Gulfcoast Networking Newsletter

Your IT Management Experts

November 2021

Hello! We’re pleased to send you this monthly issue of *[***Your 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:

"Always forgive your enemies; nothing annoys them so much."

Oscar Wilde

"Anyone who has never made a mistake has never tried anything new."

Albert Einstein

"Don't judge each day by the harvest you reap but by the seeds that you plant."

Robert Louis Stevenson

IN THIS ISSUE:

What’s the Difference Between Two-Factor and Multifactor Authentication?

Almost every time a security breach occurs, the failures can be traced back to simple issues like weak credentials and lax security standards. You’ve probably come across terms like single-factor, two-factor, and multifactor authentication.

But what are the actual distinctions between these approaches, and how can one safeguard your organization?

What exactly are factors and authenticators?
Factors are divided into four categories:
Knowledge: Something you know, such as a PIN or a password.
Possession: Something you own, such as a one-time password generator or a smartphone.
Inherence: Something that identifies you, such as a fingerprint or a face scan.
Context: Something you do in your day-to-day life, such as your reaction or a pattern.

Single-factor authentication means that only one of these elements, usually a password, is required in addition to a username or account number. That’s all there is to it. In today’s digital world, using single-factor authentication on any form of account is severely discouraged, and it has now been added to CISA’s List of Bad Practices. More verification that prove your identity is required for additional account protection.

Two-factor authentication (2FA) is when two authentication elements are required to get access, whereas multifactor authentication (MFA) is when more than two factors are necessary.
Why is multifactor authentication better than two-factor authentication?

Adding at least one more layer to 2FA, such as combining a PIN and texted passcode with a biometric layer like a face scan, provides a formidable barrier between the hacker and the protected data. MFA implies you’re in complete control of all security, especially when an MFA hardware cryptographic device is utilized, as suggested by NIST for AAL 3.
A genuinely unbreakable data protection solution involves multifactor authentication. Multifactor authentication solutions not only assist in preventing theft and illegal access, but they also provide your team more assurance that only your team has access to important and secret information.

Everything You Need to Know About Android Malware

Smartphones are similar to palm-sized computers; as such, you should ensure they are protected to the same extent as your laptop and desktop computer. While you don't need to install expensive security software to keep hackers away, there are several things you can do to safeguard your information.

Malware on mobile devices

Infected mobile devices may be just as damaging to a company's network as infected desktops and laptops. Overcharging on phone bills, stolen data, intercepted communications, phishing attempts, and bogus alerts to one's contact list are all potential issues.

Malware is most commonly found in programs downloaded from third-party app shops. Hackers can gain access to passwords, user account information, and other sensitive personal information by using these. Because many corporate users connect their Android smartphones to one another, malware might easily spread across several devices.

Who is to blame for this?

Smartphone users aren't the only ones who bear the brunt of the responsibility. App retailers are also to blame. In one case, malware-infected banking and weather apps were made available on Google Play. In response to the problem, victims were advised to upgrade their phones with the most recent security updates.

How to Stay Away from Mobile Malware

Although the Google Play Store isn't completely safe, downloading from well-known app shops rather than less-secure outlets minimizes the risk of acquiring harmful programs. If an infected app is launched and begins receiving a lot of downloads, Google will quickly delete it and notify everyone about the dangers of using it.

It's challenging to prevent mobile spyware from slipping through the net, despite app shops' best efforts. That is why it is beneficial to read user evaluations. In addition, keeping your mobile device's operating system and security software up to date helps avoid infection because the most recent versions are patched against known cyber threats.

Malware makes no distinctions, so if your software isn't up to date, it will find a method to infect your device. Consult our cybersecurity specialists immediately to find out if your business gadgets are safe and secure.

News Bytes

AMD and Microsoft Launch Fixes for Ryzen slowdowns in Windows 11

According to an AMD knowledgebase post published recently-, both Microsoft and AMD have provided fixes to solve AMD Ryzen performance problems found in early versions of Windows 11. According to AMD, a fault in Windows 11 might impair Ryzen CPU performance by up to 15%. AMD has published a new chipset driver to remedy a problem that affected the "preferred core" function, which can improve performance on high-core-count, high-TDP Ryzen CPUs. Even if you're not affected by this problem because you're using Windows 10 or a Ryzen CPU with fewer cores, the updated driver includes solutions for several additional Ryzen and Threadripper computers running Windows 10 or Windows 11. According to Microsoft, if you don't already have the patch installed on your PC, it will show as an optional update in Windows Update for Windows 11 Home and Pro users. Otherwise, the update should be included in the next Patch Tuesday package automatically.

Hackers Continue to Steal Cookies from High-profile YouTube Accounts

Since late 2019, a group of hired hackers has been hijacking YouTube producers' channels, forcing them into phony partnerships involving cryptocurrency scams or extortion. According to a recent analysis from Google's Threat Analysis Group (TAG), cookie stealing malware was used to target the video platform. The breach was carried out by a gang of hackers who were recruited through a Russian-language forum.

Since May, Google has banned 1.6 million messages and restored roughly 4,000 YouTube influencer accounts damaged by the social engineering effort, with some of the stolen channels selling for anywhere from $3 to $4,000 on account-trading markets, depending on the subscriber count. Other channels, on the other hand, were rebranded for cryptocurrency scams in which the adversary live-streamed videos promising cryptocurrency giveaways in exchange for a small donation, but only after changing the channel's name, profile picture, and content to imitate large tech or cryptocurrency exchange firms. Following Google's involvement, the perpetrators have been seen directing targets to messaging applications such as WhatsApp, Telegram, and Discord to get around Gmail's phishing defenses, as well as switching to other email suppliers such as aol.com, email.cz, seznam.cz, and post.cz. To avoid account takeover threats, users should use two-factor authentication.

Question of the Month

Question: ***How Can I Encrypt a Hard Drive in Windows 10 Using BitLocker?***

Answer:

Microsoft's patented disc encryption software for Windows 10 is known as BitLocker. BitLocker can encrypt your whole disc and safeguard your system from illegal alterations, such as firmware-level malware.

In Windows 10, here's how to encrypt your hard drive.

In Windows Explorer, look for the hard disc you wish to encrypt under "This PC."

Choose "Turn on BitLocker" from the context menu when you right-click the destination drive.

Create a strong password and choose "How to Enable Your Recovery Key" to gain access to your disc if you forget your password. You may print it, save it to your hard disc as a file, store it to a USB device as a file, or save the key to your Microsoft account.

Next, select "Encrypt Entire Drive." This option is more secure since it encrypts the files you want to delete.

Choose "New Encryption Mode" unless you require your disc to be compatible with previous Windows PCs.

To begin the encryption process, click "Start Encrypting." If you're encrypting your boot disc, you'll need to restart your computer. It will take some time for the encryption to complete, but it will do so in the background while you carry on using your computer.

Note that BitLocker is not accessible on Windows 10 Home, although there is a device encryption function that is comparable.

Why Should Your Files Be Encrypted?

The worst-case scenario would be if your laptop was taken and included a million social security numbers or bank account details. Unencrypted. Let's imagine the confidential information of 2,500 clinical trial participants was taken from a worker's vehicle. Unencrypted. You certainly don't want to find yourself in that position.

How to Strengthen Your Bring-Your-Own-Device (BYOD) Security

The way we live has been profoundly altered by mobile technology. Businesses are increasingly adopting the bring your own device (BYOD) trend. However, it isn't without its risks.

A BYOD security policy is required whether your employees use smartphones, tablets, or laptops. You should also be aware of the following significant BYOD security risks:

Device loss or theft - Employees frequently carry their own gadgets around with them. This implies there's a bigger likelihood of them being lost or stolen, which could compromise the data stored on them.

Man-in-the-middle (MITM) attacks – While public Wi-Fi hotspots are useful for getting work done, they're also favorite haunts for hackers who utilize MITM to collect data sent over public networks.

Devices that have been jailbroken – The practice of eliminating a device's manufacturer's constraints, usually to allow the installation of unlicensed or third-party software, is known as jailbreaking. There's a greater chance that an employee may unintentionally install dangerous software on a personal device.

Malware - When a personal device becomes infected with malware, it can spread to other devices on the workplace network, resulting in data loss and downtime.

It's critical to develop a BYOD security strategy that meets both your company's and workers' demands in order to reduce hazards. Here are some suggestions:

Passwords should be required on all BYOD devices.

- Enforce the usage of passwords on all BYOD devices to prevent unauthorized access to business data. Long and unique passwords are recommended.
- Make a list of programs that employees are not permitted to use. A mobile device management platform that allows IT administrators to safeguard and enforce policies on registered devices is the easiest approach to ban applications.
- Access to data should be limited. Ensure employees can only access the data and applications that they need to perform their work. This can reduce the impact of some forms of malware and mitigate the consequences of a data leak.
- Invest in dependable gadget security solutions. Protect BYOD devices with trusted antivirus software to detect and eliminate viruses before they may do damage. This is crucial for mission-critical data security and preventing downtime.
- Educate your personnel on the importance of security. Human error is at the root of the great majority of BYOD-related security problems. Educate your team on how to use their phones safely. This involves training people how to recognize potentially malicious apps, sharing security threat alerts, and teaching them how to safeguard their devices by going beyond basic security settings.

Gulfcoast Networking Newsletter

Gulfcoast Networking, Inc

6335 Grand Blvd

New Port Richey, FL

727-847-2424

rob@gulfcoastnetworking.com

https://gulfcoastnetworking.com

New Email Options

Gulfcoast Networking is currently testing some new email features.

If you need to be able encrypt emails and file attachments, please contact us.

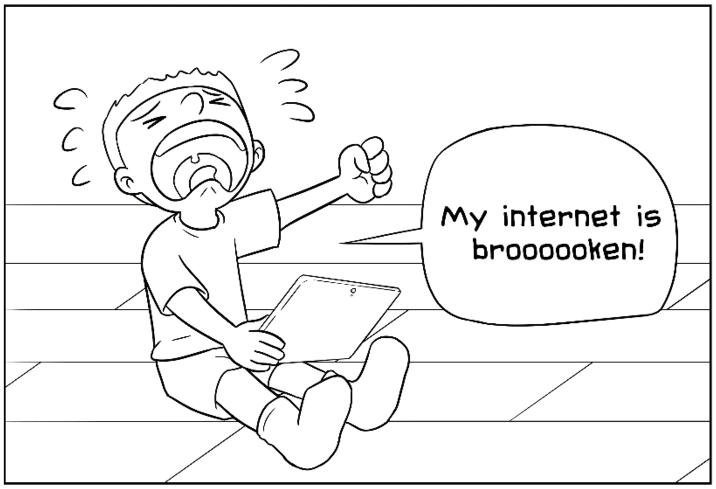
If you are interested in automatically archiving your email, please let us know.

If enhanced email filtering, spam protection and email AV are of interest, please let us know.

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

APP OF THE MONTH: RADIO GARDEN

By spinning the globe in Radio Garden, you can listen to thousands of live radio stations from across the world at the click of a button.
A city or town is represented by each green dot. To listen to radio stations broadcasting from that city, simply tap on it.
The app's developers strive to provide a pleasant worldwide radio listening experience by adding new stations every day and replacing those that no longer operate.
You can save your favorite stations to listen to later, and the radio will continue to play even if your phone goes to sleep. According to the developer, more features are in the planning, so you have plenty more to look forward to.



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

All data and information provided in this newsletter is for informational purposes only. Gulfcoast Networking makes no representations as to accuracy, completeness, correctness, suitability, or validity of any information in this newsletter and will not be liable for any errors, omissions, or delays in this information or any losses, injuries, or damages arising from its display or use. All information is provided on an as-is basis.