TECHNOLOGY TIMES

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

What's New

Interested in a FREE YETI Tundra 105?

See page 2 for more information!

July 2017

This monthly publication provided courtesy of Rick Johnston, President of Information Management Systems

"Enabling People to Provide Great Products and Services - Anytime, Anyplace, Anywhere"

The Dirty Loophole That Lets Insurance Companies Refuse to Cover a Cybercrime Theft in Your Business

As hacking hit the headlines in the last few years — most recently the global hack in May that targeted companies both large and small — insurance policies to protect businesses against damage and lawsuits have become a very lucrative business indeed. Your company may already have cyber insurance, and that's a good thing. But that doesn't mean that you don't have a job to do — or that the insurance will cover you no matter what. When you buy a car, you get the warranty. But in order to keep that warranty valid, you have to perform regular maintenance at regularly scheduled times. If you neglect the car, and something fails, the warranty won't cover it. You didn't do your job, and the warranty only covers cars that have been taken care of.

Cyber insurance works the same way. If your company's IT team isn't keeping systems patched and up to date, taking active measures to prevent ransomware and other cybercrime attacks, and backing everything up in duplicate, it's a lot like neglecting to maintain that car. And when something bad happens, like a cyber attack, the cyber insurance policy won't be able to help you, just as a warranty policy won't

cover a neglected car. Check out this real life policy exclusion we recently uncovered, which doesn't cover damages "arising out of or resulting from the failure to, within a reasonable period of time, install customary software product updates and releases, or apply customary security-related software patches, to computers and other components of computer systems." If your cyber insurance policy has a clause like that — and we guarantee that it does — then you're only going to be able to collect if you take reasonable steps to prevent the crime in the first place. That doesn't just mean you will have to pay a ransom out of pocket, by the way. If your security breach leaves client and partner data vulnerable, you could be sued for failing to protect that data. When your cyber insurance policy is voided because of IT security negligence, you won't be covered against legal damages, either. This is not the kind of position you want to be in.

"If your company's IT team isn't keeping systems patched and up to date, taking active measures to prevent ransomware and other cybercrime attacks, and backing everything up in duplicate, it's a lot like neglecting to maintain that car."

All of this is not to say that you shouldn't have cyber insurance, or that it's not going to pay out in the case of an unfortunate cyber event. It's just a reminder that your job doesn't end when you sign that insurance policy. You still have to make a reasonable effort to keep your systems secure — an effort you should be making anyway.

Contact us today about Cyber Security insurance. Call us at 701-364-2718 or email info@imsnetworking.com.

Do you want this YETI Tundra?

We love having you as a customer and, quite honestly, wish we had more like you! So instead of just wishing, we've decided to hold a special "refer a friend" event during the summer.

Simply refer any company with 10 or more users to our office. We will call and schedule an appointment. When we get the appointment we will send you a YETI Tumbler. If the referral you submitted becomes a client, you will receive a YETI Tundra 105 ($479.99 value!).

To submit a referral please go to: http://www.imsnetworking.com/about-us/referral-program/ or email info@imsnetworking.com

Shiny New Gadget Of The Month:

Alexa, Who's Winning the Virtual Assistant War?

There are multiple companies trying to break into the "smart home hub" market, but Amazon's Echo (and its sultry Alexa) are holding on to 70 percent of the market share, and it doesn't look like that's changing any time soon. That's a clear sign of victory for Amazon - and a wake-up call for its competitors.

The voice-activated home assistant market is growing, with almost a third of millennials likely to use a home assistant this year. While it might take a decade or more for the devices to find their way into the homes of older demographics (a situation Saturday Night Live has already mined for comedy), it seems that smart hubs will only increase in popularity from here on out, and that Alexa is poised to rule them all.

Chipotle Hit With Malware That Stole Credit Cards

Last month, the fast food chain Chipotle announced that they had been the victim of a large-scale data breach, but initially, the company was unable to provide any specific information regarding the scope and scale of that attack. Now, they have, and it's worse than anyone could have imagined.

The company reports that the hackers were able to affect customers in 47 states and Washington DC. They did so by orchestrating a well-coordinated attack which saw the insertion of malware onto the company's POS (Point of Sale) system, which enabled them to make off with vast amounts of data.

In terms of what was taken, the company reports that the stolen information includes everything from the magnetic strip of non-EMV cards, which includes:

- Credit card number
- Card expiration date
- Internal verification code
- Customer name and address information

In other words, it's about as damaging an attack as can be envisioned. Chipotle has announced that they have removed all traces of the malware and are working with law enforcement agencies and credit card agencies.

If you've eaten at the restaurant anytime in the last twelve months, and didn't pay with cash, it's a safe bet that your credit card information was stolen, and you should report the matter to the company that issued your card to get a replacement at once. While credit card data has fallen out of favor in recent months in preference for protected health information, it's clear that there's still a strong demand for the information. If you don't take action, you put yourself at risk of identity theft.

Unfortunately, hackers seem to be able to modify their attacks faster than digital security consultants can bolster their defenses, so this will definitely not be the last time we get word of such an incident. There's no such thing as a bullet proof security system, and no matter how robust yours is, a determined hacker can and will eventually breach it.

The best thing you can do, then, is be vigilant, and take immediate corrective action when something happens that impacts you.

Bits & Bytes

You've Been HACKED! What's the First Thing You Should Do?

There's always a chance that IT security will be breached, and one way to make a bad situation worse is not knowing the standard operating procedure when it happens. First, contact your IT personnel. The faster they can address the hack and figure out its extent, the better served you'll be. Next, understand that there are legal ramifications to being hacked; if valuable data has been compromised, you'll have to notify the individuals in question as well as the FBI. Remember, the faster you act, the better it will be.

Leave Your Life Jacket On The Shore And Swim Safely With This Inflatable Collar.

Despite their utility, orange life jackets are the opposite of cool. And when you factor in the human invincibility complex, you get a bad situation: people out on the water without adequate flotation devices. According to DigitalTrends, water safety company Ploota wants to change that with their inflatable necklace. Sleek and slim, the device is worn around the neck and doesn't get in the way of active water sports. But, if needed, it automatically inflates, potentially saving the life of the swimmer or boater.
DigitalTrends.com - May 8, 2017

Hopefully This Will Make Uberpool Way Safer And Less Stressful.

Speaking of safety, UberPOOL is getting safer and smarter by asking passengers to get out at better destinations — even if that means walking a few more feet to their destination — rather than in high-traffic zones. We're talking about distances of less than half a block, but it can cut major time off everyone else's commute and ensure passengers aren't stepping out into dangerous traffic. Of course, riders can always opt out, but getting dropped off at a high-traffic destination will take longer and cost more.
Mashable.com – May 4, 2017

Get a Refund If Your Child Made Accidental In-App Purchases From Amazon.

Some game apps allow you to buy stars, donuts, coins, or other tokens you can use to play the game. The tokens are imaginary, but the purchase is real. It's easy for kids to buy stuff within these apps without realizing they're spending money—your money. Last year, the FTC found Amazon liable for billing parents for these types of purchases, and the online retailer has now settled with the FTC, agreeing to refund these purchases. If your kid has purchased stuff without your permission via an app purchased on Kindle or the Amazon Android app store, you might be eligible for a refund. As Consumerist reports, you should get an email directly from Amazon, but you can also visit the Message Center in your Amazon account and find information under "Important Messages."
Lifehacker.com – June 1, 2017