

Technology Today

"Insider Tips To Make Your Business Run Faster, Easier, And More Profitably"
Since 1984



What To Know BEFORE Your Laptop Gets Lost/Stolen

Imagine you're in the airport. You set your laptop down for a minute, and the next second...your laptop is gone. It's not in sight, nor is the thief who stole it.

If you have a password on your laptop, that will likely prevent the thief from immediately having access to your private documents. What it doesn't stop is someone removing the hard drive from your laptop and connecting it to another computer – suddenly your hard drive is sitting there, ready to browse – just like any other folder or drive letter.

What do you do? Encrypt it! A good first step toward protecting the hard drive of your laptop and other mobile devices is to encrypt it. With the drive encrypted, a thief can't just pull it out, hook it up and suddenly have access to all your files. And, if you have our managed encryption solution, we can remotely wipe all your data.

July 2021



This monthly publication provided courtesy of Ryan Haislar, President of Computerease.

"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"



How One Compromised Password Caused Colonial Pipeline's Shutdown From Ransomware

Colonial Pipeline, a company with a 2020 annual revenue of \$1.32 billion, fell victim to a ransomware attack from a single compromised password. Despite spending \$200 million over the past 5 years on total IT costs (including cybersecurity), the cybersecurity protections in place fell short and left the company vulnerable for a cyberattack. This article will explain two aspects of cybersecurity, multi-factor authentication and the dark web, that played a role in Colonial Pipeline's ransomware attack.

The aftershock of this ransomware attack reverberated through the southeast part of the country, shutting down a main gas supply line for the entire east coast. There were runs on gas stations causing shortages, and increased prices.

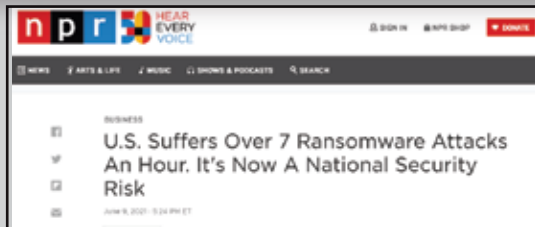
When a cyberattack happens, it's not just the company that feels the effects. Colonial Pipeline faces investigations, fines, lawsuits, reputational damage, lost revenue, and immense financial losses. This cyberattack is a national crisis!

All this damage was caused by a single compromised password. Colonial Pipeline Chief Executive, Joseph Blount stated in his testimony to a U.S. Senate committee, "It was a complicated password, I want to be clear on that. It was not a Colonial123-type password." Security experts don't know the exact way the Colonial Pipeline password was compromised. However, most compromised passwords are easily accessible on the dark web, a black market for stolen credentials.

<continued page 2>

Get More Free Tips, Tools and Services At: www.computer-service.com
(314) 432-1661 (MO) or (618) 346-8324 (IL)

Ransomware Epidemic Makes National Headlines



<continued from page 1>

What exactly is the dark web?

The dark web is a portion of the internet that is only accessible to the most advanced internet users. There are some legitimate parts of the dark web, but the majority is illicit activity. You can purchase passwords for corporations, social media platforms, bank accounts, and any website needing a password. Credit card numbers, drugs, guns, and counterfeit money can be purchased as well. It's also possible to hire hackers or purchase a ransomware virus to attack a computer or network yourself.

For a hacker, there's endless possibilities with information available on the dark web. In the case of Colonial Pipeline, once they got hold of the compromised password, there was nothing holding them back.

Multi-Factor Authentication Could've Stopped The Attack

Once hackers got their hands on a compromised password for Colonial Pipeline's system, they had unlimited access. The password was used for a legacy VPN (virtual private network) system that allows remote access to a computer or network. In the IT world "legacy" means an older version of a system that's not been upgraded. In the case of this legacy VPN system, the only access required was through a password.

Updated VPN systems operate with multi-factor authentication, an industry-recommended cybersecurity measure. In multi-factor authentication, another step is involved to be able to access a system. Typically, a cell phone text message code, key fob, or authentication app is used as the second layer of security. A person accessing a system with multi-factor authentication enabled needs BOTH the correct password, and the correct code from another source.

Large Corporations and Small Businesses Face The Same Cybersecurity Risks

There's many differences between a large corporation like Colonial Pipeline and your business when it comes to cybersecurity. Colonial Pipeline has access to more financial resources and there was a nationwide impact from them shutting down. Government agencies sprang into action to come to their aid. If and when you are faced with a ransomware attack, you might have some support from local law enforcement however, you won't have the same support from the FBI like Colonial Pipeline.

Unfortunately, your business is equally at risk for hackers. Artificial intelligence and bots have multiplied threats previously perpetuated by individual hackers. Cyberattacks are systemized and prolific, meaning that every single computer and network is at risk. Hacking rings like Darkside are motivated by the huge rewards and financial gains from cyberattacks. It's a VERY profitable business!

Some business owners aren't sure about where to start for cybersecurity. It can be overwhelming to think about all the different vulnerabilities facing your business, so they just push it off. Colonial Pipeline pushed off implementing a multi-factor authentication security step for their legacy VPN system.

The first step to improving your cybersecurity strategy for your business is to get a baseline for your existing vulnerabilities. We offer free dark web scans for our clients to determine if any of their passwords are for sale on the dark web, so that they can be changed ASAP. Also, we offer free cybersecurity awareness training for our client's employees so that they can be aware of risks of a cyberattack.

As an owner of a 2nd generation family-owned business, I'm dedicated to helping entrepreneurs protect everything they've built. I'm offering a free dark web scan and cybersecurity awareness training to any business owner who wants to take a step towards protecting their business. It's incredibly important for all business owners to learn lessons in cybersecurity from scary stories like the Colonial Pipeline hack.

Dark Web Breach Assessment & Cybersecurity Training

- Scan the Dark Web to assess risk
- Train your employees about cybersecurity
- Reduce your chance of a data breach

Visit: www.computer-service.com/dark-web

*Get More Free Tips, Tools and Services At: www.computer-service.com
(314) 432-1661 (MO) or (618) 346-8324 (IL)*

Shiny New Gadget Of The Month:



Your Car Companion: FIXD

When you're driving, there's one thing you hope to never see: the Check Engine light. This symbol often means that something is wrong, but it's rarely clear what that is. Well, here's a little help: FIXD!

FIXD is a small device that connects to your car's onboard diagnostic (OBD) port. Every car built after 1996 has this port - it's what mechanics use to diagnose vehicle issues when a dashboard light comes on. You can use it too, so you won't have to rely on a mechanic to tell you what's "wrong" with your car. FIXD wirelessly connects to your smartphone and tells you directly. Then, you can decide what to do!

Say goodbye to the mysterious Check Engine light and say hello to FIXD. Learn more at bit.ly/3alSXwy.

Soft Skills, Solid Results

Parenting seems unrelated to business, but in my experience, it is very much related to people skills - and people skills are necessary for business. There are four key people skills, often called "soft skills," that I want to talk to you about:

- Gratitude
- Listening
- Grace By Margin
- Vision

Gratitude

How do you feel when you get a thank-you note? People never forget when they get a handwritten thank-you note. A text or e-mail is nice, but they last a day. People love to feel gratitude. They love to share it and to receive it. Thank-you notes remove barriers, so make it a habit.

Listening

Listen longer and listen better. When you're speaking with someone, encourage long pauses. Let the silence do the heavy lifting. You don't have to rush into an answer or response before thinking about what a person is saying. This is helpful in sales and with direct reports. Allow yourself to stay quiet so the other person can do the talking. Don't be afraid to ask open-ended questions like "How did that go for you?"

Grace By Margin

This is all about things that save you time. Consider using the "while" system as a way to multitask. For example, place an under-the-desk bike to work out while you work at your desk. Another thing to consider: timed e-mails. Schedule an e-mail to be sent out at a specific



time and add links in e-mails to schedule time on your calendar. One more time-saving tool is speech-to-text transcription. This ensures you have a record of every conversation that you can reference as needed.

Vision

Break down your vision into small parts. Instead of feeling overwhelmed by something large, choose one smaller goal for the month. Do this with everyone in your organization. Break down everyone's goals into smaller parts. This makes it easier to track over the course of a quarter or year. Even go as far as creating a vision board. Add images of what you want to achieve. Make your vision visual. Lastly, write down your achievements as part of your vision. Where are you now and where do you want to be over the next three years?

P.S. Don't forget to check out the "Soft Skills, Solid Skills" Petra Coach webinar at PetraCoach.com/soft-skills-solid-results-with-bea-wray.



Bea Wray is an entrepreneur, innovator, mentor and author of What An MBA Taught Me... But My Kids Made Me Learn. She founded (and sold) SourceHarbor Inc. and has consulted with over 300 companies around the globe. She's the former chair of ForbesBooks and has hosted The Front Porch podcast, Savannah's: Engage SGTV, TEDx and the GeekEnd Innovation conference. With years of experience and an MBA With Distinction from Harvard Business School, she's always on the lookout for the next opportunity.

■ As A Business Owner, Are You Ready For The IT Future?

Over the past year, countless businesses moved to a remote work or hybrid model. It also meant these businesses had to change the way they operate, including a sweeping shift to cloud-based services and a renewed look at their IT security. But despite these changes, many businesses aren't where they need to be. There are still gaps in their cloud infrastructure and security. How do you fill those gaps?

Put a greater emphasis on endpoint security and monitoring. As much as you need solid IT security on your end, every employee needs solid IT security on their end as well. Not only does every device need endpoint security, but you also cannot forget about performance monitoring. This gives you the ability to see threats and potential threats to your network in real time, which means you can react accordingly and stop potential attacks or hardware failures. As

you work with your IT security partner, discuss monitoring options and give yourself one more tool in the protection of your organization. *Forbes, April 15, 2021*

■ 3 Key Ways To Keep Your Business In Growth Mode

1. Talent. You must hire a team willing and able to meet the challenge of growth. You want people who are not only talented in their field, but who also fit within your company culture, who are eager to learn and ready to solve problems, and you have to be just as willing and able to reward them for their talent.

2. Innovation. When you have a talented team at your side, innovation comes easier. You need to continuously develop products and services that customers want to buy. Understand your customers and their problems at the highest level so you can bring solutions to the table.

3. Accountability. As your team and business grow, you must put greater emphasis on accountability. Track everything and have key performance indicators (KPIs) attached to every goal and project. But don't just hold people accountable to meet certain goals – hold them accountable when they succeed; that is to say, make sure the wins are celebrated along the way. *Inc., April 8, 2021*

■ Are You In The Cloud Yet?

Some businesses have tried to avoid the cloud. There are lingering fears that cloud-based services aren't as secure as their non-cloud counterparts. However, cloud services are more prominent than ever, and service providers are fully aware that they must meet the IT security needs of today.

For those businesses still unsure, it's estimated that 97% of businesses already use cloud services. You might not realize it, but cloud services are in the mainstream. Even businesses that are hesitant to join the cloud may already be a part of it. Most e-mail and communication apps are cloud-based. If you use virtually any Google or Microsoft service, you've joined the cloud.

The bottom line is that digital security is top priority for cloud platforms. Not only do these providers need to meet the requirements of their clients, but they must also follow international rules and regulations. If you want to keep your data backed up and secure, the cloud is your answer. *Forbes, April 1, 2021*



"He opened his email and saw the attachment from an unknown source. His hand slowly reached to click on the paper clip. He had no idea what horror awaited him..."