INSIDER SCOOP

Introducing Ramona & Kara

Our new “Master of Multitasking” Ramona is from Bethlehem Pennsylvania. She first moved to Hawaii in 2008 with the US Army, served 1 term, and 1 deployment to Iraq. Her background is in Real Estate Sales / Customer Service and recently worked for Keller Williams Honolulu as the Director of Agent Services. She spends all her personal time with Alex, her 10 year old son, going to the beach, hiking, and just relaxing at home.

Our newest team addition Kara graduated with a degree in Accountancy and is reviewing for the board exam this coming October 2021. She used to work as an Accounting and Payroll officer for two private companies and as Business/Technical Support for Intuit Quickbooks US. Kara likes to read books and watch anime or movies in her free time. Cake and food make up a big part of her heart and she often says she can be bribed with sweets to do anything - as long as it's legal!

Chuck & Anne's "Healthy Journey"

Anne-Marie & Chuck participated in a health and wellness seminar that included dropping the caffeine and routine juicing. One of them took it harder than the other.

CONNECTIONS

Connect with us on social media

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

HI TECH HUI NEWSLETTER

March 2021
Volume 41

this issue

OUR MESSAGE

“If you are not willing to risk the usual, you will have to settle for the ordinary.”

- Jim Rohn

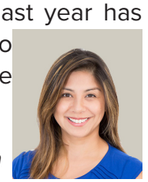
It was this time last year that we hosted our first Cybersecurity event for BSides in Honolulu. We had 14 amazing sponsors and we sold out with 200 attendees. It was such a great event, but it was the LAST event before COVID started to really make itself known in the US. We assumed we’d be back at it in a few months' time planning for the next BSides event, yet here we are – a full year later – everyone still at home and no known date for returning to live events.

Tony Robbins, an author, philanthropist, and one of my favorite teachers for personal and professional growth pivoted quickly into the virtual platform. His seminars would consistently sell out at a modest few thousand of attendees. It is rumored that he spent over a million dollars to create a virtual studio in which he had over 22,000 attendees from 143 countries for his first online seminar.

This month, Chuck and I jumped on that bandwagon and took part in Tony Robbin’s Life Mastery in the comfort of our home. In this seminar, one of the guest speakers was Kathy Buckley - the first hearing impaired comedian. Honestly, I just thought she was going to make us laugh a bit and give us a speech on how we can do anything we put our minds to, but she did so much more than that! In such a short time, she taught me about gratitude relating to things I may have overlooked in the past. Gratitude for the ability to hear, to speak, to move, to think - the basics.

She shared the story of Judy, a paraplegic who couldn’t move or speak and was confined to a wheel chair her whole life. The doctors treated her as if she was a vegetable until one day they heard a sound coming from her and realized that she was laughing at a joke. Judy later wrote a whole book with the help of a caregiver learning to read her cues she was sending by starting at specific words until it formed a sentence. This story gave me an awareness of how lucky we truly all are. So lucky, and we may not even be aware of it.

Thinking back to that BSides event, having 200 plus people in the same space. Trying to MAXIMIZE the number of people in a room and have gatherings. Going out without a mask. I took that for granted too. It's fair to say that this past year has changed my perspective. I do feel luckier than ever! We hope you also feel just as lucky!



- Anne-Marie Lerch

SHINY NEW GADGET OF THE MONTH

The Smallest Finder By Tile

First, there was the Tile – a small, square device used to find just about anything. You attach Tile to the thing you don't want to lose (keys, for example) and you pair Tile with the Tile app. Easy!

Now, Tile has introduced Sticker, their "smallest finder." It's a mini-version of their popular fob, and it can be stuck to just about anything, from TV remotes and portable electronics to tools, bikes, you name it – anything you don't want to go missing. Plus it also has a three-year battery life, so as they say, "you can set it and forget it." Learn more about Sticker at TheTileApp.com/en-us/store/tiles/sticker

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.

UPDATES AND OFFERS

In February, HI Tech Hui's service Cyberuptive was invited to attend FireEye's annual internal conference, Momentum. This invite-only event takes place over four days and is held to recognize employees, vendors, partners and accomplishments on all tiers.

This year there were over 800 partners from around the globe, representing over 175 organizations. Attendees had access to over 30 in depth presentations along with 40 "Birds of a Feather" sessions. If you're not familiar with the term, these sessions are short, mega-focused informal presentations formatted to fit gatherings of people with similar interests in a topic. With social feeds, live chat, and gamification to encourage participation, we found this event informal and FUN!

But more exciting than all the above, we feel incredibly lucky to be recognized at

this event as a Core MSSP Partner for Fireeye/Mandiant, and for our MSSP Innovation. We were asked to speak and participate in the conference. It does not go without appreciation of our great team that we were able to reach this experience within our first year of launching our SOC services. This achievement goes BEYOND luck.

OUR SOLUTIONS

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