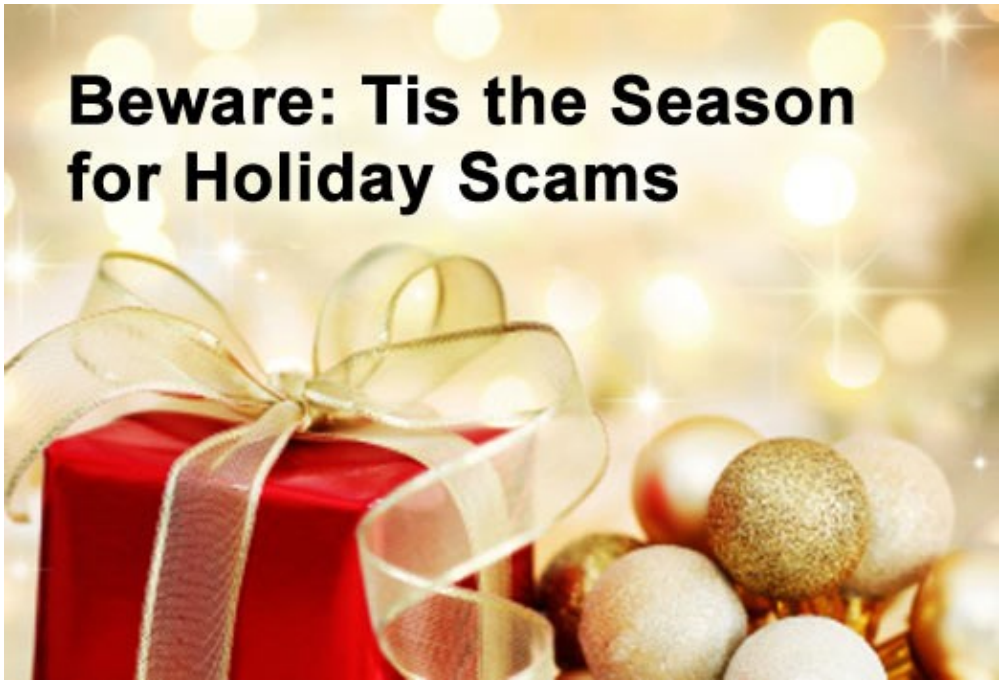
REMINDER!
The Help Desk will be closing at 4:00PM EST on December 24, 2014.

AaSys wishes you and your family a very Merry Christmas and a Happy New Year!

Inside this issue:

During the holidays, check your card activity daily. Given BillGuard's expectation that at least one or two major data breaches will occur this holiday season, it's more important than ever to remain alert to suspicious activity. If you notice any unauthorized charges, immediately contact your bank.

When you look at card activity, keep an eye out for "microcharges." The average consumer looks for big purchases, but hackers often test cards to see if they are valid by charging small amounts of $1 or $2. If those cards are found to be valid, hackers can then sell them to other crooks for a premium. That means that consumers shouldn't overlook small, unauthorized charges.

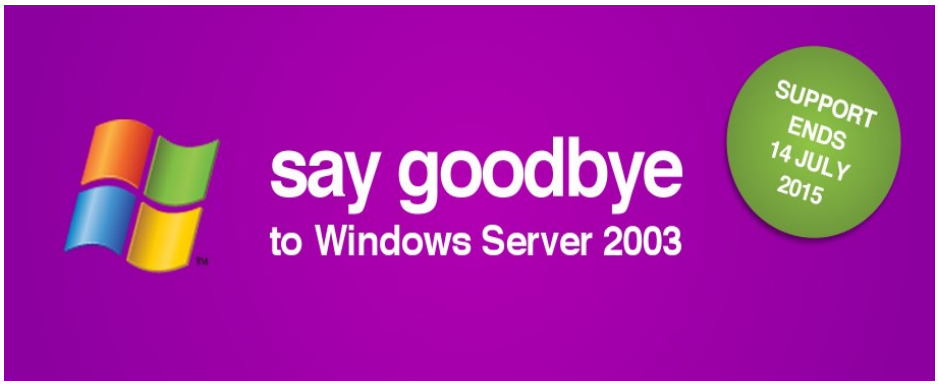


Source: Aimee Picchi, http://finance.yahoo.com/news/how-to-avoid-the--bah-humbug--of-holiday-scams-170056409.html

Sid Kirchheimer, http://www.aarp.org/money/scams-fraud/info-11-2010/scam_alert_clicking_on_cyber_monday_.html

Don't Forget...Microsoft Ending Support for Windows Server 2003 Operating System

The count down is on! On July 14, 2015, Microsoft will be ending support for Windows Server 2003. This means that those still using that operating system will no longer receive crucial security patches that help protect against viruses, spyware and malicious software. Users may also encounter problems with software and hardware compatibility since new software applications and hardware devices may not be built for Windows Server 2003. Computers using the old software will still work, however, the risk of viruses and other malicious attacks increases exponentially and could result in significant loss of data, business assets, and confidential documents.



Don't wait until the last minute to make changes. July 14, 2015 will be here sooner than you think! AaSys can help you every step of the way. Please contact your Account Manager today for more information !

McAfee's Annual 12 Scams of the Holidays List

Keeping your digital life safe!

1. **You've Got Mail!** — As holiday sales continue to migrate online, the risk for shipping notification and phishing scams are increasing. Though malware is a year-round risk, since many people do their holiday shopping online, consumers are more apt to click on a shipping notification or phishing e-mail because they think it is legit.

2. **Deceptive Advertising** — Everyone is searching for steals and deals during the holidays. Keep your eyes peeled (and your wallet in check) when online shopping for this season's most coveted products. Dangerous links, phony contests on social media, and bogus gift cards are just some of the ways scammers try to steal your personal information and ruin your holiday cheer.

3. **Chilling Charities** — 'Tis the season for giving. During the holidays, many consumers give back by donating to their favorite charity. Sadly, no good deed goes unpunished. Be wary of fake charities that could reach you via email, or are shared virally through social media.

4. **Buyer Beware** — There are just some scams that you can't help but fall victim to, unfortunately. Point of sale malware that leads to exposing credit card information falls into this category. Make sure you check your credit card statements vigilantly and stay on top of breaking news to be aware and prepared.

5. **IScams** — New mobile apps for Android and iOS devices are added every day. Thanks to the ongoing advancement of technology, your mobile device can control the temperature in your house, keep you connected to social media and add cool filters to your holiday photos. Even the most official-looking or festive apps could be malicious and access your personal information.

6. **Getting Carded** — Digital e-cards to spread the holiday cheer are fun, easy and most importantly, thoughtful. While you may want a loved one to send you "Season's Greetings," hackers are looking to wish you a "Merry Malware!" Well-known e-card sites are safe, but be wary of potential scams that cause you to download malware onto your device.

7. **Holiday Travel Scams** — With travel on the rise during peak holiday times, online scammers are ready to take advantage of the fact that consumers often become less vigilant about their safety. Fake online travel deal links are bountiful, but there are also risks that exist once you arrive at your destination including spyware that can access your information through logging onto infected PCs onsite.

8. **Bank Robocall Scam** — When holiday spending increases and consumers are aware of the abuse to their bank accounts and credit cards, hackers use this as an opportunity. In most cases, consumers receive a fake phone call from one of these institutions from an automated (or not) "security agent" stating that the user's account has been compromised and requesting personal information including the account password, to make changes.

9. **ATM Skimming** — During the holiday season, you need cash and are usually in a rush to get it. Criminals can access your information at ATMs by installing skimming devices to steal the data off your card's magnetic strip and either using a video camera or keypad overlay to capture your PIN. A simple solution: look carefully at your ATM for anything suspicious and cover the keypad when entering your PIN.

10 **Year in Review Traps** — Many news services capitalize on the holidays by developing "Year in Review" articles. Companies should warn their employees about the risks of clicking on these types of links from their work emails. Links from phony sources could infect and compromise the security of company devices.

11. **BYO…Device** — With an increase in travel, activity (and bubbly!) over the busy holiday season, people are more likely to forget their smart phones in public places. While inconvenient for them, it is also way for hackers to access sensitive personal information and business data if the appropriate security measures are not in place.

12**. Bad USB Blues** — During the holiday season, you may see an increase in gift baskets from vendors who want to continue doing business with your company in the upcoming year. One of the most popular items in these baskets includes branded USBs. Beware of allowing your employees to use these, as undetectable malware is sometimes pre-installed on them.

Source:Webpage: www.mcafee.com/12scams Robert Siciliano