frogworks
Managing Your Technology So Your Business Doesn't Croak.

Ribb"IT" Review

"Blessed is the season which engages the whole world in a conspiracy of love."

– Hamilton Wright Mabie

December 2018

Issue 12, Volume 8

This monthly publication provided courtesy of Alex Bleam, Owner of Frogworks

We are excited and proud to announce that Frogworks has been recognized as one of the world's best MSPs by Channel Futures!

Channel Futures MSP 501 2018 WINNER

THE ULTIMATE GUIDE TO THE WORLD'S BEST MSPs

The Importance of Strong, Secure Passwords

****

Unauthorized access is a potentially major problem for anyone who uses a computer or high-tech devices such as smartphones or tablets. The consequences for victims of these break-ins can include the loss of valuable data such as presentations, emails, and music. Victims may also have their bank account information, money, or even their identity stolen. Moreover, unauthorized users may use someone else's computer to break the law, which could put the victim in legal trouble.

One of the most common ways that hackers break into computers is by guessing passwords. Simple and commonly used passwords enable intruders to easily gain access and control of a computing device. *Conversely, a password that is difficult to guess makes it prohibitively difficult for common hackers to break into a machine and will force them to look for another target. The more difficult the password, the lower the likelihood that one's computer will fall victim to an unwanted intrusion.*

Information Sharing & Security Issues

Thanks to modern technology, computing devices come in many different forms, such as desktop machines, laptops, smartphones, music players, and tablets. Any one of these devices may connect with other computing devices and share information, and in many cases, they may also connect with banks to conduct financial transactions. All of these machines are potentially vulnerable to misuse by unauthorized users, and therefore, users should always protect them with passwords.

Passwords are a means by which a user proves that they are authorized to use a computing device. A single device may have multiple users, each with their own password. Passwords are not unlike a lock-and-key system, in which only the right key will enable a person to have access. The difference is that each person has a different key for the same door.

Some computing devices, such as desktop computers and laptops, also have a management-level user, or "*superuser*," who has the ability to control other users and modify the computing devices software, among other things. This superuser account is also known as the "*root*" or "*administrator*" account. This is important to know because while hackers will try to acquire any password they can get, they will generally try to guess the superuser password first, as it gives them the most control over a device.

Key points of Password Security

There are key points of password security that users must know in order to reduce the likelihood of a hacker cracking their password and thus gaining access to their device.

- Most importantly, passwords must be long and complex.
- Long and complex passwords require more effort and time for a hacker to guess.
- Passwords should contain at least ten characters and have a combination of characters such as commas, percent signs, and parentheses, as well as upper-case and lower-case letters and numbers.
- Users should never write down their passwords, as that makes it easier for the passwords to be stolen and used by someone else.

Also, never use the same password for two or more devices, as hackers who break into one machine will try to use the same password to take control of others.

Mobile Devices Security

On mobile devices, a PIN or pass code is also needed. This is like a password for a computer, but it may have a

(Continued on page 2)

(Continued from page 1)

minimum of four characters or digits and be something that is not personal or easily guessed. Pass codes for devices should also be set to time out after a short period of time. Upon timing out, the code will then need to be re-entered. Ideally, the timeout should occur in no more than 20 minutes, although shorter periods between time-outs are best.

Importance of a Strong Password
One of the concerns that people often have when it comes to creating complex passwords is a fear of forgetting them, particularly when there are several to remember. Naturally, a person should try to think of something that will be easy for them to memorize. One way to do that is to turn a sentence or phrase into something that is not easily recognized by others. To do this, use the first letter of every word in the sentence, replacing certain words with numbers or symbols. For example, the word "*for*" may be replaced with the number 4 or the word "*number*" with the # symbol. With this method, a password such as "*Save the number for later in the year*" may read *St#4LITY*.

Password Security Measures
Passwords are undoubtedly essential to security, but they are not the only method that can or should be used to protect one's computers and devices. In addition to creating a good password, people should learn how to safeguard it and use it wisely. This means never sharing it and, if unable to remember it, keeping the written copy in a secure location.
Other security measures outside of passwords include only providing personal information on websites that are encrypted. An encrypted website can easily be recognized by the presence of *https* at the beginning of the Web address. Computer security software is also critical when it comes to securing computers, and both security software and the firmware on mobile devices should be regularly updated. Security measures such as passwords are critical when it comes to preventing the unauthorized access of one's computer and mobile devices. In today's world, hackers and other cyber-criminals are continuously finding new ways to gain access to these devices in order to steal or exploit the information within. Careless use of passwords, however, can be as bad as leaving one's computing devices unprotected. For this reason, people should create and protect their passwords with care.

Are Banner Ads Coming To Some Windows 10 Apps Soon?

Given how unpopular ads are, you wouldn't think that Microsoft would be experimenting with ways of displaying more of them. Unfortunately, that's the direction the company is headed.

Currently, members of the Windows Insiders test group can see ad banners in both the Mail and Calendar apps.

Microsoft already allows third-party ads in Outlook.com for non-Office 365 subscribers, Microsoft Games, News, Weather, Travel, Finance, and Sports apps. This makes this latest expansion more of an evolution than a revolution. Even so, ad creep is both disturbing and off-putting.

Unfortunately, Microsoft isn't the only company headed in that direction. From the company's perspective, it's easy to see the attraction. After all, given the massive user base that the most popular applications enjoy, the people who control the apps have a large captive audience, which is why we're also seeing other companies following the same track.

Even so, it's not something that's seeing much support from the user community. After all, the web is currently awash in advertising, to the point that ad-blocking software has become a thriving industry as users try to limit the number of ads they're exposed to on a daily basis.

While it's understandable that companies will exploit whatever revenue streams they can, this approach almost seems like pouring salt in the proverbial wound. These companies are already earning record profits anyway.

Microsoft's head of communications, Frank Shaw, has since tweeted out that the advertising feature in the Mail app was experimental and is being turned off. Even so, most users feel that it's just a matter of time before they reappear.

The central issue is this: If a company gives its software away for free, ads are expected because they give the company a means of recouping the costs of developing a given program. However, if you're paying top dollar for software, you shouldn't have to be forced to view ads on top of that. Here's hoping these companies reverse course.

Hidden Threats: Is Your Computer Secretly Mining Cryptocurrency?

Mining cryptocurrency used to require thousands of dollars worth of equipment to see any kind of meaningful return, but not anymore. Newer digital currencies like Monero, ByteCoin, and AEON have given would-be miners the ability to mine tokens right from their laptops. This might benefit small-time miners that want to get involved in the sector, but for every good thing online there are always people that figure out a way to use it for bad.

Hackers have begun using these tools to infect computers and websites to secretly mine cryptocurrencies. This emerging type of malware attack has been dubbed as "cryptojacking," and it could cause your computer to overheat and crash. Luckily, spotting these hidden miners isn't all that difficult.

Cryptojacking essentially hijacks your computer's CPU power to mine. This means when you're browsing the web, the malware is running in the background completely unbeknownst to you. There are a few types of this malware, and some run only when you visit a certain website and others can be maliciously installed on your computer. The best way to prevent this is by using antivirus software and adblockers.

If you've already been hit with this kind of malware, you'll notice either your computer acting sluggish, getting warmer than usual, or its fan constantly spinning. If you aren't running any kind of demanding software, like video games or video editing programs, this should be the first hint that your computer is working overtime.

If you've noticed your laptop acting up, it's time to go check on what's going on under the hood. Mac users can view a detailed breakdown of everything their computer is running by searching "Activity Monitor" and using the magnifying glass icon at the top-right of the screen. Windows users can simply hold down the Ctrl-Alt-Del keys to bring up "Task Manager."

Both of these menus will display a graph of how much of your computer's processing power is being used. Any massive spikes should be red flags. You'll also see an ordered list of the programs using the most processing power at the moment. Before ending any of these programs be sure to research what they are, as you could be ending a crucial part of your operating system.

Both Tesla and the Los Angeles Times have had their sites infected by cryptojacking software. Companies with popular websites are the most at risk, as hackers can embed code onto their servers and use the CPU power of everyone who visits the site. But making it a habit to check on how your computer is running will ensure your device isn't getting used to make someone else a crypto fortune.

IBM Invests Billions To Purchase Popular Red Hat Linux

IBM has recently announced what is to be the largest open source acquisition in history. They're buying Red Hat for a staggering $34 billion dollars. This, as the saying goes, changes everything.

IBM has lagged behind its competitors for years in the area of cloud computing. When the ink dries on this deal, they'll move from a virtual non-entity in the market to the world's #1 hybrid cloud provider.

If you're a Red Hat supporter, don't worry that the company is going away. The company is to retain its independence. Rather than being rolled into the corporate structure of IBM, it will be run as a distinct entity and will continue to be led by Red Hat's current CEO, Jim Whitehurst. Red Hat's headquarters, facilities and their corporate culture will all remain intact.

Whitehurst himself had this to say about the announcement:

"...Importantly, Red Hat is still Red Hat. When the transaction closes, as I noted above, we will be a distinct unit within IBM, and I will report directly to IBM CEO Ginni Rometty. Our unwavering commitment to open source innovation remains unchanged.

The independence IBM has committed to will allow Red Hat to continue building the broad ecosystem that enables customer choice and has been integral to open source's success in the enterprise."

At this point, most of the hurdles standing in the way of the acquisition have been cleared. All that remains is gaining Red Hat shareholder and regulatory approval, both of which are deemed likely. Assuming there are no unexpected wrinkles in the plan, the deal is expected to be finalized sometime during the second half of 2019.

IBM has long supported Linux and other open source initiatives, and this deal is unlikely to change that. That is one of the reasons the proposed deal is unlikely to meet much resistance from either Red Hat's shareholders or governmental regulatory agencies.

Dark Mode On Android Phones Extends Battery Life

Google recently confirmed that "Dark Mode" on Android phones uses less power and thus, helps to boost battery life.

Most websites and OS screens do all they can to make it easier to see them on the diminutive screens of our smartphones. That means bright white backgrounds and bright colors are used to highlight what designers and webmasters want you to see.

Unfortunately, the brightness of those colors and the brightness of the screen itself both impact the power consumption of the display, and by extension, the life of your battery.

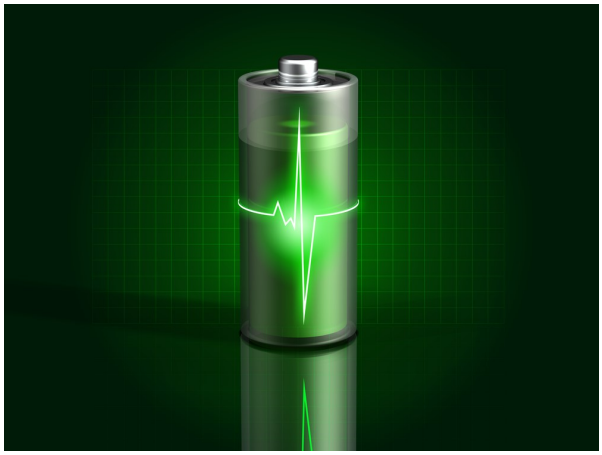
Dark Mode essentially reverses color themes, replacing white backgrounds with black. How much power does this simple change save? Well, according to Business Insider, Dark Mode uses 43 percent less power than normal mode in the YouTube App, which is white-heavy.

If it is an established fact though, that dark backgrounds are less power intensive than white ones, why does everyone insist on white backgrounds?

Actually, Google bears at least some responsibility for that, as the company has been quietly encouraging app developers to use the color white as backgrounds for their interfaces for years, via the company's "Material Design Specification."

The company is in the process of shifting gears and plans to roll out a Dark Mode for all Google apps in the future, though no firm data has been established for this.

In any case, the bottom line is that Dark Mode is good for your battery. If you want to enable it on your Android device, just do the following:



- Go to "Settings"
- Tap "Display" then "Advanced" then "Device Theme"
- Then tap "Dark"

That's it. You're in Dark Mode.

If you want to enable Dark Mode for YouTube, here's how:

- Launch YouTube on your Android Device
- Tap the profile icon (top right corner)
- Go to "Settings" and then "General"

Tap the toggle switch for "Dark Theme" to enable it, then tap the back button. Your theme changes will automatically be saved.