Volume 4, Issue 12

December 2018

Bank of Botetourt
Taking Care of You

SAFE ONLINE HOLIDAY SHOPPING

INSIDE THIS ISSUE:

Member FDIC EQUAL HOUSING LENDER

Bonsack

Buchanan

Care Center

Cave Spring

Daleville

Eagle Rock

Fairfield

LakeWatch

Lexington

Natural Bridge

Peters Creek

Salem

Troutville

www.bankofbotetourt.com
www.facebook.com/botetourt

(540) 591-5000

Did you know that last year internet scams increased by twenty two percent between Thanksgiving and Christmas? But that didn't slow down the rate of consumer spending. Economists are expecting an increase of 4.7 percent of spending during the 2018 holiday season. These are some very interesting stats, that everyone should pay attention to, but there is one group of people who are definitely keeping tabs on holiday spending-yes you guessed it-Hackers.

The holiday season is truly the most wonderful time of the year. Getting together with loved ones, overeating, making memories, and of course, shopping! It gets no better than that. Unfortunately hackers are keenly aware of this and are patiently waiting for the shopping frenzy to begin. Every year we educate our readers on the dangers of online and in-store holiday shopping. We know at times it may sound like a broken record, but it is extremely important to reiterate some of the most common scams that are out there. A report issued by Juniper Research anticipates fraud losses from online shopping and other online uses to hit 22 billion dollars by the end of the year. Although the information may seem redundant, given the amount of damage that these scams have already inflicted, it is definitely worth repeating these precautionary steps...especially during the holiday shopping season.

Lets review some of the most common holiday scams:

- ***First things first, if the deal seems to good to be true, it probably is.*** We all want a bargain, but sometimes the bargain just doesn't "pass the smell test." The hottest ticket item for the season is sold out at all major retailers, and you're almost out of shopping days. But then you get an email or see an ad in your social media feed from one store that claims to have the exact item you've been searching high and low for...and it's at a huge discount! Don't take the bait. Most of these "deals" lead to fake sites that attempt to steal your credit card information.

- ***Recognize fake websites from the real deal.*** The domain is always a good place to start when trying to decipher between a real and fake website. On a fake site, the domain name is usually peppered with extra numbers or symbols. They often also have misspelled names or add-ons to well-known site URLs (e.g., amazonsecure-shop.com). Look for key words that also send up a red flag such as "secure," "discounts" and "official." Major retailers most of the time only use their company name in their domain without any extra hyphens or words.

- ***Stay Vigilant. Don't get distracted and remember to take your time.*** Flash sales have become extremely popular. You have a certain amount of time to purchase your item at a deeply discounted price, and it's first come, first served. That time crunch can sometimes make you get distracted and not pay attention to red flags. Hackers are just as aware of these flash sales as you are and have already created fake sites to lure in shoppers. Trying to beat that clock, you do a quick scan of the site and it all looks real and legit, so you enter your credit card information and, just like that, you have become the next unwitting victim of a scammer. If you happen to miss a flash sale while trying to do your due diligence, chances are one will come up again!

Continued on Page 2

- ***Yes, you also need to scrutinize Santa's emails.*** Santa sending personalized emails to kids with video clips has become very popular; especially since this generation communicates primarily with mobile devices. But be careful which company you use so send well wishes from Santa. Make sure to vet them properly and thoroughly. Hackers know this is a hot commodity and are hoping parents and kids divulge personal information which will help them commit their crimes.

- ***Phishing is alive and well.*** Scammers know you are waiting on tracking information for all those expensive gifts you purchased online. Instead of clicking on the link from an email received, take the tracking number and go directly to the shipping company's site. This is just an added precaution to ensure you are not clicking on a bogus link.

- This one is an oldie but has proven to be one that hackers rely on. During the holiday people are more susceptible to giving to charities. ***Before you give to any charity, do some due diligence to ensure it's a legitimate organization.*** Opt to give using a method that you know is safe.

Source: https://www.cnbc.com/2018/11/21/phishing-scams-fraud-targets-holiday-shoppers.html

ZERO-DAY EXPLOIT EXPLAINED

Information security technology terms can sometimes be complicated to understand, especially if you are not working within the field. But because a majority of people use laptops, workstations, and mobile devices and are connected through the world wide web, it is important to know some basic terminology.

Zero Day Exploit is one of those often heard and seen cybersecurity terms. But what does it mean? Continue reading to get a brief introduction.

A zero-day vulnerability is essentially a flaw found in software or hardware with no immediate patch of fix. The term 'zero-day' means it's a newly discovered vulnerability giving the developer zero days to fix the security issue. These types of vulnerabilities are considered dangerous because they can be used by cybercriminals to exploit a weakness within the software or hardware. When a hacker recognizes the flaw, he can write codes to infiltrate the system through the security hole.

Once it is public, a developer must act fast in order to protect its users. Unfortunately, sometimes a developer may fail to release a patch in a timely manner causing the vulnerability to be fully exploited, which is known as a ***zero-day attack***.

Fortunately there are ways to protect yourself. Of course the first line of defense is to always ensure your antivirus software is up to date. Software updates provide the latest and greatest protection, so it is important to follow the recommended update schedule provided by the antivirus company. Also, make sure the antivirus can protect against known and unknown threats.

Prevention is key. Protect yourself by establishing good online security habits. Avoid web browsing on sketchy sites and clicking on unknown links.

Keep in mind, though, that sometimes the best defenses are not enough. Having a plan to deal with such an attack is crucial to minimizing the damage and to protecting employees, customers, and your data.

Zero Day attacks are a real concern for even the most vigilant IT administrators. These types of attacks are not usually found right away and can sometimes take days or months to discover. There is never 100% protection when dealing with cybersecurity, however having the proper safe guards in place can help reduce the risk of important data falling into the wrong hands.

Sources: https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html