First Bank & Trust Company

The Bank That Puts You First

Member FDIC

June 2020 Issue 6

Signs Your Device May Have Been Compromised

The COVID-19 pandemic has caused many companies to shift from working in a shared office to working remotely almost overnight. Although some were prepared for the transition, many were not. With the urgency to stay safe and try to stop the community spread of the coronavirus by staying home, many workers had to leave their offices in a rush, not realizing it would be several weeks or months before they were able to return and took susceptible hardware home to help continue their daily responsibilities.

Cybercriminals have used this pandemic to their advantage and there has been a major uptick in attempted attacks against remote devices. Cybercriminals and hackers continue to use their common tactics such as default passwords, revisiting unpatched vulnerabilities, scanning for open ports and services and installing backdoors. One major vulnerability are smartphones which have become a critical part of every work environment. Hackers have been able to expose many flaws and vulnerabilities in the smart devices being used to complete everyday business tasks.

EQUAL HOUSING LENDER Member FDIC

Abingdon Virginia, East
276-628-3838

Abingdon Virginia, West
276-628-9558

Bridgewater Virginia
540-828-2020

Bristol Virginia, East
276-466-9222

Bristol Virginia, West
276-669-1122

Bristol Tennessee, Volunteer Pkwy
423-652-2022

Christiansburg Virginia
540-260-9060

Fairlawn Virginia
540-633-3793

Gray Tennessee
423-467-9966

Harrisonburg Virginia
540-434-0671

Johnson City Tennessee
423-975-9900

Kingsport Tennessee
423-246-3700

Lebanon Virginia, East
276-889-3401

Lebanon Virginia, West
276-889-4622

Lynchburg Virginia
434-455-0888

Norton Virginia
276-679-7401

Staunton Virginia
540-885-8000

Verona Virginia
540-248-7700

Waynesboro Virginia
540-943-5020

Wise Virginia
276-328-3439

Wytheville Virginia
276-228-1125

Operations Center
276-623-2265

Continued on page 2

Both laptops and smartphones are susceptible to hacks and although manufactures and security firms are trying hard to find the flaws before the cybercriminals do, unfortunately, hackers continue to work overtime to ensure they can take advantage of the loopholes before programmers find them. During these uncertain times, remote workers need to remain vigilant and pay attention to signs that their device may have been compromised.

You may have been compromised if you notice:

- Slower performance on your devices
- Increased pop ups
- Increased network activity
- More spam emails getting blocked
- You start receiving emails from unknown senders
- Unknown text messages being sent to contacts
- Your battery drains faster
- Websites fail to upload or have poor quality
- Apps begin to crash
- You are unable to make or receive calls or calls are dropping
- Apps suddenly are installed or uninstalled
- Apps suddenly open by themselves

Protect your data and your device by following these tips:

- Download the latest and official patches
- Install a multi layered protection system
- Use a virtual private network (VPN) when connecting to your company's' network
- Avoid public or unsecured networks
- Use a strong passcode to lock all devices. Don't use common words, birthdays or any personal information
- Turnoff geotagging. Many phones are set to embed location tags as a default. Make sure that feature is turned off.
- Don't keep your Bluetooth connection on. Hackers can access your connection if they are in range. Any unknown requests through a Bluetooth connection should ALWAYS be ignored or declined
- Always switch off a wireless connection when it's not in use. This will ensure that malicious parties can't connect to your device without your knowledge
- Only download mobile applications from authorized application stores like the Apple App Store or the Android Market.
- Keep security software current by having the latest version of OS and apps on devices
- Check all devices connected to your router
- Don't respond to fraudulent texting, calls or voicemails

During this pandemic, the last thing anyone one needs is to have their device compromised. Unfortunately, cyberattacks will continue to increase; hackers are constantly looking for any chance to steal and misuse data. Taking precautionary measures can help protect your devices and all the data they contain.

Sources:
http://techlife.samsung.com/keep-smartphone-being-hacked-1067.html
http://www.computerworld.com/article/2488450/mobile-security/how-to-keep-your-smartphone--and-its-data--secure.html
https://www.digitalunite.com/technology-guides/smartphones-tablets/smartphones/10-top-tips-smartphone-security

How to Keep Your Device Clean

COVID-19 is a respiratory virus that has caused our world to change. It has caused us to interact with each other differently and to take more precaution than ever before. What is top of mind for everyone is protecting themselves, loved ones and colleagues. According to the Centers for Disease Control and Prevention (CDC), cell phones, tablets and laptops are considered “high touch” surfaces. The novel coronavirus may be able to live on surfaces for hours or days. If you touch a contaminated surface then touch your face, the virus could be transmitted to you via your mouth, nose, or even eyes. Because we rely on our devices to work and conduct important daily activities it is critical to ensure those devices are kept clean.

In 2016 a study done by research firm Dscout showed that people touch their phones about 2,617 times a day. The study monitored 100,000 demographically diverse users for 5 days 24 hours a day and recorded every touch on their phones. That study was done four years ago. Undoubtedly, we have become more dependent on our devices since then. Technology has allowed us to conduct more activities on our devices while being mobile, as a result we probably touch our devices more. Couple that with a study done in 2015 by a Sydney university where they observed medical students on video and recorded how many times, they touched their faces. The study observed 26 students and found that each of them touched their face on average 23 times per hour. Of those facial contacts 44% of them made contact with their eyes, nose and mouth which are entry points for most viruses into the body.

These studies show how easy a virus like the coronavirus can spread and why it is important to practice good device hygiene.

<u>First and foremost, always refer to the manufacture’s guidelines for cleaning and disinfecting devices.</u>

If there are no specific guidance, below are a few tips that may help keep your device clean and in turn keep you and those around you safe.

- ⇒ Before cleaning your device, it is always best to turn it completely off and have the device unplugged.
- ⇒ For cell phones, tablets, touch screens, remote controls, and keyboards, remove visible contamination if present.
- ⇒ Use an alcohol-based wipe or spray containing at least 70% alcohol and be sure to dry surface thoroughly to avoid liquid pooling. If you have an Apple device, it is recommended to use a 70 percent isopropyl alcohol wipe or Clorox Disinfecting Wipes to gently wipe the hard, nonporous surfaces of your device, such as the display, keyboard, or other exterior surfaces.
- ⇒ Ensure moisture doesn’t seep into any openings.
- ⇒ Consider use of wipeable covers for electronics.
- ⇒ Refrain from using compressed air.
- ⇒ **Do not use abrasive cloths, towels, paper towels, or similar items.**
- ⇒ **Do not use window cleaners, household cleaners, aerosol sprays, bleaches, solvents, ammonia, vinegar, hand sanitizer or other abrasives.**
- ⇒ **Do not spray cleaners directly onto your phone, or other electronic devices. Spray the cleaning agent on a soft, lint-free cloth when wiping devices.**
- ⇒ **Do not submerge your phone in cleaning agents.**

Disinfecting our devices is **NOT** a replacement for washing our hands. Keep in mind that cleaning our gadgets will provide an extra layer of protection, but washing our hands more frequently with soap and water for 20 seconds is still one of the best ways to protect ourselves from COVID-19, other viruses and bacteria.

Sources:
https://blog.dscout.com/mobile-touches#3Words by Michael Winnick, Visuals by Robert Zolna
School of Public Health and Community Medicine, UNSW Medicine, UNSW Australia, Sydney, NSW, Australia. Electronic address: m.mclaws@unsw.edu.au.
https://www.cnet.com/news/why-its-time-for-you-to-choose-a-cheaper-phone-plan/
https://www.cdc.gov/coronavirus/2019-ncov/community/disinfecting-building-facility.html
https://support.apple.com/en-us/HT204172?mod=article_inline
https://pubmed.ncbi.nlm.nih.gov/25637115/