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

Ribb"IT" Review

March on. Don't look in the rearview, just the windshield.

March 2018

Issue 3, Volume 8

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

*"As a business owner, you don't have time to waste on technical and operational issues. That's where we **shine**! Call us and put an end to your IT problems finally and forever!"*

- Alex Bleam, Frogworks

It's business as usual at the office, until a ransom note pops up on your computer screen. Your files have been encrypted and the only way to get them back is to pay up. You've become ransomware's next victim and getting your files back and your system up and running again is going to cost you, but not in the way you think.

Unfortunately, cyberattacks like this are becoming all too common for small and medium-sized businesses. In fact, an Osterman Research survey of 1,000 small and medium-sized businesses last year revealed that 35% of them were victims of ransomware attacks. 22% of the businesses surveyed had to cease business operations immediately because of a ransomware attack.

90% of those ransomware infections resulted **in more than an hour of downtime** and lost productivity, while 1 in 6 infections resulted in **more than 25 hours of downtime**.

Clearly, it's more important than ever to protect your network from ransomware attacks to prevent downtime and lost productivity from devastating your business. Here's what you need to know to keep your business safe.

Education Is Key

Cybercriminals and hackers are getting smarter, but it isn't their knowledge of technology that is the real threat. It's their ability to convince human beings to click malicious links or open booby-trapped attachments that make them so dangerous.

Many perpetrators craft their emails to look like they come from legitimate institutions, family members or friends. They may even pose as law enforcement agencies, the CIA or the FBI to scare users into paying ransom to avoid criminal prosecution.

To avoid falling for these tricks, everyone in your organization needs to be educated about these potential threats. Scheduling regular training sessions to discuss network security is one of the best ways to prevent cybercriminals from accessing your systems, whether they are fishing for information or launching a ransomware attack.

Topics that should be covered regularly include:

Software to avoid

- The dangers of clicking links from unknown or suspicious sources
- Browsing insecure websites
- Accessing data from unprotected networks, such as public Wi-Fi

Establish and disclose clear security policies and make a plan to enforce them for everyone in the organization, from the staff interns to the CEO.

Use Strong Passwords for Everything

Remember the old saying that a chain is only as strong as its weakest link? That definitely applies to the use of passwords throughout your organization. Be sure that every employee sets up a strong password for EVERY device that they use on your network.

Strong passwords should have at least 8 characters and contain at least 1 number, 1 uppercase letter, and one symbol. However longer passwords are even better.

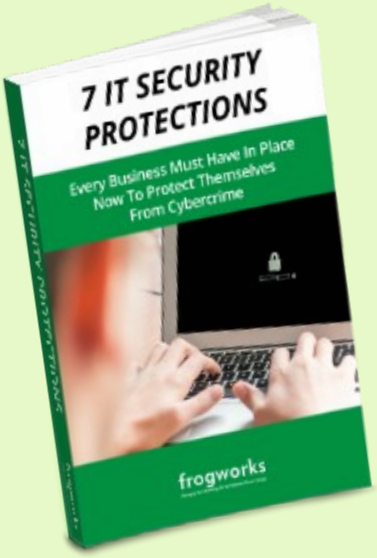
Encourage your staff to create password phrases that make passwords more secure without being too difficult to remember. For example, a phrase like “My mother's chicken pot pie is the best!” makes a pretty strong password when you add numbers, uppercase letters and symbols to it, like this:

MyMother'$ChickenP0tpieistheBEST!

Update All Software

Yes, software updates are a pain, but performing regular updates to your computer's operating system and software is essential to keeping hackers out and malware of all kinds off of your network. Set all software to update automatically, so this step never gets missed. Remember, human beings often have dreadful memories.

Have you ever lost an hour of work on your computer?



After working with dozens of small and mid-size businesses in the DC Metro area, we found that 6 out of 10 businesses will experience some type of major network or technology disaster that will end up costing them between $9,000 and $60,000 in repairs and restoration costs on average.

Gain Instant Access To Our Free Report, “7 IT Security Protections Every Business Must Have In Place Now To Protect Themselves From Cybercrime” TODAY! at https://www.getfrogworks.com/Cybercrime

Or call us today at (240) 880-1944

Invest in Antivirus & Anti-malware Protection

Be sure that every computer on your network has antivirus and anti-malware software installed to catch potential threats before they become a problem. Advanced anti-virus software will monitor the behavior of your computers and not simply rely on signatures that can be out of date. It should also provide the ability to rollback an infected computer to eliminate an infection. So you never pay the ransom.

Add the Right Firewall

Invest in a professional-quality firewall to block incoming threats to your network before they ever reach your computers. A firewall purchased from a big-box store is not sufficient to protect your business. You need a firewall that is designed for small or medium-sized businesses. You'll also need to make sure that your firewall is monitored and updated on a regular basis for maximum protection.

Monitor Your Network and Log Activity

Setup monitoring systems to monitor and log all network traffic that comes through your firewall, routers, and applications. Be sure to review this information on a regular basis to thwart potential threats.

Setup a Secure Backup

In the event that your network is attacked by ransomware or other malicious software, you should have a secure, encrypted backup of all your data and files that can be restored at a moment's notice. Your backup should be stored offsite so it won't be destroyed in the event of fire or other natural disaster. Online backups are a great solution that are becoming more affordable for small and medium-sized businesses.

What To Do If You're a Victim

While cybersecurity is becoming more sophisticated all the time, no system is 100% bulletproof. So what should you do if you're the victim of a ransomware attack?

First, DON'T pay the ransom! There's no guarantee that your attacker will release your files, even after they receive payment. Paying the ransom also encourages more cybercrime against you and other business owners.

(Continued on page 4)

Nvidia Dropping Driver Support For Older Operating

AMD long ago dropped support of 32-bit operating systems, and now, Nvidia is following suit. The long-anticipated move by the company will mean the end of driver support for the 32-bit builds of Windows 7, Windows 8, Windows 8.1, Windows 10, Linux and FreeBSD.

Nvidia is taking a balanced, responsible approach here. The company has pledged to continue offering 32-bit driver security updates until January 2019, but will immediately discontinue making performance updates to the drivers of older OS's.

In some respects, it's long overdue. Today's application environment is incredibly resource intensive, with a growing number of applications requiring more computing horsepower than 32-bit systems can deliver, since a 32-bit OS can only support up to 4GB of RAM.

The picture gets even bleaker if you're a gamer. Even modest games tend to require more than 4GB of RAM these days, and most top-tier titles no longer offer support for 32-bit systems. That, combined with the fact that 32-bit systems are somewhat less secure overall, it's probably time they were put to pasture.

Given this landscape, it's probably time to pronounce the 32-bit operating system dead. If you've got some legacy applications still running on an old machine, now is the time to get serious about your migration plan.

Most of the older OS's are no longer receiving security updates, which leaves you increasingly vulnerable to a wide range of hacks. That, coupled with the increasingly sparse driver support makes it inevitable that you'll have to migrate at some point, and it's always better to do it on your terms than someone else's.

If you haven't yet worked out what to do about your old legacy systems, it's long past time to do so. The clock has been ticking for a while now, and the ticking just got a little bit louder.

(Continued from page 3)

Instead, call an IT professional right away. Don't try to "Google" a solution or try to fix the problem on your own in order to save money. You could end up making the situation worse and extending your downtime even more. The best approach is to seek professional intervention as soon as possible.

Want to find out if your network is ready for the next ransomware attack? Get a FREE IT Security Assessment from the cybersecurity experts at FrogWorks!

4 Reasons You Should Be Using LinkedIn

The other day one of my clients asked me what I thought of advertising on LinkedIn. While people often use LinkedIn for networking, hiring, and finding a job, it can also be a great opportunity for marketing your business.

Become An Expert By Interacting On Community Pages

Find and join some Community Pages that your target audience might frequent. Now, spend a few minutes each day to participating in the conversations there. Don't just try to sell your product. Instead take the time to help answer people's questions and maybe ask some of your own. Over time you will build rapport and can naturally bring up your product or service in conversation. This also helps build your company brand and keeps you on top of what is happening in the vertical you sell to.

Opportunity for Laser Focused Targeted Advertising.

The paid advertising opportunities on the LinkedIn website enable you to narrow down the list of individuals who will see your advertisement by vertical, company size, and employee title. If you sell B2B services, this is an amazing opportunity. Imagine the money you will save by only targeting C-Level prospects that can actually make purchasing decisions.

Advertising on LinkedIn Can Mean More Referrals

It is possible a LinkedIn advertising project might become a big part of building your brand. Even if your ad is seen by someone who can't use your services, it is possible they can become a referral source for you. People love to help their friends and will recommend services they saw online. Remember, the power of Social network advertising is the fact that it doesn't end with just one interaction. A LinkedIn advertising project might become a big part of building your brand.

No Cat Photos Means Less Garbage To Sort Through

Facebook is full of distractions. It is a place where anything and everything is marketed and it makes cutting through the noise more difficult. LinkedIn is built for business. People on LinkedIn expect to do business there so you don't have to compete for ad space and attention with the latest Farmville update.

While LinkedIn has a smaller audience that what you might find at Facebook, it is also a much more focused audience if you sell B2B products or services. Many of LinkedIn's features are free to use so go create an account and get started today.