# Bank of Botetourt

DECEMBER 2020 Issue 12

# 2020 Holiday Scams


It's that time of the year again. Although, due to the pandemic, many will be doing their shopping online, the same precautions still apply. Bad actors are gearing up for a potential windfall and an early Christmas gift by using old and new tricks.

Every year we warn about holiday scams and this year is no different. As the holidays approach, expect an uptick in scamming activity.

Fraudsters are taking advantage of the pandemic and using online scams to steal consumers' money and personal information through phishing, malware, and other schemes. With more commerce occurring online this year, the Cybersecurity and Infrastructure Security Agency (CISA) are reminding shoppers to remain vigilant.

Here are some of the most common holiday scams to be aware of this year.

### Fake Charities

Many Americans have been hit extremely hard due to the pandemic and good Samaritans are trying to do their part to help their fellow citizens by giving to charities to help those in need. But be careful who you give to. This time of year fake charities may pop up on your social media feed and on internet ads. Sometimes the names are similar to other well known organizations, but in reality they are a hoax. For example the charity could be named "Salvation Armies" (we know the real charity is Salvation Army).

*Continue on Page 2*

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**

### Gift Card Scams

Although gift cards are extremely popular because they take the guess work out of gift giving, shoppers are being warned of "payment red flags". If sellers and websites demand payment solely through gift cards that should give you pause. Once you provide the gift card number, chances are the money will be gone, and it's nearly impossible to recover once it's lost.

### Fake Websites

Recognize fake websites from the real deal. The domain is always a good place to start when trying to decipher from 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.

### Not All Deals are Good Deals

We are always looking for the best bang for our buck, but not all deals are a bargain. 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! Unfortunately, if it sounds too good to be true, it most likely is. Most of these "deals" lead to fake sites that attempt to steal your credit card information at check out and sometimes even send you counterfeit or knock-off imitations.

### Porch Thieves

Since many people will be doing  majority of their holiday shopping online this year, remember not all thieves are hackers on the other end of the computer. Some bad actors still use good old-fashioned theft. Once packages are delivered to your door step thieves come by and swipe them. Last year almost 26 million Americans reported being victims of porch theft and that number is expected to increase. To protect your online orders consider requiring a signature at delivery or have them delivered to somewhere else where someone trustworthy will be available to get them for you.

### Be Careful with Your Emails, Even Emails from Santa

Ask yourself is this for REAL? If you get an unsolicited email with a free gift card from your favorite retailer, take a pause and ask yourself some questions? Why would a retailer send you a gift card? When was the last time you purchased something from this retailer? Did you apply for any promotions from this retailer? The most recent scam involves a fake email offering a $50 Amazon gift card via a malicious link. The link takes you to a fake Amazon site asking you to enter your password for "security purposes" and may even ask you to provide sensitive information such as your social security number. If, you see something suspicious in your inbox, just delete it. 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.

Holiday online shopping brings more opportunities for bad actors to take advantage and scam unsuspecting shoppers. The good news is many organizations and cyber experts are ringing the alarm and are making consumers more aware of the potential pitfalls of shopping online and educating them on ways to reduce the risk of being a victims of any of these crimes.

Happy Holidays and remember to stay vigilant!

*Sources:*
*Online Scams 2020: 5 Holiday Scams to Look Out For | Money*

# 5 Signs You're a Ransomware Target

Ransomware is a type of malware that threatens to publish the victim's data or block access to it unless a ransom is paid. Employees are prone to this attack when they open a link in a suspicious email which activates the malicious software into the system.

But there are some red flags that could indicate that your organization may be a target of a ransomware attack. Here are some things to look for:

### 1. You Are Locked Out of Your Computer

A specific kind of ransomware known as “locker ransomware” will deny you access to your device. This kind of ransomware does not only target your files but your entire computer. In this instance our first instinct is to reboot the computer. Typically once the computer is turned back on it is common for the ransom note to be displayed on a splash screen upon restarting up the device.

### 2. Patterns of Suspicious Behavior

Every day activities, from small one to the major ones should be seamless. But when there is abnormal shift or a hiccup and IT professionals are revisiting the same issue at the same time every day, or in a repeating pattern is often an indication that something else is going on and should prompt security teams to investigate immediately.

### 3. Unusual Time Stamps Appear on VPN Connections

Be on the lookout for anomalous time stamps on VPN connections. If your organization has normal levels of traffic between 9 a.m. and 5 p.m. ET, and then all of a sudden there's traffic with IP addresses from Russia or Mozambique at 3 a.m., that should set off warning signs.

### 4.Phishing Emails With Strange Domains

Phishing is the delivery mechanism of choice for ransomware and other malware. Organizations need to watch for emails that come in with strange domain names that have never been in the company's environment before.

### 5.Security Tools Are Being Disabled

Once attackers have admin rights, they will try to disable security software using applications created to assist with the forced removal of software, such as Process Hacker, IObit Uninstaller and PC Hunter. These types of tools are used by IT security teams when needed, however if they suddenly appear it could be a sign that the network has been infiltrated and security protocols need to be implemented promptly.

*Sources:*
*The realities of ransomware: Five signs you’re about to be attacked – Sophos News*
*Ransomware: These warning signs could mean you are already under attack | ZDNet*
*3 Signs You’re a Target for a Cyber Attack (netrixit.com)*