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

Ribb"IT" Review

It is only the farmer who faithfully plants seeds in the Spring, who reaps a harvest in the Autumn.

April 2018

Issue 4, 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

Bitcoin in the Workplace - An Intro to Crypto Currency

The rise in popularity of Bitcoin and other cryptocurrencies is presenting new challenges for small and medium businesses, including security threats that can compromise company data, significantly diminish PC and network performance and adversely affect employee productivity.

The biggest obstacle to these new threats is awareness. Most business owners, while aware of Bitcoin's existence, aren't aware of how cryptocurrency is used, mined and acquired. Once found only in the realm of sophisticated programmers and computer geeks, Bitcoin and other cryptocurrencies have now caught the attention of average users, and most deadly of all, hackers looking to profit from the vulnerabilities and resources of business owners.

In this cryptocurrency primer, we'll cover the basics of cryptocurrency and what you should watch out for in order to keep your systems safe and your employees productive.

What is Cryptocurrency?

Cryptocurrency is the general term for any encrypted, decentralized digital currency. The most popularized cryptocurrency is Bitcoin, developed in 2009 by Satoshi Nakamoto and released as open-source code.

Cryptocurrencies, like Bitcoin, are exchanged in a peer to peer network, from one party to another. Each transaction is recorded in a digital record known as a "blockchain". Individuals store their cryptocurrency in a digital wallet that can only be accessed using a complex key of letters and numbers.

Developed in response to the fear sparked by the financial crisis in 2008, cryptocurrency does not rely on a bank, government or central authority. Instead, each transaction occurs between one person, directly to another person or entity, without interference from fledgling financial markets.

Each transaction of Bitcoin or other cryptocurrency is posted to a blockchain and verified by all the other computers connected to the network. This prevents the same unit of cryptocurrency from being used more than once. Transactions are completely anonymous and do not contain personally identifiable information (PII).

The most popular cryptocurrencies include Bitcoin, Litecoin, Ethereum and Ripple, though there are over 700 cryptocurrencies in circulation across the internet currently.

How Cryptocurrency Can Compromise Your Business

The process of earning Bitcoin or other cryptocurrencies is largely done through a process called mining. Mining uses cryptographic algorithms on a network of computers across the internet to register transactions on the blockchain.

Computers and servers with mining software installed can earn units of cryptocurrency in exchange for supplying the resources to carry out mining activities.

The process of mining cryptocurrency is computationally intensive and requires significant resources, usually in the form of dedicated processors, graphics cards and other hardware.

Because of the costs involved to purchase and run the hardware for mining, cryptocurrency miners often look for other ways to mine cryptocurrency, beyond the resources they have available. In some cases this means "borrowing" hardware from other users.

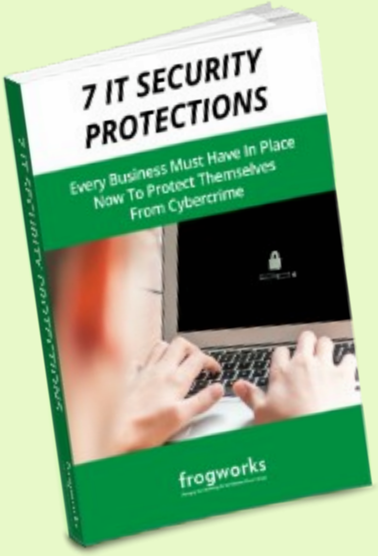
Installing Cryptocurrency Mining Software on Work Machines

Businesses should be on the lookout for Bitcoin miners or other cryptocurrency mining software installed on employee PCs. These applications utilize your company's electricity, internet connection and processing power in order to earn cryptocurrency for the employees who install it. Because these programs utilize so many system resources, they may compromise employee productivity and cause computer hardware to wear out prematurely.

Due to the increased processing power requirements, some employees choose to run the software during overnight hours and monitor the software from their home computer, like Vladimir Ilyayev, a computer systems manager for the New York City Department of Education, who was caught mining Bitcoin on his company PC in 2014. But running the software at night is still unacceptable, since an employee is still taking advantage of company resources for personal gain.

Business owners should educate their employees about the dangers of installing cryptocurrency miners on their machines and institute concrete policies regarding the consequences for doing so. Employees need to understand that you will treat cryptocurrency mining in the same way you would handle theft of materials or the doctoring of a company timesheet.

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


7 IT SECURITY PROTECTIONS
Every Business Must Have In Place Now To Protect Themselves From Cybercrime
frogworks

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

To prevent mining software installation by your employees, add safeguards to your systems to prevent software installation and run regular scans for spikes in computer activity.

Mining Malware

In addition to ensuring that your employees are not installing mining software on their company computers, companies also need to be aware of the growing threat of mining malware that can be installed and run without a user's knowledge or consent.

In the latter part of 2017, Kaspersky Lab detected several large botnets that were designed to profit from concealed cryptocurrency mining on host computers. These botnets use a variety of tactics to install mining software on victim computers from convincing unsuspecting users to click on links to exploiting software vulnerabilities on PCs within a network.

But this pervasive malware isn't limited to individual PCs. Kaspersky Lab has also observed a growing number of attempts to install mining malware on servers owned by organizations. When infiltration is successful on a company network, the data processing speed of the network can fall substantially, resulting in errors, denial of service, and lost productivity.

Proper network monitoring and the use of anti-malware programs is important to keep cryptocurrency mining software off of your network.

Cryptojacking

Unfortunately, malicious mining software doesn't need to be installed on a host computer to rack up profits for strangers all over the world. A new wave of malware, known as cryptojacking has exploded in popularity in recent months.

Cryptojacking involves injecting Javascript into compromised web pages that begin working instantly when a user loads the compromised page into their browser. Most users are completely unaware that the software is even running.

> According to Wired, "The idea for cryptojacking coalesced in mid-September [2017], when a company called Coinhive debuted a script that could start mining the cryptocurrency, Monero, when a webpage loaded. The Pirate Bay torrenting site quickly incorporated it to raise funds, and within weeks Coinhive copycats started cropping up. Hackers have even found ways to inject the scripts into websites like Politifact.com and Showtime, unbeknownst to the proprietors, mining money for themselves off of another site's traffic."

(Continued on page 4)

If You're Using Social Media, You're Ahead of the Game

CEOs range from big and popular all the way to owners of failed companies. A CEO can come in just about any package, with any personality. However, what the world is lacking is CEOs that not only are technology savvy, but social media savvy.

Recently, IBM conducted a survey that indicated that only a very small percentage – 16%, to be exact – of CEOs participate in social media. However, it appears that in the next five years, the number will climb from 16% to 57% because CEOs are starting to realize that one of the best ways to reach their audiences is to venture online.

"As CEOs ratchet up the level of openness within their organizations, they are developing collaborative environments where employees are encouraged to speak up, exercise personal initiative, connect with fellow collaborators, and innovate," the IBM study stated.

If your CEO participates in social media networking, it can make the company more competitive as a whole – and more relatable, too, which is key in building solid relationships with potential clients.

Still not convinced? Social media is the second most used engagement method with clients, only outclassed very slightly by face-to-face interactions. More than half of CEOs are planning on bringing technology on board to help them partner with other organizations to promote their businesses. Maybe most impressive of all is the fact that most of these CEOs are not planning to toss the social media ball to another member of their organizations; many CEOs indicated that they were going to learn the systems themselves and "lead by example".

That is how absolutely important learning and using social media is: CEOs are planning on taking time out of their very busy schedules to learn something new.

If a company wants to stay competitive, it must evolve, and this idea is reinforced by the IBM study. To gain a client's trust, a company must act on a personal, intimate level, which means a lot is at stake when it comes to social media. No more are the days of tall towers with CEOs hidden at the top because they hired someone else to interact with clients – coming soon are the days of friendly, straightforward, honest interactions with the people a company wants to do business with.

(Continued from page 3)

Fortunately, there are ways to protect against cryptojacking, according to Wired. "You can add sites you're worried about, or ones that you know practice in-browser mining, to your browser's ad blocking tool. There's also a Chrome extension called No Coin, created by developer Rafael Keramidas that blocks Coinhive mining and is adding protection against other miners, too."

With the rise of Bitcoin and other cryptocurrency mining, it's more important than ever to make sure your network is protected for maximum performance. Preventing employees from installing Bitcoin miners, educating your employees about the dangers of cryptocurrency mining software and developing iron-clad network security procedures will go a long way to keeping cryptocurrency mining software off of your systems.

If you have questions about cryptocurrency mining software or are concerned about the vulnerability of your network or company PCs, FrogWorks is always here to help. We've been helping business owners secure their networks since 2002!

Annoying Things on Your Website that Will Drive Business Away

Chances are that you have worked very hard on your website. You're probably proud of it, but that doesn't always mean the design and "feel" of the website are optimal. To drive more clients to buy while they're visiting your website, you have to make sure you don't annoy them on accident. Here are a couple of things that are commonly used on websites that just aren't good for business.

Flash

Flash can be used in a good way, but most of the time it just means annoyance for your customers. They often take forever to load (especially on slow connections) and don't provide a lot of information to your website visitor. You want to use your website space wisely; instead of having a Flash intro, write some interesting and helpful content and post it where you had the intro instead.

Hiding Your Contact Information

Your potential clients are likely very busy people. Routing around your website for contact information not only takes up time, it's a frustrating process. A lot of the time, it'll convince your almost-client to go to another website that clearly states a number (or an e-mail) at the top of every page that can be used to contact the company.

Pop-Ups

Most people think 'ads' when they think pop-ups, and those are obviously irritating. However, there are other types of pop-ups. For example, what about a pop-up that tells you about a new ebook that the website has produced? Or one that tells you that you'll get a discount if you don't click on the "x" button in the corner? These pop-ups are just as bad and very unprofessional. The take away the air of simplicity and style your website might otherwise have.

Music

A lot of people like music, but not everyone likes the music you like. Putting any sort of sounds on your website that can't be stopped will cause most people to click back to the search engine page. Playing music on your website (or auto-starting a video that can't be stopped until someone locates the pause button) is often viewed as downright rude and disruptive. Instead, kill the music, and make sure your videos have to be started manually.