MAY 2019
ISSUE 5

UNION BANK

Mobile Banking App is HERE!

Inside This Issue

EQUAL HOUSING LENDER Member FDIC

5 Interesting Facts About IoT

If you don't know what IoT is, some may say you have been living under a rock. IoT, or the Internet of Things, is basically the remote control to our daily lives...how we "stay connected." And let's face it, being continuously connected is the norm now.

The Internet of things is the extension of Internet connectivity into physical devices and everyday objects. Embedded with electronics, Internet connectivity, and other forms of hardware, these devices can communicate and interact with others over the Internet, and they can be remotely monitored and controlled.

It is important to understand the magnitude and influence of IoT as it is not going away, and only getting more creative and more robust. Here are five interesting facts that everyone should know.

1. **Your home is probably a lot smarter than you!** Amazon Echo has changed the game. By just a simple voice command, Alexa can tell you anything you want to know. Alexa can also be programed to assist with a multitude of household appliances and devices such as your coffee maker and alarm system.

2. **Soon there will be a smart city near you!** It turns out that not just homes can be outfitted to be smart, but so can cities! If your city has not already started the transition, there is probably one near you that has. Many cities are looking at how to implement IoT within their infrastructure, from transportation to energy sources.

3. **IoT is winning the race.** Its hard to keep up with technology. Literally every year cell phone manufacturers come out with the latest and greatest devices that are always more advanced than the last. But regulations struggle to manage the technology of these advancements and have found implementing policies to keep up with the pace of technology challenging.

4. **IoT is getting bigger.** From its inception in 1982 with a modified Coke vending ma-

Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
Kroger Plaza 19 Acme Street Marietta, OH 45750
740-374-0010
This is not a full service location. Deposits/withdrawals cannot be processed at this location.

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155
304-455-2967

chine at Carnegie Mellon University, IoT has been modified greatly. The capability is somewhat endless. There are more things connected to the internet than there are people in the world! It was calculated in 2017 that there were around 8.4 billion IoT devices, up 31 percent from 2016. And this will likely reach 20.4 billion by 2020.

5. **Don't forget about your car.** I know it's hard to imagine but yes, cars are going smart too. Experts estimates that 90% of automobiles will be connected to the internet by 2020. Many of the car manufactures have invested billions on research and development to create driverless cars. Look no further than the strides Elon Musk has made with is Tesla brand. Although you do not see them on the highways now, there is a string possibility that will happen sooner rather than later.

One of the biggest drawbacks with using IoT for your personal use or business is, of course, security. But making sure proper security measures are in place can significantly reduce threats and potential breaches. This will become the new normal. Learning how to embrace, manage and balance IoT usage will be key.

Sources:

http://iotinfluencers.com/5-things-to-know-about-the-internet-of-things/
https://www.vxchnge.com/blog/iot-statistics

Wikipedia, https://en.wikipedia.org/wiki/Internet_of_things

Data Security Tips

5 Ways to Handle Potential Security Threats

Safe security practices are still at the forefront for many Chief Information Officers (CIOs) and IT professionals. It is definitely the most thought about issue that many tend to lose sleep over. The reality is, just by conducting business online, any company can suffer a breach in data security. We know…no organization can be completely protected. It is true, though, that with an appropriate plan and strategy in place you can reduce the potential of a data breach and theft of information, or at least minimize the negative impact such acts can have on a company and organization.

Here are five ways that can help companies and organizations prepare to handle a potential security threat.

1. **Securely archive and/or delete data you no longer need** - Data is a hot commodity and typically can be sold on the dark web to the highest bidder. Good housekeeping includes getting rid of data that is no longer needed by encrypting it and moving it to offline storage or just deleting it all together. This minimizes the amount of data that is exposed to an attacker.

2. **Monitor EndPoint devices** - The number of devices that are connected to a network is expected to surge this year. It is imperative that IT departments actively identify, monitor and control any devices that attempt to access corporate information. Conducting regular audits to review the access and permission levels to critical systems for employees and contractors will help mitigate risk. Being able to have visibility of these devices are now a necessity.

3. **Have a plan for Data Extortion** - Financial institutions especially, face a variety of risks from cyber attacks involving extortion, including liquidity, capital, operational, compliance and reputation risks, resulting from fraud, data loss, and disruption of customer service. Companies and organizations should conduct ongoing information security risk assessments and maintain an ongoing information security risk assessment program that considers new and evolving threats to online accounts and adjust customer authentication, layered security, and other controls in response to identified risks. In the event a data extortion attack should a occur, you should be able to react quickly to minimize the damage. Make sure to work with all departments of your company and organization such as IT, human resources and legal departments to have a plan of action that addresses these types of scenarios. Also reach out to local and federal law enforcement agencies to ensure all your bases are covered.

4. **Social engineering** - Employees need training on how

to avoid social engineering attacks. Training employees on cyber security best practices and how to mitigate problems when or if they occur is one of the best defenses against cybercrimes. Social engineering attacks are becoming increasingly more sophisticated and can fool the savviest employees. Making sure employees know what phishing, elicitation and impersonation attacks look like and how they are used is essential. It is also equally important to provide ongoing support to make sure all employees have the resources they need.

5. **Test your security** - One of the best ways to look for vulnerabilities is to audit your own system. Mimicking an attack on your own network helps look for gaps and weaknesses. Changes and improvements can be made from those results and can help organizations take an active role in their protection.

We know companies will continue to face challenges in this arena and the solutions are never "one-size-fits-all." However, implementing these tips and having a plan of action can make a significant impact on the outcome should a cybercriminal get their hands on your data.

Sources:
https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe
https://security.berkeley.edu/resources/best-practices-how-to-articles/top-10-secure-computing-tips
https://smallbiztrends.com/2017/01/data-protection-tips-for-data-privacy-day-2017.html