October 2021
Issue 10 Volume 11

frogworks

Managing Your Technology So Your Business Doesn't Croak.

Run your business without worrying about technology

Ribb"IT" Review

INSIDE THIS ISSUE:

What to do with your Desktop?

Reboot? Shutdown? Lock? Logoff? Hibernate?

This week's article "What to do with your Desktop" is written by our owner Alex Bleam. It will be featuring how to shut down your Desktop. Check out next months newsletter on how to shut down your Laptop.

At the end of your day, what do you do with your computer? Computer problems happen, there is no getting around that but the way you end your day on your computer can save you many future problems that will occur if done improperly. At Frogworks, we help you get those problems resolved as quickly as possible. While there are new computers coming out all the time and both Microsoft and Apple release new operating systems (and update to those operating systems) all the time, one thing has not changed.

Rebooting your computer is both **necessary** and **helps in the day-to-day operation** of your computer. Let's start with what is necessary and for the sake of this article, we are going to just refer to our frenemies at Microsoft – but this applies to Apple computers, too.

Microsoft releases updates all the time. These updates plug holes in the operating system of the computer, helping to keep you safer. Other updates include hardware updates (known as drivers) as the hardware manufacturers determine that THEIR software needs updates too, so they release their updates to Microsoft and in turn Microsoft pushes them down to your computer.

Any combination of these updates could require you to reboot your computer. Frogworks will sometimes let you know, via a message that pops up on your screen, that we have installed an update on your computer that requires an IMMEDIATE reboot – these are usually urgent security or critical updates.

(See page 2 to keep reading)

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

What to do with your Computer

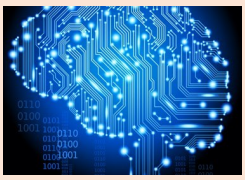
Reboot? Shutdown? Lock? Logoff? Hibernate?

So, if we do that, why reboot your computer at all? Rebooting your computer helps keep it running smoothly. It clears the memory, stopping any tasks that are eating up RAM. Even if you've closed an app, it could still tap your memory.

If your computer is still running slow, this one insider trick could help.

At the end of the day, click the start button, then the power button and choose restart, then walk away from your computer knowing that your computer will be freshly booted in the morning and all you must do is login. You may see that updates were installed on the overnight reboot and that is okay. You should expect that.

What happens if you shut your computer down at night? Well, if you do this, Frogworks cannot do any maintenance on your computer, this includes anything from disk maintenance to updates, to regular checks. But fear not, as soon as our software connects to the internet on the next boot up, some of things will run but not affect your computer nearly as much as being vulnerable to attacks because your computer is not getting updated. Locking your computer at the end of the day (or during the day) is something you can do. Our clients will typically do this when they are in the middle of work that is not really possible to save and walk away. Think multiple browser tabs open, emails open, documents open. By locking your computer all of those items stay open. Our software is smart enough to understand the computer is being used and will not reboot the computer while it thinks it is being used. There are times where Frogworks is syncing your email or **Cloud9 powered by Frogworks** and locking your computer is a safe way to allow those things to sync overnight.



Above all, if you have a problem or question, don't hesitate to reach out to us, we are here so you can focus on your business, and we will focus on your technology.

Here at Frogworks, we make sure that security and critical updates are pushed to your computer as soon as we have vetted them to make sure they don't break. This has been a common occurrence with Windows. Other updates we manually put on your computer as you have problems. Nothing is worse than you being able to print or scan just fine then to have HP send an update to Microsoft that gets pushed down and suddenly you can't print or scan anymore.

Struggling with that WI-FI?

You've probably been there before—about 10 seconds away from pulling your hair out and throwing the router at the nearest wall. It's nothing short of depressing when you're about to win Super Mario or fully engrossed in the latest Netflix Original, and then—bam—your signal drops off.

Things don't have to be this way, though. There are ways to improve your Wi-Fi and decrease those signal drops. Here are three simple tips to help you keep your signal strong and reliable:

Buy a new router.

It's recommended that you use a router with 802.11ac, which is three times faster than the previous standard. Not only will you get yourself a great router with a fast connection but a pretty sweet touchscreen, as well.

Keep it secure.

It is relatively easy to hack into other people's Wi-Fi connection. And if people are piggy-backing onto your connection, it's only natural to assume that your connection speed is going to lag. Because of this, it's important to keep your router locked up tight. For start-ers, change the password on your router. Your router will come with a preassigned admin password, and many security experts point this out as a major culprit of Wi-Fi hijackings.

Put it out in the open.

Lifehacker says that if your router is obstructed, then the signal will be, too. Don't keep your router hidden in a cabinet or tucked behind your sofa—sitting on top of your TV console or bookshelf is more suitable. And, if at all possible, stra-tegically position your router in the middle of your home to ensure even coverage throughout.

How Hackers Use Your Employees To Their Advantage

Social engineering is a tactic hackers are using more and more frequently to infiltrate systems. It involves a variety of approaches that focus on manipulating employees to drop standard security protocols. And if you expect to protect your data these days, then you'll have to take the necessary steps to educate and train your employees on how to detect and avoid these approaches.

Here are a few of them to look out for:

Phishing:

Most business professionals are familiar with the concept of phishing, but not everyone is able detect an attack. Phishing attacks usually come at you via email and is an attempt to gather information about you or your business illegitimately. It could be an email asking you to update your login credentials, click on a link, or download an attachment. Doing so reveals sensitive information and can lead to malware!

Exchanges:

Whether it's on a website, through an email, or in person, a criminal practicing social engineering might offer you something in return for information. The things offered will turn into ransomware, and in a hijacked password and hacked database. Once your data is in the wild, it stays in the wild and can be used by any number of unscrupulous characters.

Sneaking:

Some criminals will resort to lightweight espionage to get what they want, and they rely on the human element to help them do this. If computers are visible from the waiting room, a criminal can just glance over the counter to gather sensitive information. Everyday interactions and simple observations can tell the common hacker more than you might think. Taking that extra step to hide your screen can save you from an attack.

We Have an E-Newsletter!!!

Do we have your e-mail address??? If you would like to receive our newsletter though email please visit us at:

www.getfrogworks.com/newsletter

Channel Futures. Leading Channel Partners Forward

NEXTGEN 101

MSP TO WATCH • 2021 WINNER

WE'VE MOVED!

2670 Crain Highway, Suite 304
Waldorf, MD 20601