BSSi2 Innovations

Review Twice, Implement Once. Doing IT Right the First Time.

On the Lighter Side

What do you call a kid who doesn't believe in Santa?
A rebel without a Claus

How much did Santa pay for his sleigh?
Nothing. It was on the house!

What's every parent's favorite Christmas Carol?
Silent Night

Why do Christmas trees like the past so much?
Because the present's beneath them

What do you get when you mix a Christmas tree and an iPad? *A pineapple!*

What's St. Nicholas's favorite measurement in the metric system? *The Santameter!*

I love when they drop the ball in Times Square …
... It's a nice reminder of what I did all year.

My New Year's resolution is to be more optimistic by keeping my cup half-full …
... with either rum, vodka, or whiskey.

2020 was a unique Leap Year. It had 29 days in February, 330 days in March, and 5 years in April.

Can you believe Tiger King was the most normal part of 2020?

Check on your conspiracy theory friends, they haven't had a day off in months.

Year End Thank You to You, our Clients

Here is the obvious: 2020 was not particularly a good year for the state, country, or the world. We are all tired of hearing about COVID/Coronavirus… masks, lockdowns, social distancing, Zoom/Teams, PPP, PPE, etc. You get it. When will it all stop?

The vaccines are on the way. But we all are wondering "When can I get my shots and what kind of aggravation do I have to go through to get it on a timely basis?" The logistics for this is incredible. Add to that we may have to do it twice since some of the vaccines require two shots. AAAHHH!

Will 2021 be better? Another obvious answer – "We hope so!" If you or someone you are close to has suffered through a COVID infection, we wish for fast and hopefully easy recovery. No one deserves this but we all are at risk.

Through all the hardship, aggravation and inconvenience, we want to say THANK YOU to our clients, trusted alliances, vendors, and staff. We are not aware of any clients having to close down their business, which is amazing news. You continued to trust in BSSi2 to oversee your IT and cybersecurity needs. You have helped us weather this storm, as I hope we have helped you. Your trust in us has allowed us to not only maintain our staff but to grow our team to better service you. We are moving forward so we can continue to help you.

THANK YOU, FROM THE ENTIRE STAFF OF BSSi2! May 2021 be safer, easier and prosperous for all of you. Happy Holidays, stay safe and get vaccinated when you can.

Scott Bernstein, Nick Espinosa,
and the entire staff of BSSi2

Cybercriminals Confess:
The Top 3 Tricks And Sneaky Schemes They Use To Hack Your Computer Network That Can Put You Out Of Business

Cybercriminals and hackers are rarely shy about the methods they use to attack their victims. Many of them are more than happy to share how they broke into a business's network or how they walked away with thousands of dollars after successfully extorting a business owner whose company is now destroyed.

There are new stories out there to get your blood boiling as cybercriminals work to ruin people's lives and livelihoods. These criminals don't care what kind of damage they do. They only care about one thing: money. If they can get away with it – and many do – they'll keep on doing it.

It's up to the rest of us as business owners (and employees) to stay at least one step ahead of these cyberthugs. The single best way to do that is to stay educated on the latest threats. The second-best way is to stay up-to-date with the latest technology designed to combat cyber-attacks.

Here are three tricks of the trade cybercriminals are using right now in an attempt to get their hands on your money:

Ransomware. This is very common. It's a form of malware, and it can sneak onto your network and into your computers in a number of different ways:

- **Ad Networks.** These ads can appear on social media sites and on familiar websites. Someone clicks a compromised ad or pop-up, and it initiates a file download. It's quick and it can be confusing. This is where anti-malware and anti-ransomware come in very handy.
- **Malicious Links.** The cybercriminal sends you a legitimate-looking e-mail, supposedly from your bank or a familiar online store. It may even be disguised as an e-mail from a colleague. The e-mail contains a link or file. If you click the link or file, it installs the ransomware.
- **Hidden Files On Thumb Drives.** This happens way too often where someone brings a thumb drive from home. While the user doesn't know it, the drive has a malicious file on it. When the thumb drive is inserted into a networked machine, the file is installed.

No matter how the ransomware gets onto your devices, the result is basically the same. The ransomware goes to work and begins encrypting your files. Or it may completely block you from accessing your computer altogether. You'll get a full -screen message: Pay up or never access your files again. Some ransomware programs threaten to delete all of your files. Others say they will never restore access.

DDoS Extortion. Short for distributed denial of service, DDoS attacks are a relatively easy way for hackers to take down your business's online presence and wreak havoc on your network. These attacks mimic online users and essentially "flood" your network with access requests. Basically, it's as if millions of people were trying to access your website at once.

Your network simply can't handle that kind of traffic and, as a result, it goes down. The hackers can continue the attacks until you take action. That is to say, until you pay up. If you don't pay up, the hackers will do everything they can to keep you offline in an attempt to destroy your business. If you rely on Internet traffic, this can be devastating, which is why many businesses end up paying.

Direct Attacks. Some hackers like to do the dirty work themselves. While many cybercriminals rely on bots or malware to do the work for them, some hackers will see if they can break through your network security in a more direct way. If successful at breaking in, they can target specific files on your network, such as critical business or customer data.

Once they have the valuable data, they may let you know they have it. Sometimes they'll ask for money in return for the sensitive data. Sometimes they won't say anything and instead simply sell the data on the black market. Either way, you're in a bad position. A criminal has walked away with sensitive information, and there is nothing you can do about it.

Except, that last sentence isn't true at all! There are things you can do about it! The answer is preventative measures. It all comes around to these two all-important points:

- Stay educated on the latest threats
- Stay up-to-date with the latest technology designed to combat cyber-attacks

If you do these two things and work with an experienced IT services company, you can change the outcome. You can put the cybercriminals in their place and have a digital defense wall between your business and those who want to do your business harm.

Ransomware is Growing and Getting Worse... Are You Prepared

by Scott Bernstein

We are paranoid about infections and ransomware, and you should be too. It is an easy, cheap and profitable venture for cybercriminals. They don't care how big or small you or if you have cash in the bank. Pay up or suffer the consequences.

Can you stop ransomware?

How to stop such infections is the ongoing question. **No solution is 100% guaranteed;** if you encounter anyone making such a claim, run away from them. You can put up barriers and layers to make it more difficult for the bad guys and that is what we stress to our clients.

The protections that were recommended years ago and are probably still in place may not be adequate. The criminals are more sophisticated, have better tools and have learned how to get around many of the protections that were in place. Antivirus applications often are too easy to evade, simple firewalls will not stop a determined criminal. And don't forget your weakest link, your staff. Phishing emails look legitimate and don't always get caught by spam filtering applications; they sometimes just do not appear to be a risk.

I hate to be the bearer of bad news, but more sophisticated and advanced protection will cost more. The free antivirus programs and retail store firewalls and those integrated into internet modems do not cut it anymore. We know it hurts to put these protections in place, we hate it too. We have invested in the protections that we recommend. We know we are not guaranteed to never get infected, but we have greatly reduced our attack surface; so should you.

Ransomware has gone to new level

Ransomware has gone to a new level. Ransomware has increased by over 700% in 2020 and the cybercriminals have added a second level to their demands. Not only do they require you to make a payment to free up your files but now they ask for another ransom or **they will make public any private or confidential information they steal from you**. Before they were content with just encrypting your data, now that want money to keep that data private.

Why do you need this protection?

Before you dismiss the need for the added spending, keep a few things in mind:

- How inconvenient is it if your bank account or investment are reduced to zero?
- How happy will management be if you make a payment to a vendor's "new" bank account that was not really to your vendor, and you still owe them the money?
- How surprised will you be when your cyber insurance carrier refuses to pay since you did not have all the protections in place you claimed you had?
- How productive will your company be if a ransomware infection shuts you down for a week?
- What will become of your reputation if client data is published on the internet?

Any cost you expend to protect against these will be less expensive than the actual damage caused by the infection. The average ransomware cost in 2019 was $5,900 and is expected to go up, again. Downtime costs are up 200% and the average downtime cost is 23x greater than the average ransomware request in 2019. 1 in 5 small businesses report they have fallen victim to a ransomware attack.

What can you do to reduce your chances of an infection (reduce, not eliminate)?

What can you do to put barriers between your data and cybercriminals? Remember, these recommendations make it more difficult to infect you but not impossible. You have to decide how far to go, but cyber insurance carriers will be looking to make sure you implement what you say you have.

- A cybersecurity assessment of your environment. Too often companies want to bypass this step and jump straight to adding products for protection. This would be a mistake as policies and procedures can help cut down on staff errors and confusion. What we have seen is such assessments will often recommend the additional items noted below.
- Next generation monitored endpoint protection (the new wording for antivirus protection)
- Next generation monitored firewall with integrated layers of protection applications
- Enterprise level spam filtering
- Implement two-factor authentication (2FA) for any cloud-based application, if possible
- Security Awareness Training, to help staff recognize bad emails
- For remote access to your network, use either VPN or business grade remote access software with 2FA enabled
- Frequent, offsite, disconnected and tested backups. This is for recovery of ransomware; it is not a barrier to protection and does not stop a criminal from publishing confidential data.

Cybercrime is not going away, it is too profitable. Even the mafia is a player for this activity. You have to decide how paranoid you are about your data and network protection. BSSi2 is here to assist and provide recommendations. But you have to make the decision to act.

December 2020

35 Aztec Court
South Barrington, IL 60010
(312) 752-4679
www.bssi2.com

"We make all of your computer problems go away without the cost of a full-time I.T. staff"

"Sorry about this. I wanted to email or text you my list, but she insisted on a picture."

Shiny New Gadget of the Month

SelfieSpin360 For GoPro

A GoPro camera is great for a crystal-clear, wide-angle video of yourself or your subject, and you can attach it to the end of a selfie stick for some nice static shots, too. But if you're ready to take things up a notch and capture even more truly awesome moments, then you need the SelfieSpin360.

It's all there in the name: the SelfieSpin360 gives you a way to get incredible 360 degree footage of yourself in any setting. You attach your GoPro or smartphone to the end of a sleek and secure base, which is attached to a long cord with a handle for camera controls on the end. Hit Record, then start swinging the device up and around your head lasso-style to capture a unique version of yourself in a special moment. The SelfieSpin360 kicks boring old selfies to the curb.
Visit SelfieSpin360.com to purchase yours.

Stay up-to-date with the latest Cybersecurity News!

Follow our Chief Security Fanatic and CIO, Nick Espinosa, on social media for cybersecurity videos and articles:

f www.facebook.com/NickAEsp

twitter.com/NickAEsp

in www.linkedin.com/in/nickespinosa/

Follow BSSi2 at:

f www.facebook.com/bssi2

twitter.com/BSSi2llc