Bank of Botetourt

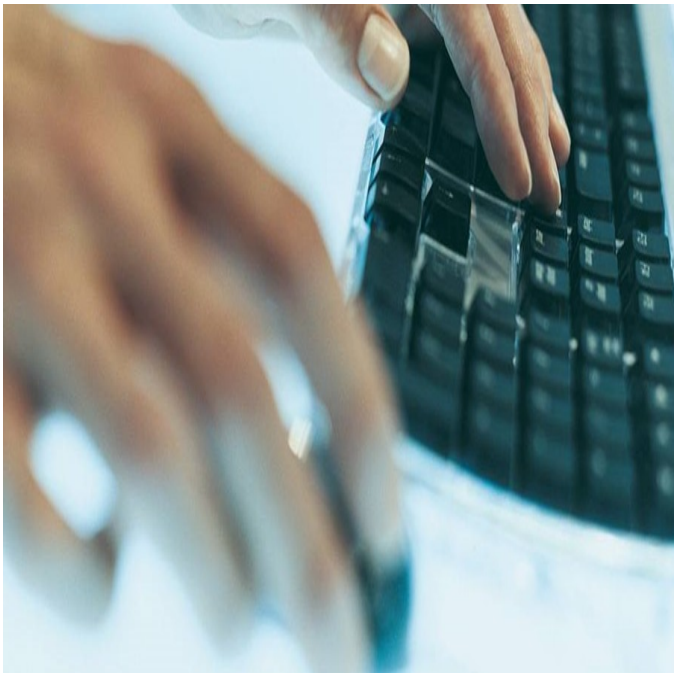
March 2021 Issue 3

Member FDIC

EQUAL HOUSING LENDER

Merchant Websites

6 Tips for Safe Online Shopping



We all love online shopping and probably couldn't imagine a world without it. For the most part, shopping on merchant websites is relativity safe; however, that does not mean there are no risks.

Merchant websites are sites that are able to accept electronic credit and debit card transactions from customers. Merchant websites will always be a target for cyberattacks because of the data that is associated with them. Financial data and personal data, which is usually collected on these sites, are a goldmine for cybercriminals. Typically, consumers gravitate towards sites they trust and know and have done business with over a long period of time. But during the pandemic, many consumers found products were scarce at their normal retailers and opted to try new retailers. A recent study showed 56 percent of consumers tried a new retailer during the pandemic. This trend is expected to continue until consumers feel safe going back to normal in-person shopping.

But the increase of transactions on merchant websites comes with risk. In 2019, the FBI's Internet Crime Complaint Center got an average of 1,300 online theft complaints a day which resulted in over $3.5 billion in losses to individuals and businesses and the 2020 numbers are expected to be higher. Many of the complaints included merchandise not being received or receiving some obscure product with no way to return it without paying enormous additional fees.

During a time when online shopping is the go-to method, it is important that consumers understand the potential risk of using merchant websites, especially the not so common ones.

Continue on Page 2

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

Here are six tips for safe online shopping.

* ***Shop with reputable retailers*** -It is always best to shop with companies you know and trust. It is also best to bookmark your favorite sites instead of typing the address. Typos can lead you to a fake site that looks legitimate and can possibly compromise your data.

* ***If it's too good to be true, it probably is***. - Social media platforms may sometimes have ads that seem unreal or even display offers for free products. This should be a red flag. If the prices are not comparable with other merchants it should give you pause. Investigate further before you decide to buy.

* ***Check the sites security before you buy***. - Reputable sites want their customers to be as secure as possible. Look for the locked keypad on the browser bar of the website. This indicates they use SSL (secure sockets layer) encryption. Also, a secure site's URL will start with "https" instead of "http."

* ***Do not disclose your personal information***. - No merchant website should request your social security number to complete a transaction. If they do, leave that site immediately.

* ***Do not shop using public Wi-Fi***. - Public Wi-Fi is not secure and hackers are literally just waiting for someone to make their next transaction while sipping their latte at a coffee shop. Use a Virtual Private Network (VPN) or your phone as a hotspot for more secure shopping.

* ***Research new retailers before completing a transaction on their site*** - Do your homework on any new business before you purchase, especially if you have never purchased from them in the past. Check out their reviews and search the Better Business Bureau website for complaints. Also check their contact page to verify it is a US based address and phone number and call to make sure the number is legitimate.

The convenience of online shopping saves us all time and sometimes money, but it is also lucrative for scammers. Being a safe and secure shopper starts with understanding the risks and taking steps to mitigate those risks.

Sources:
https://www.mobilepaymentstoday.com/ Mobile Payments Today | Technology, Trends & Insights | Mobile Payments Today
15 Tips for Safer Online Shopping (lifelock.com) https://www.lifelock.com/learn-internet-security-safe-online-shopping.html
Online Shopping - Stay Safe Online https://staysafeonline.org/stay-safe-online/online-safety-basics/online-shopping/

What are Botnets?

The Internet is filled with security threats like phishing and malware, but we rarely hear much about botnets. A botnet is a string of connected computers coordinated together to perform a task. That task does not necessarily have to be something negative, however it has been used as such by cybercriminals. Unfortunately, botnets are just one of the many dangers on the Internet we must contend with.

Botnets are designed to collect and save data, such as passwords, Social Security numbers, credit card numbers, and other personal information. The data is then used for criminal purposes, such as identity theft, credit card fraud, spamming, data breach attacks and malware distribution.

Botnets gain access to your machine through some piece of malicious coding. Once a device becomes a bot, it is usually part of a botnet. The botnet is a larger network of other infected devices that can have anywhere from a few hundred to many thousand devices controlled remotely by hackers. The hacker, also known as a bot-herder, sends a command from its "command and control" computer to an unknowing recipient using file sharing, email, or a social media application or other bots as an intercessor. Once the recipient opens the malicious file on his computer, the bot reports back to the bot-herder and can dictate commands to the infected computers.

Typically, cybercriminals use bots for financial gain or to steal personal or sensitive date. But they also use this method to assist in distributed denial-of-service (DDoS) attacks to shut down websites, send spam out to millions of people, create fake banner ads on web browsers and bogus popup ads selling fake anti-spyware software.

All internet users should be vigilant and help protect themselves against bots and other malicious attacks by following these steps:

⇒ *Keep a clean machine!*

⇒ *Run regular antivirus scans. This is one of the best ways to prevent your device from becoming part of a botnet network. Most antivirus are able to prevent most botnet malware from ever being installed on your computer.*

⇒ *Make sure your security software, web browser and operating system are up to date. Hackers often utilize known flaws in operating system security to install botnets.*

⇒ *Back up all your data.*

⇒ *Have strong and unique passwords that contain at least 12 characters and are made up of numbers, letters, and symbols.*

⇒ *Never click on links from unknown sources in email, social media posts and online advertising.*

scams-targeting-seniors/
https://www.protectseniorsonline.com/resources/cybersecurity-best-practices/