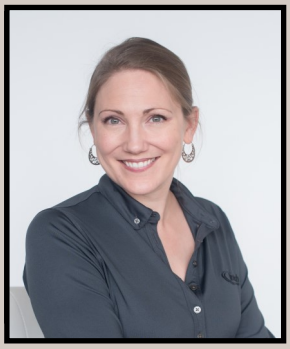
InTech Intelligencer

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"



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

- Leia Shilobod,
President & I.T. Princess of Power

Inside This Issue…

InTech SOLUTIONS

One Northgate Sq., Ste. 202
Greensburg, PA 15601
724.235.8750

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.

Continued on pg.2

Continued from pg.1

- **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:

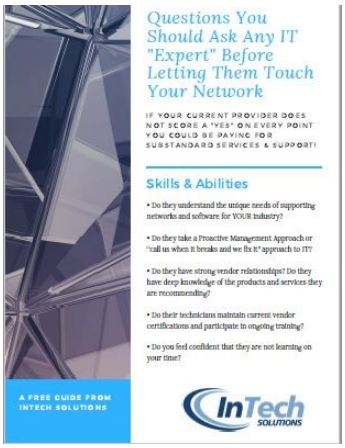
- Stay educated on the latest threats
- Stay up-to-date with the latest technology designed to combat cyber-attacks

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.

Call today to schedule a Cyber Security Risk Assessment for your business. 724.235.8750 or email Leia@intechit.net.

"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."

Free Report Download:
Questions You Should Ask Any IT "Expert" Before Letting Them Touch Your Network

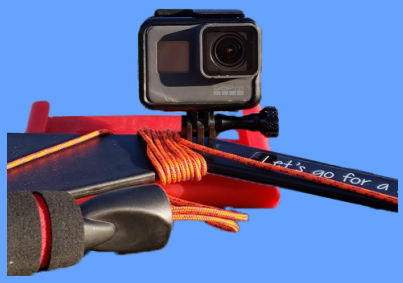


How can you tell if you are going to receive poor or substandard service? How do you know if your computer guy or network consultant is doing everything possible to secure your network from downtime, viruses, data loss or other frustrating and expensive disasters? Could your current provider actually be jeopardizing your network?

This valuable Free Report helps you avoid common pitfalls of choosing an IT Provider. Download yours today!

Claim Your FREE Copy Today at www.intechit.net/whattoask

Shiny New Gadget Of The Month:

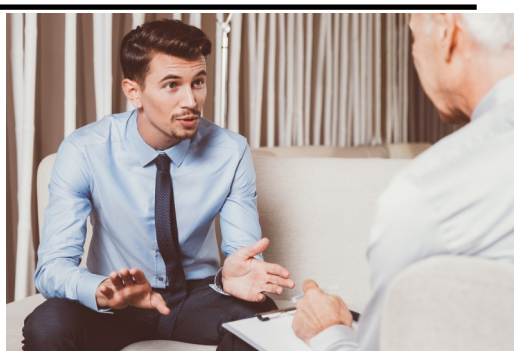


SelfieSpin360 For GoPro

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.

Successfully Convince A CEO In 3 Steps



Here is your chance. You don't want to blow it.

You have a meeting scheduled with a CEO. Your goal is to convince them...

- To spend $1 million on your product or service or to make a large donation to your cause
- To hire you, promote you or give you your dream job
- To invest in your idea

Ineffective Ways To Convince A CEO

Many people "show up and throw up" and push a lot of information at the CEO — either verbally or by PowerPoint. I'm not sure why so many unpersuasive people follow this approach. Maybe it's to "show you know what you are talking about." But it does not make a CEO say "yes."

Another bad approach is to phrase your request as a "we ought to." CEOs don't decide to do things just because other people say they ought to do something. Or worse yet is when people only talk about why they want something to happen, fully ignoring the wishes, concerns and perspective of the CEO.

Successfully Convince A CEO In 3 Steps

1. Seek first to understand the CEO's perspective — that is Stephen Covey's advice. It needs no further explanation. Your first step in discussing a topic with a CEO is to put all your energy into asking probing questions, listening and learning what the CEO thinks about a topic and why. Forget about your agenda or your needs for a moment.

2. Reflect the CEO's perspective to their satisfaction. This step is hard. Most people cannot objectively reflect or restate another person's perspective about a topic without putting their own personal slant on it. I first learned this step during my psychology PhD training in a class on conflict resolution. At this step, you must restate the CEO's perspective on the topic simply and without putting words in their mouth or trying to spin it in your favor. You know you have succeeded at this step once the CEO says the magic word. The magic word is "exactly." This means that the CEO believes that you understand their perspective. Then, and only then, have you earned permission to move to the final step.

3. Propose your idea as a way to help the CEO achieve their goals. The mindset for this step is not that you are about to trick or fool a CEO into doing something that's not good for them. Your mindset is that you are about to convince a CEO to do something that is good for them. (And by the way, if what you are about to propose is not in the CEO's best interest, then don't propose it!) A simple way to propose your idea is to say, "Your goals are X. Your concerns are Y. So, I propose you do Z."

And, contrary to popular belief, great ideas don't sell themselves. It takes a skillful leader to successfully convince a CEO.

Geoff Smart is chairman and founder of ghSMART. Geoff is co-author, with his colleague Randy Street, of the New York Times best-selling book *Who: A Method For Hiring* and the author of the #1 Wall Street Journal best seller *Leadocracy: Hiring More Great Leaders (Like You) Into Government*. Geoff co-created the Topgrading brand of talent management. He is the founder of two 501(c)(3) not-for-profit organizations. SMARTKids Leadership Program™ provides 10 years of leadership tutoring, and the Leaders Initiative™ seeks to deploy society's greatest leaders into government. Geoff earned a Bachelor of Arts in Economics with honors from Northwestern University and a Master's and Doctorate in Psychology from Claremont Graduate University.

Who Else Wants To Win A $25 Gift Card?

You can be the Grand Prize Winner of this month's Trivia Challenge Quiz! Just be the first person to correctly answer this month's trivia question and receive a $25 Visa gift card Ready?

How many bits make a byte?

- **A) 16 bits**
- **B) 8 bits**
- **C) 24 bits**
- **D) 12 bits**

Email us right now with your answer!
info@intechit.net

InTech SOLUTIONS
One Northgate Sq., Ste. 202
Greensburg, PA 15601

US POSTAGE
PAID
GREENSBURG, PA
PERMIT NO. 1117

- RETURN SERVICE REQUESTED—

"There Is Nothing Magical About January 1"

Do you notice that we always seem to think things will be better in the future? In a different time, or a different place? On social media memes about how 2020 was awful and how 2021 is going to be "my year." Christmas ornaments abound showing things like a dumpster fire with "2020."

Let me tell you folks, there is nothing magical about January 1. The Winter Fairy isn't going to fall from the sky with the white snow and tap you on the head so 2021 is full of wealth, happiness, and joy.

Now I know that logically you know this. But deep inside we keep telling ourselves stories like this and those stories unconsciously impact our daily actions. Those daily actions manifest our future. What happens to you is no accident. It is the cumulation of small choices you make at each moment each day.

So, what does this all mean anyway? You have the power at every moment to CHOOSE the way you interpret a situation. You have the power to CHOOSE the actions to take (or not take) in response to that interpretation.

Nothing is magically going to happen on January 1. So right now, at this very moment, make the CHOICE to "looks things in the face and see things as they are" and not create a judgement about them.

PS – If you're interested in training your mind to think this way more often, check out "The Daily Stoic" by Ryan Holiday and "The Practicing Stoic" by Ward Farnsworth. And don't get down on yourself if you find yourself falling into your old ways. The titles of these books contain "daily" and "practice" for a reason!

To Your Success,

Lisa