HI TECH HUI NEWSLETTER

August 2020 | Volume 36

this issue

"It is not the strongest or the most intelligent who will survive but those who can best manage change."

– Charles Darwin

ANNE-MARIE'S MESSAGE

I was a victim of cyber fraud and it was so eye opening! I belong to a few Facebook (FB) group pages where people buy and sell items. I buy things online all the time through different platforms. When shopping on the open marketplace, there's always assumed risk, so I made sure not to spend too much money. In a recent purchase, I was SCAMMED, and the process of how this went down was so eye opening. After a week of not getting a tracking number for shipment from the seller, I started to get suspicious and the detective in me started going to work.

There were about 20 other people talking to the seller on the public forum, so I was able to capture information of those that could possibly be in the same boat. Shortly after I made my purchase, the seller Chelsy deleted her profile from FB. Apparently, this person has been in other FB groups defrauding people for years and getting away with it! How can someone get away with such illegal activity?

This is what I found out...

- - I paid her via Venmo which is owned by Paypal. Paypal offers Payment Protection, but Venmo does not guarantee your goods or services;
- - After discovering her real name, I found all her online profiles for each social media platform;
- - I found her license online with her birthdate and address. (Be sure to educate your kids never to post their info online);
- - Others who were scammed, also helped investigate and discovered that Chelsy has swindled a lot of people out of money;

At this point, I called the police to file a police report, to better understand how this process works. I had all the details necessary, her telephone number, her license info, her name etc.

The response, "We can't do anything". They wanted each of the defrauded parties to contact the police department where they lived. When pushed further, we pretty much did all the detective work for the police, they simply said: "We're too busy investigating murders and rapists, we don't have time for cyber crime because it's done over the internet across different states so it's under the jurisdiction of the FBI.

And that's why cybercrime is so prevalent, there's no punishment or process.

Tips for buying online:

If possible try to avoid purchasing from non monitored platforms like Facebook groups, but if you do, try to follow these things:

- - Only use Paypal when buying online;
- - Consider the buyer/seller ratings in the marketplace. Be observant of types of transactions and reviews they have;
- - Never use your home address when sending items;
- - Lock down your social media so others can't see anything without permission.

Per an FBI 2011 report, 300,000 people were victimized over the Internet to the tune of $1.1 billion. Although that averages out to only $3,666 per victim, the typical Internet hacker commits thousands to hundreds of thousands of these crimes and almost never gets caught. This is why cybercrime is prevalent. It's hard to get caught, and when caught, penalty is minimum (often just a few years of jail time). Protect yourself!

- Anne-Marie Lerch

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 – 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.

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.

OUR SOLUTIONS

Cyberuptive
FIREEYE
SOPHOS
Fidelis Cybersecurity
datto
backupify
JUNIPER NETWORKS
proofpoint.
BlackBerry
CYLANCE
DEMISTO
thycotic
cisco
Microsoft 365 Business
bitglass
Qualys.
paloalto NETWORKS
DUO
KnowBe4

CONNECTIONS

Connect with us on social media

Call us at
808.206.8549
or email us at
info@hitechhui.com

SHINY NEW GADGET OF THE MONTH

FitTrack – A Smart Scale That Does More

The bathroom scale isn't always the most useful device in the home. FitTrack is a smart scale that aims to change that. It's a different kind of bathroom scale that gives you much more than a single number.

Traditional bathroom scales don't tell you anything about what's happening in your body. FitTrack does. It gives you an "inside look" into what's going on inside your body. It measures your weight, body fat percentage, body mass index, muscle and bone mass, hydration and more. In fact, it tracks 17 key health insights.

The advanced scale pairs with the FitTrack app, which you can download to your smartphone and connect to the smart scale. All you do is step on the scale with your bare feet – the scale actually reads electrical signals from your body – and it sends the results to your phone. Simple and useful. Learn more about FitTrack at bit.ly/2VOg7Vs.

3 Critical Cyber Security Protections EVERY Business Must Have In Place NOW To Avoid Being Hacked

Five years ago, you might have had state-of-the-art security protecting your business and network. You had the latest malware protection, highly rated firewalls and a great data backup plan. Maybe you even had a handbook on how to address cyberthreats. You were set. But then you forgot to do one crucial thing: you didn't stay up-to-date with your IT security policy.

This is a trap countless businesses fall into. They invest in great cyber security once. Five years ago, this was fantastic. The problem is that cyberthreats are constantly evolving. Methods used by hackers and cybercriminals have come a long way in the past five years. Criminals stay on top of what's going on in the IT security industry. They are always looking for new ways to steal your data and make a quick buck at your expense.

What can you do to stay up-to-date in an ever-changing digital world? Here are three things every business must do to protect itself.

Understand The Threats

It's easy to assume that hackers are trying to get into your network the "old-fashioned" way. You might picture them hacking your network trying to get your passwords and usernames or breaking through your firewall protection. While some hackers will do this (it's easy for them if you use simple passwords), many of today's cybercriminals rely on social engineering.

The most common form of social engineering is the phishing scam. The criminal sends you or your employees an e-mail, hoping someone will click a link or open an attached file. Cybercriminals have gotten VERY sophisticated. These e-mails can mimic the look of a legitimate e-mail from a legitimate business, such as the local bank you work with or another company you buy from (or that buys from you). Social engineering is all about tricking people.

This is why you need a cyber security handbook – one that is regularly updated. It's something you can reference. Your team needs to know how to identify a phishing e-mail, and you need to have procedures in place for what to do if a questionable e-mail shows up. This helps keep your employees from becoming the weak link in your security setup.

Update, Update And Update

From software to hardware, you must stay updated. There is no such thing as "one-and-done" when it comes to network security. Something as simple as a wireless router can DESTROY your security if it's not regularly updated. Hackers are always looking for vulnerabilities in both hardware and software, and when they find them, they WILL exploit them.

What happens when a piece of hardware (like a router) is no longer supported by the manufacturer? This occurs all the time, particularly as hardware ages. Manufacturers and developers drop support for their older technology so they can focus on their newer products. When they drop support for a product you use, this is a good indicator that you need to replace that piece of hardware. The same applies to software.

You might balk at the cost of buying new technology, but in the long run, the cost is well worth it. Think of the cost of buying a new router versus the cost of cleaning up after a data breach. Some small businesses never recover after a hack – it's just too expensive. Keep your malware software updated, keep your firewall updated, keep your cloud backups updated and keep all your devices and software UPDATED!

Invest In Proactive Network Monitoring

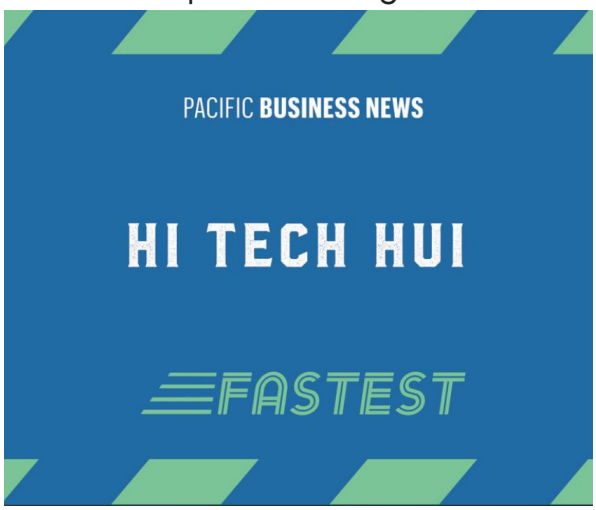
When it comes to the security of your network and overall business, being proactive can make a huge difference. Proactive monitoring means your network is being watched 24/7. Every little ping or access to your network is watched and assessed. If a threat is found, then it can be stopped.

The great thing about proactive network monitoring is that you can customize it. Want to know about every threat? You can request a real-time report. Only want updates once a day or once a week? That can be done too! This approach means you have one less thing to think about. Someone is always keeping an eye on your network, making sure the bad guys stay out.

You might think, "How am I going to do all this?" You don't have to go it alone – and you shouldn't. Work with an IT services firm. Work together to find the best solutions for your business. When you work with IT specialists, you can rest assured your team will be updated on today's threats. You'll know your network – and everything connected to it – is updated. And you'll know someone is watching over you. That's the ultimate peace of mind.

INSIDER SCOOP

HI Tech Hui is honored to be the only IT company in Hawaii to be nominated among Fastest 50 growing companies for 2019 & 2020! This year's virtual event took place on August 7th.



Woohoo! HI Tech Hui has made it to TOP 3 rated on threebestrated.com!

Three Best Rated® was created with a simple goal to find you the top 3 local businesses, professionals, restaurants, health care providers, etc., in your city. They display only businesses that are verified by their team since customers deserve only the best.

TECH TALK

3 TECHNOLOGY TRUTHS FOR TRANSFORMING YOUR BUSINESS

1. You have to keep up. Tech changes fast. By the end of this year, 5G will be more widely available – along with devices that can use it. More businesses will be relying on artificial intelligence to supplement productivity and customer interaction, putting them light-years ahead of the competition that lags behind.
2. You have to invest. Change comes with cost. If you aren't willing to invest in new tech, then you will fall behind, and so will your support and security. If you run into any problems, then you could be in big trouble.
3. Don't fall behind on cyber security. It's easy to forget about cyber security when things are running smoothly and working as intended. But cybercriminals never stop. They are always looking for a way in, and if you fallbehind the times on your IT security, then you make it easier for them. Keep your data and your customers as secure as possible. (Source: Inc., July 30, 2019)

HOW MALWARE CAN CRIPPLE YOUR BUSINESS

Every year, the number of malware attacks on small businesses increases. Semantec's 2018 Internet Security Threat Report found that between 2017 and 2018, malware increased by 54%.

The term "malware" covers a number of different malicious programs, including ransomware, spyware, viruses, worms, Trojan horses and more.

In many cases, malware is designed to take over your computer. It may be programmed to look for specific data or it may give a hacker remote access to your files. In the case of ransomware, it locks you out of your computer until you pay the hacker a ransom. After that, the hacker may give you back control – or they might delete everything on your hard drive. These are not good people.

If you don't invest in cyber security, then hackers can destroy your business. It's already happened to countless businesses across the country. It's estimated that websites experience up to 58 cyber-attacks every day. Protect yourself before it's too late. (Source: Small Business Trends, Oct. 12, 2019)