September 2021

TechTidbit.com

brought to you by Tech Experts

Lessons Learned From The Colonial Oil Pipeline Attack

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

May 6, 2021 will be a day that goes down in history. This is the day the Colonial Oil Pipeline went down, causing a nationwide disruption. Even though the pipeline only services a portion of the east coast, the effects of the shutdown was felt across the country.

Gas prices skyrocketed, lines at gas stations were so long it took hours to get through, and gas stations were pumped dry as people bought gas and put it in whatever container they could gather just to assure themselves they would have enough to get through the closure.

If you think about it, this type of ripple effect is not confined to energy and utility providers. While the scale of the effect would not be at the level of the pipeline, the devastation it could leave in its wake for your business and your customers is just as likely.

What's the big deal?

To start - part of what rocked many in the cybersecurity industry is that no matter the size of your business, or the expertise of your cyber professional staff, no one is immune to an attack. These malicious hackers are so well-funded (some even by their government as was the case with Colonial) and highly-skilled that it is like playing whack-a-mole with all the best cybersecurity best practices.

As soon as you patch a hole, they find another and the game begins again. So the problem is deeper than just improving cybersecurity. However, there are things you can do that can reduce the risk of falling victim to a cyber attack.

Effective password management

Initial surveys are suggesting that one of the biggest problems with Colonial Oil's cybersecurity was inadequate passwords. Cypress Data Defense lists some of the biggest password mistakes that open your network to increased risk.

They are: weak passwords, using the same password across multiple sites, or password recovery systems with generic authentication questions (i.e., birthday, pets name, etc). Some ways to counteract potential password problems are to enforce strong passwords, set up two-factor authentication, encrypting system passwords, and installing stronger authentication rules for lost passwords.

Outdated software

Another problem found for Colonial Oil was that an outdated version of Microsoft Exchange was still in service, creating an opportunity for unknown users to access their network.

In early March, Microsoft announced four vulnerabilities on the Exchange server that syncs email and calendar functions. This "gap" allowed hackers to gain access to users' email accounts and install malicious code on the organizations' servers.

While Microsoft reacted quickly and developed patches for the gap, it's clear that Colonial Oil did not update theirs in time. his is why updating software is so important and needs to be done proactively and frequently.One of the best ways to counteract this risk is to set a schedule of when you will perform routine software updates to minimize the disruption to your employees but help you maintain effective security for your network.

Lack of cyber education for employees

Phishing attacks have increased by 11 times since 2016, according to the FBI, and nearly doubled from 2019 to 2020. 96% of phishing attacks are delivered via e-mail and 74% of attempts in the US are successful, highlighting the significant need for thorough, effective staff cyber security education.

The challenge remains…

Cyber criminals are increasingly

Continued on page 4

Phishing attacks have increased by 11 times since 2016, according to the FBI, and nearly doubled from 2019 to 2020. 96% of phishing attacks are delivered via e-mail and 74% of attempts in the US are successful, highlighting the significant need for thorough, effective staff cyber security education.

An Easier Way To Secure Your Password

"A password cracker will break "Password" the same as it will break "ushtGsgt." The second example will just take a little longer to crack because programs try common words and phrases first, then start brute-forcing every combination."

Mark Funchion is a network technician at Tech Experts.

Between new threats and new tech, security is something that can always be improved upon to make sure your systems are as secure as possible. Passwords are the first level of security, and the area that seems to cause the most headache for end users and IT managers.

In an ideal world, every password would be super complex. For example, a 32-character randomized password with capital letters, lowercase letters, special characters, and numbers. This is possible with a password manager – or if you're really skilled at memorizing random character strings (unlikely).

The reality is that this does not occur, leading to most of us using a password that is not as secure as hoped. There are a few ways that attackers gain access to our passwords, and the most common methods are an algorithm that "cracks" the password and guessing. Usually, these two are combined, creating databases that nefarious individuals can use for gaining access to your accounts.

The biggest issue with passwords is the human factor. We like things to be simple, so we use things that are familiar. When we have to change a password, we change it in predictable ways, and usually write it on a sticky note.

Let's look at "Password" as a password. Yes, it's terrible, but really, it's eight characters with one capital letter. A password cracker will break "Password" the same as it will break "ushtGsgt." The second example will just take a little longer to crack because programs try common words and phrases first, then start brute-forcing every combination.

Again, looking at human nature, if one hundred people are asked to make the word "Password" harder to guess, most will swap the "o" for a zero. That's then added to the list of words and phrases checked first. If the same one hundred people are asked to add a special character and a number, most will probably create something like "Password1!"

Why? Because it is easy to remember, and the "1" and "!" are convenient. Since so many of us will use the same variations of passwords, these become common and therefore are more easily broken.

These reasons are why it's recommended to use three uncommon, unassociated words as a password (and to not use that combination for all your passwords). For example: "GiraffeDiamondCoffee." An algorithm will still crack this eventually, but it's easier to remember and not easily guessed so it will take a while to crack.

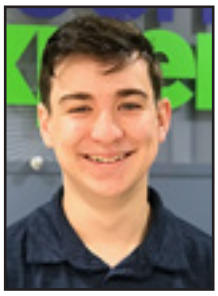
The longer it takes, the less likely they will actually get to your data. By using three different random words for your passwords, it is much less likely that your combination of words ends up in the frequently used list, adding more security. You can also easily add numbers and special characters to meet security requirements as needed.

The best practice is to use a password manager and use super complex passwords. Otherwise, using three-word passwords like "GiraffeDiamondCoffee" can boost your security. It may look easy – but it is a 20-character password, so it's more secure than "P@$$w0rd1!"

Computers that are cracking passwords will try every combination and can test over 100-million per second, so a 10-character password (even with numbers and special characters) only has so many combinations. However, a 20-character password using only capital and lowercase letters like "GiraffeDiamondCoffee" has even more. While the second password seems much easier to crack to the human eye, it's much more complex in reality.

Do yourself a favor: change how you create your passwords and make your information that much more secure – without making it impossible for you to login to your applications and websites.

Don't Let Working From Home Lower Your Guard



Wyatt Funchion is a tech support intern at Tech Experts.

When working from home or taking online classes for school, it is very easy for us to get caught up in our work and forget about the potential risks of using the Internet.

Whether you are using Zoom, assisting clients, writing assignments, or even just sending a simple email, cybercriminals have figured out ways to exploit our everyday tasks.

Email is one of the most vulnerable territories for users, and cybercriminals love it because it works. Phishing emails, which are emails that try to trick you out of your sensitive information, are one of the most common Internet threats and are easy to overlook if you're overworked or in a hurry. Some can be extremely convincing, especially at a glance.

One of the best ways to keep your personal information and your work information protected is to avoid clicking links, opening attachments, and replying to emails when you don't know where or who the email came from. Don't provide them with extra information like a password, log-in, or anything else sensitive.

Cyberattacks are another common threat while working from home, and your computer and network are targeted just for existing. An easy way to prevent these attacks would be to use an antivirus suite.

These run in the background of your computer and automatically update themselves. They can protect against zero-day attacks (viruses taking advantage of security flaws before they are patched), malware, spyware, viruses, trojans, worms, and more. Some can alert you of phishing scams, including those sent via email, and alert you when a download is suspicious.

Something else that could put both your work and personal information at risk is your web camera. Cameras are used frequently for Zoom calls or Google Meets for both schools and employers and can be a huge risk if you have any documentation like passwords written in your workspace.

It's also a big risk to your privacy in general, so make sure there isn't anything else confidential in frame, such as personal phone numbers on a whiteboard.

A simple way to get rid of the potential risks would be to either unplug your webcam or cover it when it's not being used. Sliding webcam covers are a good way to cover them and are fairly easy to install. They can be found in all shapes, sizes, and colors.

If your workspace is easily accessed by your family or you also use your personal computer for work, it can create threats for your company. Make sure to not leave your computer unlocked or open on any sensitive information that could be accessed by someone other than you. Another risk can be using your work account for personal use because you may not be as careful about what you access during your personal time versus work hours.

In the end, it is important to keep your work life or school life separate from your personal life.

Taking a few extra steps to make sure everything is secure can be the difference between a stolen identity or encrypted computer.

"Make sure to not leave your computer unlocked or open on any sensitive information that could be accessed by someone other than you."

Changing Your Password Has Changed

If you didn't know, changing your password regularly is so 2018. No, as ever in the world of tech, things have moved on and there are better, easier ways of doing it now.

We're not suggesting you stick with the same password you've been using for the last 10 years. And certainly not suggesting you use the same password across multiple apps.

Today, the most secure way to keep your passwords un-hackable is to utilize a random generator for each new password. And then use a password manager to keep them all safe for you.

A random generator will create passwords you couldn't possibly remember yourself - even if you could recite pi to 100 digits. They're really… random. Which is perfect for keeping your accounts secure.

The password manager comes in and stores these passwords safely for you. So no more jotting down random characters in the back of a notebook.

Together, they make the perfect team. And we suggest that you get your own team to use them, now.

If you're unsure how to set this up, or you would like some help to find the password manager that would be best for your business, call us at 734-457-5000. We'd love to help.

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(888) 457-5001
sales@MyTechExperts.com

Take advantage of our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

Lessons Learned from the Colonial Oil Pipeline, continued

industrialized and well-funded - meaning they have resources well above what the average business could manage.

As a result, they are able to evolve rapidly and strategically, and cyber defense has been unable to evolve as quickly. While there is no foolproof cyber protection, following the general best practices can put you in the right direction to significantly reduce your cyber-risk.

How to prevent cyberattacks

Even with such significant growth in the rate of cyberattacks, all hope is not lost. TechRepublic recently compiled a list of 10 things you can do to help prevent your business from being a victim of ransomware. While speaking specifically to ransomware, the same principals can be applied to malware and other hacking protocols. These are taken directly from TechRepublic and include:

1. Keep clear inventories of all of your digital assets and their locations, so cyber criminals do not attack a system you are unaware of.

2. Keep all software up to date, including operating systems and applications.

3. Backup all information every day, including information on employee devices, so you can restore encrypted data if attacked.

4. Backup all information to a secure, offsite location.

5. Segment your network: Don't place all data on one file share accessed by everyone in the company.

6. Train staff on cybersecurity practices, emphasizing not opening attachments or links from unknown sources.

7. Develop a communication strategy to inform employees if a virus reaches the company network.

8. Before an attack happens, work with your board to determine if your company will plan to pay a ransom or launch an investigation.

9. Perform a threat analysis in communication with vendors to go over the cybersecurity throughout the lifecycle of a particular device or application.

10. Instruct information security teams to perform penetration testing to find any vulnerabilities.

Social Media: Friend Or Fraud?

Hopefully you're aware of the risks of fake accounts on social media. Accounts are created to catfish; con people out of money; and for other kinds of exploitation.

But did you know that fake accounts can be created for other services too?

Most of the businesses we interact with now need you to create an account. Think food ordering, online shopping, maybe even for businesses like yours.

But what's the harm in that, right? These fakes won't be creating accounts on your website to trick you into anything. They won't be able to access your products or services for free. Aside from creating spam in your CRM, what's the problem?

Actually, these fake accounts can result in huge fraud. Recently, for example, the US Secret Service announced it had recovered $2 billion in fraudulent Covid-19 relief claims.

And it's on the rise, because there are now software tools which automate account creation and mask real identities.

In the world of retail, bots exist to buy up limited edition or highly desired items, aiming to resell them for a higher price.

And the lengths these bots go to in order to make fake email accounts look like real humans is incredible.

They sign up to mailing lists, send emails, watch YouTube videos, all to build up normal email account activity, before creating accounts with the desired retailer, ready for the drop.

When the item is released, these bots are all logged in and checking out at the same time, making it next to impossible for real humans to make a purchase.

While this may not directly affect your business in this way, it's making it very difficult for all of us to be recognised as real individuals online. It may be only a matter of time before this is recognised as a form of fraud.

Have you considered how fake account fraud could affect your business? Perhaps it's time to take a look at the way accounts are created to do business with you.