First Bank & Trust Company
Member FDIC

Volume 4, Issue 6

June 2018

INSIDE THIS ISSUE:

Member FDIC EQUAL HOUSING LENDER

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

KIDS ONLINE SAFETY TIPS

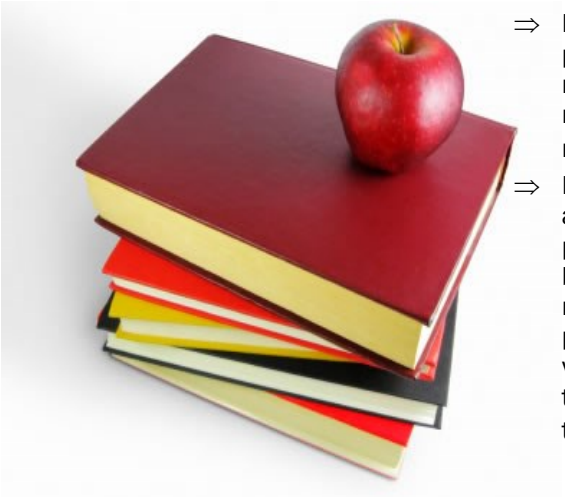
Another school year is over for many students around the country. Parents and teachers are breathing out a collective sigh of relief that they made it through another term, while kids are excited at the thought of not having to follow strict "school night" rules as they did throughout the school year.

This summer, some kids will be going to camp or going on family vacations, but many will be at home enjoying sleeping in and more time to play around on their mobile devices. Internet safety and mobile device safety are popular topics, but it's not that often that the topics focus on children specifically. Let's face it: the average five-year-old is most likely more tech-savvy than his or her parents, and criminals make it a point to know this. That's why it is more important than ever to discuss how children interact and behave online.

Technology has played a major role in how kids today learn and that has been a positive thing. Kids can now virtually see the world, and with the help of social media, stay connected to friends, family and even teachers! But there are some disadvantages to this constant access to information. Although they may seem to know a lot about the Internet, children are still very vulnerable to the dangers of the online world and can easily become victims of online criminals. It is important to educate kids on how to spot phishing scams or links that can potentially carry harmful viruses or malware and to keep personal information secure.

Below are a few tips to help keep children safe while they are online.

⇒ Know what social media sites kids are on. Make sure privacy settings are set on those sites to limit access.



⇒ Privacy. Talk to kids about the dangers of putting personal information on the Internet, such as names, addresses, phone numbers, birthdays, etc. That type of information is a goldmine for cybercriminals.

⇒ Know what is appropriate to post. For example, posting a picture to a social media page may seem harmless, however, embedded in that picture are GPS coordinates which are stored as metadata in the picture file itself. This information provides the exact location of where the picture was taken. This setting needs to be turned off on all devices.

- ⇒ Use software that helps block certain sites that are not appropriate for children.
- ⇒ File Sharing also known as Peer to Peer (P2P) file sharing. Kids sometimes share music, apps or video games with their friends, but if not done properly and with the right guidance, kids may accidentally share other personal files, files that are corrupted or have malware attached or even download copyrighted material which is illegal.
- ⇒ Teach kids about phishing scams and how to be wary of deals that seem too good to be true. Show them signs to look for such as misspelled websites or pop-ups that claim they won a prize such as 100 lollipops or Xbox video games.
- ⇒ Explain the consequences of clicking or downloading potentially harmful links and the chain reaction that can have a multitude of negative effects.

The Internet plays a huge role in all our lives, including kids'. Make sure they have the appropriate tools and knowledge to enjoy their online experience safely during the summer and beyond!

Sources:
https://www.consumer.ftc.gov/topics/protecting-kids-online

Five Ways Businesses Can Control Data Leaks

Technological advancements have made working in the business world easier than ever. Long gone are the days of having to set up physical meetings or only communicating via the telephone. We now have the ability to do web calls with participants from all over the world, our smartphones allow us to stay connected at all times and we have the capability to access and share documents with virtually little or no downtime. This is the beauty of technology; allowing us to work smarter not harder. But along with these exciting benefits of technology also come the real possibility of data leaks.

A data leak is an unintentional or intentional release of private and/or confidential information that is pertinent to a business. The information can be copied, shared, viewed, stolen or used by unauthorized parties. Data leaks can occur while the data is moving through its different stages.

Data has three different stages:

1. ***While in transit.*** *Our data travels in different ways such as email, web chatting, internet use, etc. Data in transit is information being moved from one point to another.*
2. ***At rest.*** *When data is at rest it is usually information that is fixed on the device such as files saved to a desktop or information that is stored on a hard drive.*
3. ***In use.*** *Data in use is data that is stored in memory or a database, data that is processing or data that is inputted.*

Understanding the above stages of data will help businesses to categorize their data and ensure that all information has the appropriate levels of security.

Here are five ways organizations can help avoid the pitfalls of falling prey to data leaks.

1. **Encryption.** All sensitive data should be encrypted. Encryption disguises information to make it unreadable to those who the information is not intended for. Many types of organizations have mandatory encryption laws that are enforced by regulators.
2. **Make sure endpoint protections are in place.** Endpoint security is a technology that provides an additional layer in protecting computer networks from having malicious code downloaded from any source. The goal of endpoint security is to help ensure there are no gaps and that all devices maintain a level of compliance and standards that help protect a network's sensitive data; data such as a customer's private and financial information which can be devastating if in the wrong hands.
3. **Email Controls.** Make sure measures are put in place to scan incoming emails for text, images and attachments that may be harmful and have viruses, malware or anything nefarious. Email controls will flag if confidential or sensitive information is being transmitted from an internal source via email as well.
4. **Firewalls are a must.** Firewalls are a necessary component to help ensure an organization's network is secure. A firewall's main objective is to block unwanted traffic from penetrating networks with malicious viruses, worms and any other threat. Having firewalls in place can help protect and enhance an organizations network security.
5. **Know who has permissions.** Managing who has permission to read, change or modify files is important for keeping files secure.

Sources:
http://bigdata-madesimple.com/15-ways-to-prevent-data-security-breaches/
https://www.computerworld.com/article/2553217/security0/six-