Gulfcoast Networking Newsletter

Your IT Management Experts

September 2021

Hello! We're pleased to send you this monthly issue of the Gulfcoast Networking, Inc Newsletter. It's our way of saying that you're important to us and we truly value your business. Please feel free to pass this newsletter on to friends and colleagues. Enjoy!

MONTHLY QUOTES:

"Life is what happens when you're busy making other plans."

John Lennon

"Tough times never last but tough people do."

Robert H. Schuller

"If we have the attitude that it's going to be a great day it usually is."

Catherine Pulsifier

IN THIS ISSUE:

Four Ways You Can Ensure Safe Password Sharing in the Workplace

There is a myriad of reasons why people may need to share passwords in the workplace; however, it is important that you understand that this practice is not without risks. If a password finds its way into the wrong hands, you may find yourself on the receiving end of a ransomware attack, compliance review, or serious data breach.
Here are four practices you can adopt to limit the risk of password sharing in the workplace.

1. Avoid password sharing
We'll start with the obvious one: Password-sharing should not be common practice. Aim to ensure all employees have their own login details so that you can fully control and monitor their activity. Employees should not share passwords unless there is a tangible business need.

2. If passwords need to be shared, ensure safe practices
In some cases, employees may need to share passwords. In such scenarios, security measures must be implemented to make sure the passwords are only shared with authorized individuals. Passwords should never be shared via text message or email. The most secure way to share passwords is via an enterprise password management platform; for instance, Keeper. Software such as this allows IT admins to create shared folders for groups of users according to their roles and subsequently grant people access to those folders. Employees simply log in to their Keeper vault to access the device.

3. Reset shared passwords when people leave the organization
Research has found that around one-third of employees in the US have accessed an online account that belongs to a previous employer. Regardless of the reasons why an individual leaves an organization, IT administrators should ensure all their access rights are immediately revoked. Again, this task can be simplified by using an enterprise password management platform like Keeper, which allows IT to disable multiple accounts within minutes.

4. Don't overlook the risk of shared passwords
It is important that shared passwords adhere to the same security rules as all other passwords that are used in the organization. Specifically, they need to be formed of a combination of numerals, uppercase and lowercase letters, and special characters. Passwords should not be used across accounts, and multifactor authentication (2FA) should be deployed to ensure the maximum level of protection against hackers. Again, enterprise-grade password security should be employed.

Good News! You CAN Install Windows 11 on Older PCs

To many users' joy, Microsoft recently announced that it would not block users from installing the Microsoft 11 operating system on older PCs. While Microsoft has revealed its recommended hardware requirements for Windows 11, any restriction designed to prevent you from installing the upgrade will only kick in if you try to download the latest version via the Windows Update function. As such, any users with an older CPU that doesn't technically meet the update requirements can still access the Windows 11 ISO file and upload it manually.

However, you would do so at your own risk. According to Microsoft, the Windows 11 update is only suitable for users with Intel 8th Gen and beyond. However, it has since advised that users can upgrade at their own risk provided they acknowledge that Microsoft can not assure that the driver will be compatible. Further, systems that are upgraded despite not meeting the requirements will not be automatically fed Windows updates, even security patches. Effectively, if you install Windows 11 manually, you will also need to manually install all later updates, which will undoubtedly be a huge inconvenience.

A further risk associated with installing Microsoft 11 manually is that devices that do not meet the minimum user requirements are prone to failure. According to data released by Microsoft, computers that are not equipped with the required technology typically exhibit 53% more kernel mode crashes. On the contrary, those that do meet or exceed the specs benefited from a 99.8% crash-free experience.

Microsoft intends to update its PC Health Check app to incorporate the Intel CPUs and offer users a greater level of clarity in terms of what PCs are, and are not, suitable for Windows 11. When introduced, the PC checker app will inform users whether they can simply enable the Secure Boot to upgrade.

Microsoft has also disclosed how it determined the minimum system requirements associated with Windows 11. Microsoft is consciously aiming to push Windows in the direction of contemporary DCH divers and modernity security, incorporating virtualization-based security (VBS) and Trusted Platform Module (TPM).

Although there is never a great time to attempt to modify hardware requirements, given the workaround that is available, it does soften the blow in terms of Microsoft's efforts to improve the reliability, security, and compatibility of Windows 11.

News Bytes

Windows 11 is Coming!

The long-awaited moment has come: Microsoft has finally announced when it will release Windows 11. According to Microsoft, it will start rolling out Windows 11 on October 5, 2021. As such, we're not going to have a long wait until we finally get our hands on the latest version of the operating system. However, some of us will have to wait longer than others. According to a post on Microsoft's blog, the rollout will be gradual. Devices that meet all the OS' compatibility requirements will be prioritized, and all other devices will subsequently be evaluated for suitability according to age, hardware, and reliability metrics. According to Microsoft, all devices that are deemed to be suitable for the operating system will be offered the free update by the middle of 2022. So how do you get the upgrade? All users with an eligible PC will be automatically informed when the update is available. However, you should note that some of the features available in the operating system, such as Android Apps, may not be available immediately as Microsoft has plans to roll them out at a later date.

Accenture Falls Victim to Ransomware Attack

It seems that Accenture may have been the latest victim of the LockBit ransomware gang, which has offered to sell data that has been taken from the global consultancy organization. However, while a spokesperson from Accenture has confirmed to CNN Business that the company has been targeted in a cybersecurity attack, it did not reveal what form the attack took and whether ransomware was involved. On a page on their dark website, LockBit issued a statement confirming the breach and stated that it would release data from Accenture's systems if they did not pay the required ransom. Previous victims of the notorious LockBit ransomware gang include Mersey rail and Bangkok Airlines. Historically, ransomware attacks involved hackers stealing data and then encrypting the associated files until the victim paid a ransom. However, tactics have since evolved to groups executing DDoS attacks on websites, informing journalists and customers of the infringement, and even threatening to inform stock exchanges.

Initial reports revealed that LockBit had published around 2,400 of the stolen files. However, these were later removed, and a new countdown was set by LockBit. It will be interesting to see what happens next. However, what is clear for now is that the clock is ticking to the deadline…

Question of the Month

Question: ***How Can I Prolong my Laptop Battery Life?***

Answer:

You can take a few simple steps to prolong the battery life of your laptop. Here are some top tips and tricks for making sure your battery achieves its full life potential.

Ensure you fully charge the device on first use: After buying a new laptop or battery, ensure you put in on charge for at least 24 hours. This will make sure the battery is fully charged before it is first use and increase its life expectancy.

Remove the battery if you do not expect to use the device for a while: If you intend to use the laptop mostly while it is plugged directly into an outlet or will not use the laptop for over a month, remove the battery from the computer. After putting a battery back into a device, it should be fully charged for a full 24-hour period once again before you turn the laptop on.

Avoid extreme temperatures: Both your battery and your laptop should not be exposed to extremely cold or hot temperatures. For example, you should avoid leaving your laptop in a car during a very hot summer's day or overnight in the car in the winter months.

Clean the contacts regularly: Every few months, remove the laptop battery from the device and clean the contacts using a cotton swab and alcohol.

Fully discharge and recharge the battery every month: If you are using a battery that is not a Li-ion, every month, you should fully discharge the battery before recharging it for at least 24 hours.

5 Top Tips for Protecting Your Email Accounts

Think your email is protected against hacking? You're wrong.

Many email accounts lack the security protocols required to protect against unauthorized access, theft, and malware attacks. Fortunately, you can take positive action to protect your account. Here are five top tips for protecting your email account.

Set up different email accounts for personal and business purposes
Most people use one single email for all purposes, meaning that shopping deals, messages, newsletters, and invoices all get sent to the same place. This can be a massive problem if someone gets unauthorized access to your inbox. Set up at least two email accounts to separate business from pleasure. In addition to increasing your security, it may also enhance your productivity.

Use strong passwords
Far too many people underestimate the importance of using strong passwords on their email accounts. Ensure you use a long password that contains numbers, a combination of upper- and lowercase letters, and special characters. You may want to go one step further by putting in place multifactor authentication (MFA). This helps provide an extra level of security by requiring a second validation process; for example, a fingerprint scan.

Be on the lookout for spam emails
If you receive an email from an unrecognized source that contains a link, do not click on the link until you have verified that it is authentic. Sometimes, emails of this nature are safe. However, there is also a risk that they may contain malware that infects your computer. Attacks of this nature are known as phishing and the emails involved often come from hackers posing as notable companies such as Amazon, the Bank of America, or FedEx.

Keep an eye on your account activity
Periodically monitor your account activity and limit the access privileges you allocate to apps. Screen your logs for suspicious activity on a regular basis to make sure no unauthorized IP addresses or devices have accessed your accounts. If you do spot anything that looks suspect, log out of all your web sessions immediately and change your passwords.

Use email encryption
If you encrypt emails that can not be intercepted mid-route and viewed by unauthorized parties. In addition, ensure you install the latest updates for your firewalls, anti-malware, and email security software to find and fix any vulnerabilities before the hackers do.

Your Newsletter

Gulfcoast Networking, Inc.

6335 Grand Blvd

New Port Richey, FL 34652

727-847-2424 ext 103

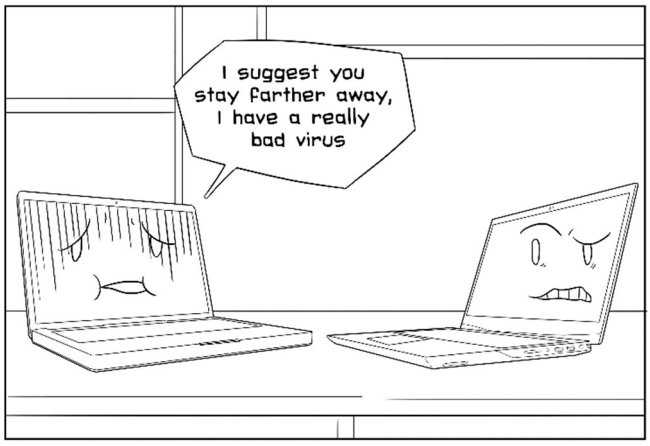
rob@gulfcoastnetworking.com

https://gulfcoastnetworking.com

A MONTHLY NEWSLETTER TO INFORM AND ENTERTAIN OUR CLIENTS **SEPTEMBER 2021**

APP OF THE MONTH: OVERDROP

Overdrop is a storm radar and hyperlocal weather app that is powered by top weather forecasting experts such as WeatherBit and AccuWeather. You can use Overdrop to access real-time weather data related to variables such as humidity, cloud cover, UV index, wind speed, rain, snow, and hail. Overdrop also allows you to set customizable weather notifications so you can receive an instant warning if the weather is set to make a change for the worst. Users with privacy concerns can rest assured that Overdrop is fully secure. Location data never leaves your device, and the app is never connected to other services.



Gulfcoast Networking, Inc.

FROM THE DESK OF:

Rob Marlowe

If you don't have a managed-service agreement in place, please let us know and we'll conduct a needs analysis and provide you with a proposal free of charge!

Email: *rob@gulfcoastnetworking.com*

Phone: 727-847-2424 ext. 103