First Bank & Trust Company

The Bank That Puts You First

Member FDIC

January 2021 Issue 1

What to Expect in 2021

Many are happy to put 2020 behind and welcome 2021 with open arms. But although it's a new year, there is sure to be more challenges we will all face. 2020 was unprecedented and was filled with uncertainty. The pandemic is not over yet and we know bad actors will continue to test the security limits. But we also know technology will be one of the most important tools to help us get through these difficult times. Below are not only some security issues to expect but also technology enhancements that may have an impact on people and businesses in 2021.

- **Phishing as a Service will become more lucrative**-Phishing scams are not going away. It is the easiest and affects the most people. Hackers will continue to profit from these types of scams which will provide incentive for others to develop more phishing kits and sell on the dark web.

- **COVID-19 scams will not stop**-We are still in the pandemic, and cybercriminals are keenly aware of how to take advantage of this moment of insecurity to attack. They will continue to prey on human emotions, using fake information and websites to engage the most unsuspecting victims.

Member FDIC

EQUAL HOUSING LENDER

Virginia Bank Locations

Abingdon, Virginia, East
276-628-3838
Abingdon, Virginia, West
276-628-9558
Blacksburg, Virginia -
540-951-1656
Bridgewater, Virginia
540-246-0003
Bristol, Virginia, East
276-466-9222
Bristol, Virginia, West
276-669-1122
Christiansburg, Virginia
540-260-9060
Fairlawn, Virginia
540-633-3793
Harrisonburg, Virginia
540-434-0671
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
Woodstock, Virginia
540-459-7228
Wytheville, Virginia
276-228-1125
Operations Center
276-623-2265

Tennessee Bank Locations

Bristol, Tennessee
Volunteer Pkwy
423-652-2022
Gray, Tennessee
423-467-9966
Johnson City Tennessee
423-975-9900
Kingsport, Tennessee
423-246-3700

First Bank & Trust Loan Production Offices

Bedford, Virginia
540-583-5458
Hanover, Virginia
804-550-5700
Lynchburg, Virginia
434-509-0444
Roanoke, Virginia
540-774-0269
Rocky Mount, Virginia
540-484-0338
Winchester, Virginia
540-545-8110
Wytheville Annex

First Bank & Trust Mortgage Lending Division

Bristol, Virginia
276 -644-9900

Continue on Page 2

- **VPN's will be a targeted-**Virtual Private Networks (VPN) has allowed remote workers to have some sense of security. But hackers know if they can penetrate a VPN, they have an open door to a company's network. With that type of access, they can steal credentials that perpetuate other types of forceful attacks including Ransomware attacks. Cybersecurity professionals believe the targeting of VPNs will ramp up in 2021.

- **Ransomware Attacks will target the most critical assets of an organization**- In a recent Fireye report called "A GLOBAL RESET Cyber Security Predictions 2021" it highlighted the ongoing concern of Ransomware attacks and how it is now a national security concern. Ransomware attacks increased in 2020 and they believe will only get worse. These types of attacks can have dire effects especially in the healthcare sector where not having access to hospital systems can have life or death consequences on patients.

- **5G**-COVID-19 has accelerated the need for faster and more reliable connectivity. In 2021 this will become increasingly important to help businesses maintain their workforce.

- **Augmented Reality (A/R)-** A/R is an interactive experience of a real-world environment where the objects that reside in the real world are enhanced by computer-generated perceptual information.COVID-19 has required certain sectors to think outside the box to continue business as usual while still trying to lower the transmission of the virus. The education sector will benefit from this technology allowing students to still get their education by reducing the need for crowded classroom conditions.

- **Cloud Security**-Migrating data to the cloud was always in the works. Many companies were already slowly making the transition. However, due to Covid-19 it has accelerated. Because of the rapid change some security expert believe there may be gaps that can be exploited by cybercriminals. 2021 will bring a major emphasis on cloud security.

- **Artificial Intelligence (A.I) will grow**- A.I is the ability to build smart machines capable of performing tasks that typically require human intelligence. Because of the pandemic the demand for A.I is expected to increase and will be seen as a helpful tool to help healthcare professionals detect and stop the spread of COVID-19.

While threats continue to evolve, and cybercriminals employ new strategies there are also new innovations being developed to help our healthcare professionals, educational sector and the business world get through the pandemic. There is definitely a new normal, but if 2020 has taught us anything, it is to expect the unexpected in 2021.

Sources:
https://www.eweek.com/innovation/eleven-important-tech-trends-to-expect-in-2021
The 5 Biggest Technology Trends In 2021 Everyone Must Get Ready For Now (forbes.com)
https://www.inc.com/anis-uzzaman/top-business-technology-trends-in-2021.html

Text Message Scams on the Rise

Text message has been the go-to for marketing and has benefited every industry. Most people always have their phone in hand, and sending a text is more useful than sending an email. Businesses and even our government have taking advantage of using text messages to get their messages to people quickly and more efficiently. Studies have shown that majority of incoming text messages are opened within 15 minutes of receipt. Hackers are well aware of this and they too take advantage of being able to contact their next victim via text message.

Text message or SMS (short message system) phishing is also called "smishing". Smishing occurs when scammers use fake text messages to entice consumers into providing their personal or financial information. The scam artists that send smishing messages often impersonate a government agency, bank, or other company to lend legitimacy to their claims. Smishing messages typically ask consumers to provide usernames and passwords, credit and debit card numbers, PINs, or other sensitive information that scam artists can use to commit fraud. They also provide dangerous links in hopes the victim will click on it providing them easy access to their data.

These types of attacks are on the rise and like other scams the goal is for it to look legitimate. But don't be misled. Here are a few things to remember:

⇒ **No government agencies, banks, and other legitimate companies will ever ask for personal or financial information, like usernames, passwords, PINs, or credit or debit card numbers via text message.**

⇒ **Never click on links in unsolicited text messages. Clicking the link may infect your mobile device with a virus or malware designed to steal the personal or financial information stored on the device.**

⇒ **Don't respond to smishing messages. Not even to tell the sender to stop texting you. Responding to smishing messages verifies that your phone number is active and that you are willing to open such messages, which may lead to an increase in the unsolicited text messages you receive.**

⇒ **Be selective to whom you provide your cell phone number to in response to pop-up advertisements and "free trial" offers. This personal information can be easily bought, sold, and traded, and make you a target for smishing scams.**

⇒ **Don't be fooled by the sense of urgency in an unsolicited text message. Smishing scams attempt to create a false sense of urgency by implying that an immediate response is required.**

Your cell phone essentially has the same capabilities as your computer or laptop and thus the same safety and security practices should be used. Always keep your security software and applications up to date and be extremely cautious of text messages from unknown senders.

Sources:
https://about.att.com/pages/cyberaware/ae/smishing
https://www.ag.state.mn.us/consumer/publications/TextMessagePhishing.asp