In this issue:

**The following content is provided courtesy of Horsesmouth, LLC, and provided courtesy of Miles Harris.*

This month we'll be talking about cybersecurity lessons for kids. Read on for more information on that, as well as:

- The T-Mobile data breach affecting 40 million customers
- Government agencies failing cybersecurity standards
- The biggest cryptocurrency hack
- And much more

Back to School: 4 Cybersecurity Lessons

Notebooks, pencils, password managers? As we begin the back-to-school season, it is important to review good cybersecurity practices with school-aged children. Whether school is virtual or in-person, many aspects of education now use the Internet as a learning tool. Here are some cybersecurity topics to discuss with your kids or grandkids before they head back to school.

1. The power of passwords

One area of cybersecurity that most children have been exposed to already is creating passwords. Many kids have a password for some sort of account. And many more may need to create passwords for school accounts this year. Be sure your kids understand the importance of creating strong passwords—especially if they are protecting personal information.

You may want to share some of these password techniques so kids can begin creating their own unique passwords that are tough to crack but memorable.

- **Mnemonic device password:** Your child is likely already familiar with mnemonic devices to remember the order of the planets or the color of the rainbow. They can use this same technique to create a strong password. Encourage them to take a line from a favorite song or book and use the first letter of each word to create a password. This will be easy for them to remember, but tough for a hacker to crack.
- **Goal setting password:** Does your child have a goal for the school year? Maybe they want to make the soccer team? Or get straight A's? Keep this goal front and center by turning it into a password! Every time they type their password, they'll get a boost of motivation towards that goal.

2. Back up data

If your child is of an age where they are writing reports on a computer, you should teach them about the importance of backing up their data. Ransomware and simple mistakes can lead to documents being deleted before they are turned in for a grade. Consider setting up a Dropbox, OneDrive, or Google Drive

account with your child so they can save all of their important documents to the cloud in addition to their physical device.

This is an important cybersecurity practice for kids to learn at a young age since ransomware has become such a prominent cybersecurity threat. Having a backup of their files means that even if they do fall victim to a ransomware attack, they'll be able to access all of their files on the cloud.

3. Protect personal information

Kids should understand what personal information they should think twice before sharing online. You can help your kids decide if a particular app or website should know things like their birthdate, address, and full name.

For younger kids, you'll probably want to review this on an account-by-account basis. Older kids may have a better understanding on their own.

4. Keep devices up to date

Lastly, kids should be taught to keep all of their devices and apps/programs up to date. Many cybersecurity incidents occur due to outdated software that is exploited by hackers. Talk to your child about checking their computer, iPad, or phone for updates regularly. This will help keep their devices safe and working properly.

This time of the year is a great time to review cybersecurity actions with kids, as they might have new devices. Talking to your kids regularly about cybersecurity will help keep them safe and begin to learn how they can protect themselves online. (Keep in mind that this advice is good for people of all ages!)

Emerging threat: T-Mobile Data Breach

More than 40 million T-Mobile customers have had their personal information exposed in a massive data breach. The cell phone provider reported that its computer networks had been breached resulting in information such as names, birth dates, Social Security numbers, and driver license information being stolen. Active T-Mobile customers as well as individuals who applied for credit with T-Mobile are believed to be affected.

At this time, T-Mobile says that no phone numbers, account numbers, PINs, or financial information of customers were exposed. However, phone numbers and PINs for pre-paid plan customers were stolen. T-Mobile has reset the PIN codes of those affected. All T-Mobile customers should consider changing their PIN and password information.

Cybersecurity shorts

Three cybersecurity challenges for remote work. Remote work has been extremely helpful over the last year and a half. It also has major advantages for both employees and employers. However, from a cybersecurity perspective, major challenges persist that are extremely important for businesses to recognize and address. Forbes outlines the top three issues here.

Multiple federal agencies fail to uphold cybersecurity standards. Agencies across the federal government continue to fail to meet some basic cybersecurity standards. With the rise of hacks and ransomware cybersecurity incidents, multiple agencies have failed to effectively secure data, a senate report has stated.

U.S., UK, and Australia team up to issue joint cybersecurity advisory. The three cybersecurity agencies and the FBI came together and issued a joint cybersecurity advisory that announced the top 30 exploited vulnerabilities throughout 2020 and 2021. In this issue, they noted that government-

sponsored and independent malicious cyber attackers continued to exploit publicly known software vulnerabilities where the intentions were to compromise governments globally.

Covid-19 isn't the only virus employees could bring back to the office. Many IT leaders believe that employees have picked up bad cybersecurity habits while working from home due to the Covid-19 pandemic. With 40% of employees plan to bring their personal computers back to the office with them, IT decision makers are becoming more worried remote workers will bring in infected devices and malware. You can read more about that here.

Employee Benefits Security Administration (ERISA) covered plans are tempting targets for cybersecurity hackers. Recognizing this, ERISA (a part of the Department of Labor) issued its very first cybersecurity guidance concerning employee benefits this past spring. You can learn more about their focus on cybersecurity here.

Businesses need cybersecurity protection. With ransomware attacks getting worse, cybersecurity is no longer an option for businesses. A recent survey found that 51% of businesses in America were hit by ransomware attacks in 2020 alone. Ransomware is not going away anytime soon and although crimes of this nature are almost inescapable, protecting yourself and your business is important. Read Forbes' article on why cybersecurity is no longer optional for businesses.

Pegasus Spyware is a cybersecurity danger. Pegasus, spyware that can sneakily enter a smartphone and gain access to everything on it, including the camera and microphone, has been created to infiltrate devices running Android, Blackberry, iOS, and Symbian operating systems which are then turned into surveillance devices. Pegasus has been built solely for governments to use in counterterrorism and law enforcement work.

$600 million of cryptocurrency stolen and then returned. An unidentified hacker stole $600 million worth of virtual currencies from Poly Network. But 24 hours after the incident, something unusual happened – the hacker began to return some of the stolen money after the company made a public plea. Click here to learn more about the incident.

Multiple ransomware groups jump at PrintNightmare's vulnerability. The vulnerability in Microsoft software has started to turn into a dream for ransomware gangs. For the second time within a week, security researchers warned that extortionists exploited the critical flaw in an attempt to lock files and shakedown victims. Vice Society, a ransomware group recently seized on the PrintNightmare bug to move through an unnamed victim's network and attempted to steal data.

Software updates

Microsoft: Over 40 security vulnerabilities were patched in this month's Microsoft release. One of these security issues, which is responsible for patching Windows 10 PCs is already being exploited. Microsoft users should update their devices as soon as possible. You can learn more about the updates here.