THE BeckTek Journal

May WannaCry

May saw hackers use leaked NSA Cyber-Weapons to create a virus that became the fastest spreading malware hitting over 150 countries and infecting hundreds of thousand of computers in mere hours. This is the new cyber-world we find ourselves living. Thinking bad things would never happen to you, just happened of hundreds of thousands. If you were spared this time around, don't rejoice yet, there are more malware variants—roughly 390,000 a day–being found. Thinking a good firewall and Anti-Virus is enough protection all well behind us. The bad guys have proven they can digitally monetize and automate all forms of crime in the digital world: Ransom, Blackmail, & Identity Theft to name a few. We're going to focus on some tips to help protect yourself, your business and family this month. **Free Cyber-Security tips** are also available at: https://goo.gl/rqgPO4

June 2017

This monthly publication provided courtesy of Scott Beck , President

"As a business owner, I know 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 once and for all!"

No matter how "bomb-proof" we make your network, you and your employees can still invite a hacker in if you click on a link or open an attachment in an e-mail sent by a cybercriminal. Some spam is obvious (can you say, "Viagra at a discount"?) but others are VERY cleverly designed to sneak past all the filters and trick the recipient into opening the door. Known as a "phishing" e-mail, this still is the #1 way hackers circumvent firewalls, filters and antivirus, so it's critical that you and your employees know how to spot a threatening e-mail. Here are four types of e-mail ploys you should be on high alert for.

The Authority E-mail. The most common phishing e-mails are ones impersonating your bank, the Canada Revenue Agency or some authority figure. The rule of thumb is this: ANY e-mail that comes in where 1) you don't PERSONALLY know the sender, including e-mails from the CRA, Microsoft or your "bank," and 2) asks you to "verify" your account should be deleted. Remember, ANY important notification will be sent via old-fashioned snail mail. If it's important, they can call you.

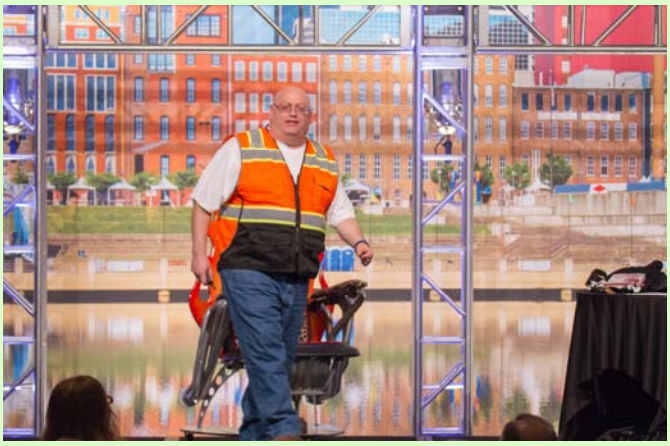
The "Account Verification" E-mail. Any e-mail that asks you to verify your password, bank information or login credentials, OR to update your account information, should be ignored. No legitimate vendor sends e-mails asking for this; they will simply ask you upon logging in to update or verify your information if that's necessary.

The Typo E-mail. Another big warning sign is typos. E-mails coming from overseas (which is where most of these attacks come from) are written by people who do not speak or write English well. Therefore, if there are obvious typos or grammar mistakes, delete it.

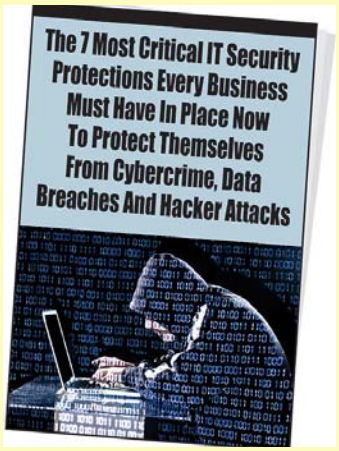
The Zip File, PDF Or Invoice Attachment. Unless you specifically KNOW the sender of an e-mail and have verified it's from them, never, ever open an attachment. That includes PDFs, zip files, music and video files and anything referencing an unpaid invoice or accounting file (many hackers use this to get people in accounting departments to open e-mails). Of course, ANY file can carry a virus, so better to delete it than be sorry.

Call Us To Cut Down On 99% Of The Spam E-mails You're Getting Call us this month and we'll come onsite to perform a free spam-protection analysis. Simply contact us today at **506-383-2895** to reserve yours. Do it now... before a ransom demand -or worse - shows up in your inbox.

Scott Working the Stage in Nashville, speaking before 1100+ IT Peers at the May TMT Mastermind Peer Group Meeting



FREE REPORT: The 7 Most Critical IT Security Protections Every Business Must Have In Place Now To Protect Themselves From Cybercrime, Data Breaches And Hacker Attacks



This report will outline in plain, nontechnical English the #1 Threat to your business that even the BEST firewalls and anti-virus software can't protect against and other common mistakes that many business owners make with their computer network that leave them exposed to cyber-attacks that can cost thousands in lost sales, productivity and expensive computer repair bills, as well provide easy, proven ways to reduce these risks and financial exposures caused by these oversights.

Download your FREE copy today at:
www.becktek.ca/7protections_cybercrime

OR call our office at 506-383-2895 to request your copy.

Shiny New Gadget Of The Month

Surface Studio: All Beauty, A Little Brains

"We want to move from people needing Windows…to loving Windows."

So said CEO Satya Nadella after taking over Microsoft. And their new Surface Studio takes a bold step in that direction.

In a bid to win over creative types, they designed the Studio with a gorgeous desktop screen that easily glides from vertical to almost horizontal, like an artist's sketchpad. With its Apple Computer-like brushed aluminum finish and ultra-thin screen, it's feels right at home in an open-plan office with microbrews on tap.

The guts of the machine are stuffed into a nine-inch-long base that's joined to the screen with an überslick hinge design, allowing it to fold nearly flat for stylus- or touch-driven design work.

Downsides? Well, you'll pay at least $3,000. And it's a bit underpowered to be in that price range. But all in all, even the graphically challenged will find this machine tantalizing.

Time to Get Vulnerable

When you hear the term "leader," adjectives like strong, assertive, and powerful come to mind. But what about vulnerable? Those in leadership positions often believe that displaying vulnerability to their team is a sign of weakness.

I'm here to tell you that they couldn't be more mistaken. In reality, vulnerability is a strength, and all skilled leaders have it. And in order to help you grow into a better leader, **I want you to be vulnerable**.

Patrick Lencioni once said to me, "Start by coming to terms with your own vulnerability as a leader and then translate that to your team and then the rest of the organization." Waldo Waldmen, a top fighter pilot and a good friend of mine, once said something similar. He explained that after every mission, they would have a debriefing. Before it started, everyone was required to take off their name tags and their rank. Now, with an even playing field, they would go over the good, the bad, and the ugly of the mission. The leader would take the lead, admitting their own mistakes first.

They call this "exposing your chest to daggers," and it creates an environment for the new hires, the young wingmen, and the young folks that are in the formation to say, "You know what? If so and so, the flight lead, or so and so, the top gun, is going to share his or her mistakes, then I can do the same thing." But it has to come from the top down, and it means being vulnerable, more honest, and more open about what's going on. Waldo said the key is to show you are a human being first and a top gun or high-ranking officer second.

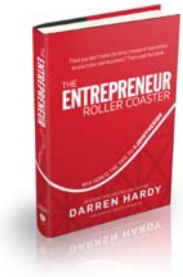
Do you start meetings by exposing your mistakes first?

I'm not talking about being passive-aggressive. "I never should have trusted so and so with this." I see and hear that all the time, and it's the opposite of exposing your chest to daggers. I'm talking about where you underperformed, did something wrong, or made a bad call. Those are the things to expose.

Many years ago, Les Brown gave me some great advice. He said, "You are a compelling speaker and certainly you have had a tremendous track record of success — but you can't just talk to people's heads or only appeal to their intelligence." He continued, saying, "They have to feel your story, the whole story — failures, shortcomings, fears, and pitfalls — both the triumphant and the terrible." That, he told me, was what would make me a real leader.

As you can imagine, this was an awakening, and it changed my life. You'll notice it if you read my first book and my new one; "The Entrepreneur Roller Coaster" is a lot more honest about my personal journey, warts and all. While people may be inspired by your success, they are empowered by knowing that they can fail at times and still succeed wildly.

If you want to be a leader, open yourself up to others. If people can feel and connect with you, they will charge through walls for you. That is real leadership, real influence, and real achievement. So, right now, think of one failure with which you can open up to your team.



Are you in? I promise you will see immediate results.

Darren Hardy is the creator and visionary behind SUCCESS magazine as well as the NYT-bestselling book "The Compound Effect." His newest book is "The Entrepreneur Roller Coaster." For more, visit darrenhardy.com.

The Lighter Side...

How's Your Job?

Q. How's your job at the clock company?
A. Only time will tell.

Q. How's your job at the banana company?
A. I keep slipping up.

Q. How's your job on the new highway?
A. I'm so busy I don't know which way to turn.

Q. How's your job at the travel agency?
A. I'm going nowhere.

Q. How's your job at the swivel chair company?
A. It makes my head spin!

Q. How's your job at the lemon juice company?
A. I've had bitter jobs.

Q. How's your job at the pie company?
A. It didn't pan out.

Q. How's your job at the balloon factory?
A. We can't keep up with inflation.

Q. How's your job at the crystal ball company?
A. I'm making a fortune.

Q. How's your job at the history book company?
A. There's no future in it.

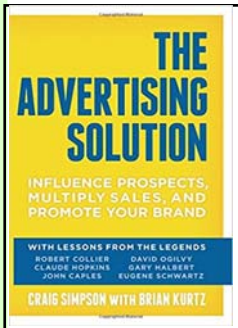
Q. How's your job at the clock company?
A. I'm having second thoughts about it.

Q. How's your job on the farm?
A. Problems keep cropping up.

Quote of the Month:

"Success is a little like wrestling a gorilla. You don't quit when you're tired. You quit when the gorilla is tired."
— Robert Strauss

Do What You Do So Well
That People Can't Help Telling Others About You



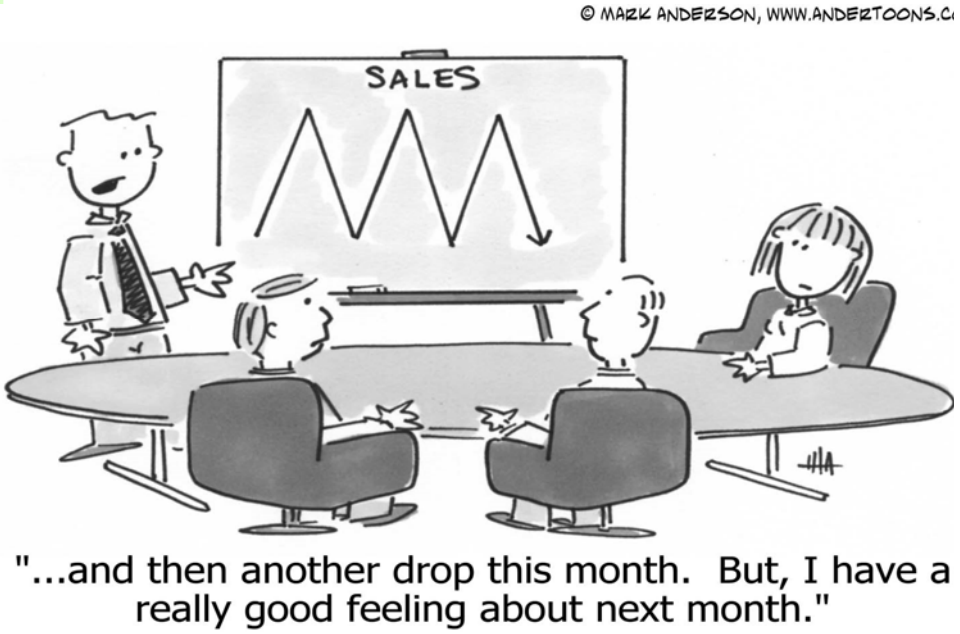
What We Are Reading

First glance at the title and you might think this isn't for me, I'm not in advertising. Yet the book proves we all are, as we are all trying to present ideas to others in one way or another.

The book features the work of 6 of the world's greatest advertisers of all time—the real "Mad Men" the TV show was based around. Yes, there are great lessons in how to market your business to develop sales (a bonus if you own a business owner!!) however it deals a lot with how people think, react and interact with others.

The authors, **Craig Simpson** and **Brian Kurtz** present the knowledge in an easy to understand way and bring forward the concepts of yesteryear into the modern day world. If you are presenting ideas to teams, looking for employment or trying to develop your business through advertising—this book will help assist in how to present yourself and your ideas in a manner that increases the likelihood of them being accepted.

Be the first to email me the title of the book to scott@becktek.ca and I will send you a free copy of the book



Mike Rowe

Larry Winget

May Mastermind Meetings and The Hidden Business Dangers Of "Shadow IT"

Mike Michalowicz

Jack Daly

In May I had the pleasure of hosting the meetings for the IT Mastermind group I belong to in Nashville. For those that may not know, I spent 15 years in Radio Broadcasting and have had to get on stage in front of thousands, and it appears public speaking in front of large crowds is like riding a bike, you don't forget…thankfully!!

As an added bonus I got to meet and talk with the amazing speakers including:

Mike Rowe, host of Dirtiest Jobs and Deadliest Catch. His talk on how Dirtiest Jobs came about was hilarous. He is well educated and cultured – even singing Opera and Happy Birthday to a member celebrating his 70th birthday. Also, he got his big break hosting on the QVC TV sales network on the all night shift, because he was able to talk about the benefits of a pencil for 8 minutes—his quick thinking and ease of speaking landed him the job

Larry Winget is a 6 time best selling author, TV celebrity and social commentator. His talk about the need to just work to reach your goals, was direct and in your face and SO right. He encouraged folks to stop whining and thinking they are entitled to things, that you need to get to work and "Grow a Pair" which happens to be the name of his latest book.

Mike Michalowicz is a best selling author, former IT guy, frequent contributor regarding business financial matters on MSNBC and has had a profound positive impact on BeckTek. His books The Pumpkin Plan and Profit First should be must reads for growth orientated business owners.

Jack Daly is a master at building culture and sales departments within companies and wore me out watching him work on stage. He is an Ironman that frequently participates in Triathlons, oh did I mention he is closing in on 70 years young? I've featured his book **Hyper Sales Growth** as book of the month previously, a really great read.

It truly was an amazing experience to share the stage with these gentlemen. There message provided many opportunities for learning and I enjoyed each of their speaking styles and picking up some extra tips and tricks of the trade.

One of the hot tech topics at the conference was "Shadow IT", technology your employees are using that isn't part of your official IT plan. We're talking about messaging apps, Excel macros, cloud data storage, collaboration spaces, and even hardware like USB drives, smartphone storage, and personal laptops that you don't control. Even if you ignore the dangers of having accounts hacked, data stolen, and websites vandalized, shadow IT can be very inefficient. You don't control it, so you don't know where important information is or what work is being done. It makes it hard to avoid duplication of efforts and even harder to manage employee productivity.

What are you to do?

Well, your gut reflex might be to "crack down" on using unauthorized technology for work purposes. Swallow that reaction, though - you can't stop it, and you'll just harm morale and your people won't be honest with you for fear of reprisal. That means that if a compromise occurs, you'll be the last to know. ***Continued on next Page***

In some cases, you will have to crack down on specific apps, programs, or devices being used at your work; they're just too risky. Remember to avoid blaming employees when shadow IT becomes a problem - especially if they bring the issue to your attention themselves. There's nothing wrong with asking your people to stop using a specific program or device, as long as you're transparent and have good reasons.

Last, but not least, try to look on the bright side. If they're using a piece of technology, it's probably doing something that the currently "approved" tech is not. They're also showing self-starter tendencies and trying to do their job better and be more productive.

The key takeaway was "Shadow IT" is risky however the benefits can offset that risk as long as you know what is being used, do your research on associated risks and work to integrate them into your network and data security planning if you decide the use is acceptable.

Anti-Virus Is DEAD

The Problem With Anti-Virus (AV)

By design, AV relies on virus definitions to protect us. Meaning the **AV software must already KNOW about the threat in order to stop it.** With upwards of 390,000 new threats variants being discovered daily, it's just a matter of time before you stumble across a new virus you aren't protected against.

Current trend of discovery of a new threat to a fix being developed is running around 100 days (sometimes more). That means for over 3 months, you are at risk of the new infection before you get protection. NOT great odds. This model of security simply can't keep pace with the threats—the numbers don't work.

As we saw with the recent headlines the WannaCry ransomware virus "scrambled" infected files so you couldn't open them and then demanded money before the bad guys would "unscramble" them. In the business world this is compounded as viruses spread across corporate networks, so instead of one person getting hit it can be the whole company. Talk about oodles of lost productivity, downtime, lost sales, damaged reputations and major repair bills to try and recover!!

Advanced Endpoint Protection - Why You Should Care

After much research and testing, the solution we found is called **Sentinel One,** a new breed of security software that has been used for quite some time by large organizations like Nasdaq, Walmart, and Netflix and now we've found a way to make it affordable and available to companies with less than 500 computers.

The three major benefits of this new form of protection include:

1) It's **Behavior Based**, meaning it doesn't have to know about a threat to protect against it. If a Word document you just opened from an email attachment calls out to servers in several different countries, tries to download and install software—it knows this isn't normal Word document behavior and would stop it from happening.
2) It has **Built in Forensics**, so if something slipped by, we can tell what file caused the issue and what other files it touched. Meaning, for Canada's new Data Breach laws, we'll know what was actually compromised and to what extent. We'll also know where the threat originated from and potentially what staff member needs a refresher on Cyber-Security
3) **Roll Back Feature** – this isn't a backup, however it does track files changes (as noted in the forensics mentioned above) and allows us to roll back any changes a virus was to make to files – meaning instead of hours or days of expensive downtime it would be more like minutes.

To learn more on how to better protect your computer systems and business, give me a call: 506-383-2895 or email me: scott@becktek.ca