

# HI TECH HUI NEWSLETTER

September 2020 | Volume 37



## this issue

Our Message P. 1

Why Your Business Is The PERFECT Target For Hackers ... P. 2

Vendor Feature: KnowBe4 P. 3

Insider Scoop P. 4

We Need Your Help! P. 4

## OUR MESSAGE

### CEO Fraud. The Billion Dollar Scam

Last month I shared a story about a social media scam. This month I want to share a story about a type of Business Email scam called CEO Fraud.

“CEO Fraud is a scam in which cybercriminals spoof company email accounts and impersonate executives to try and fool an employee in accounting or HR into executing unauthorized wire transfers, or sending out confidential tax information. According to FBI statistics, CEO fraud is now a \$26 billion scam.”

I was recently contacted by a friend & previous co-worker who returned to the islands to help his father with their local food distributor business. His father received an email from one of their vendors, only hours after his company had sent the vendor information regarding payment processed, requesting that check payment be stopped and ACH payments be made instead. The email contained details pertaining to the exact payment and directions on how to make a new payment. It's a vendor they had worked with many times and trusted, so no big deal.

It wasn't until AFTER the company, sent a \$130,000.00 payment via ACH did they realize, it was a scam! Immediately after they identified this, my friend called the company's bank, only to be told there was nothing the bank can do. Thankfully, my friend was VERY persistent and had a family member (Auntie) within the bank that was able to step in and assist. Auntie was able to figure out what bank received the large transfer, contacted them to STOP the bank from releasing the funds to the account holder, and reverse the transfer back to the victims. This is NOT a common outcome. Without a connection, you'll likely receive “out of luck” responses from your bank.

The findings; hackers had infiltrated the vendors emails and obtained enough information to:

- Identify a trusted vendor of company that sent or received large/frequent payments.
- Know the amount of the transfer and how payment was being made.
- Create a similar email address that was hard to spot the fake to send correspondence from. Example changing ie to ei in the email. Instead of accounting@lies.com the email was from accounting@leis.com

Hackers tried AGAIN to steal money from this company within the same week. This time sending an email from a spam address with a contact name familiar in the food distributors contact list. The recipient had to review sender details to spot the scam, where they again asked for a large sum of money.

All of this opened the victims up to being hacked themselves. Hackers made it into the food distributors web mail and started doing re-directs on incoming emails, creating more scams and more hacks.

Businesses beware! It's not just you or your employees under attack. In the same week I heard the above story, another friend revealed a vendor of their company was hacked and had emails sent on their behalf. So emails coming from true verified email addresses, asking for money or sensitive information, and changing account numbers so your money is routed to the hackers direct account.

We share this with you to encourage you to consider using a program like KnowBe4 to train yourself and your employees to spot fraudulent emails and respond appropriately. Contact us for more information!

- Anne-Marie Lerch



*"Nothing in life is to be feared, it is only to be understood. Now is the time to understand more, so that we may fear less."*

- Marie Curie

## SHINY NEW GADGET OF THE MONTH



### Weber Connect Smart Grilling Hub

Grilling can feel like guesswork. You throw the food on the grill and keep a close eye on it, hoping for the best. Say goodbye to guesswork and overcooked steaks with the Weber Connect Smart Grilling Hub.

The Weber Connect takes the thermometer and timer into the WiFi era. It monitors your food and sends updates to your smartphone. It lets you know when to flip the burgers or steaks – and then notifies you again when it's time to take them off the grill. You can even have the Weber Connect tell you when your meat of choice has reached your ideal level of doneness. It's great for those who are new to grilling or don't grill often, and it works with every grill! See more at [bit.ly/3eTL69Y!](https://bit.ly/3eTL69Y)



## Why Your Business Is The PERFECT Target For Hackers... And What You Need To Do NOW To Protect Yourself

**Everybody gets hacked, but not everything makes the evening news.** We hear about big companies like Target, Home Depot, Capital One, and Facebook getting hacked. What we rarely hear about are the little guys – the small businesses that make up 99.7% of employers in the United States, according to the Small Business Administration. It's these guys who are the biggest targets of cybercriminals.

Basically, if you run a business, that business is a potential target. It doesn't matter what industry you're in, what you sell or how popular you are. Cybercriminals go after everybody. In 2018, a cyber security survey by the Ponemon Institute found that 67% of small and midsize businesses in the US and UK were hit by a cyber-attack.

For the cybercriminal, casting a wide net makes the most sense because it gets results. It puts them in a position where they are able to extort money, steal sensitive information and ultimately profit off of destroying the property, prosperity and reputation of others.

Why do cybercriminals love to target small businesses? There are a handful of reasons why small businesses make sense to attack.

### 1. Small Businesses Are The Most Vulnerable.

Business owners, entrepreneurs and executives aren't always up-to-date on network security, current cyberthreats or best practices in IT. They have a business to run and that's usually where their focus is. Unfortunately, that means cyber security can take a back seat to other things, like marketing or customer support. This also means they might not be investing in good network security or any IT security at all. It's just not top-of-mind or they may feel that because it's never happened to them, it never will (which is a dangerous way of thinking).

### 2. Small Businesses Don't Take IT Security Seriously.

Coming off that last point, it's true that many businesses don't properly secure their network because they feel that they aren't vulnerable. They have the mindset of "It hasn't happened to me, so it won't." Along

those same lines, they might not even take password security seriously. According to research conducted by Trace Security, upward of 80% of ALL breaches come down to one vulnerability: weak passwords! Even in 2020, people are still using passwords like "12345" and "password" to protect sensitive data, such as banking information and customer records. Secure passwords that are changed regularly can protect your business!

### 3. Small Businesses Don't Have The Resources They Need.

Generally speaking, medium to large companies have more resources to put into IT security. While this isn't always true (even big companies skimp on cyber security, as the headlines remind us), hackers spend less time focused on big targets because they assume it will take more of their own resources (time and effort) to get what they want (money and sensitive data). Many small businesses lack the resources like capital and personnel to put toward IT security, so hackers are more confident in attacking these businesses.

Just because you haven't had any major problems for years – or at all – is a bad excuse for not maintaining your computer systems. Threats are growing in number by the day. While many small businesses might think, "I don't have the time or resources for good security," that's not true! You don't need to hire IT staff to take care of your security needs. You don't need to spend an arm and a leg securing your network. IT security has come a LONG way in just the last five years alone. You can now rely on IT security firms to handle all the heavy lifting. They can monitor your network 24/7. They can provide you with IT support 24/7.

That's the great thing about technology today – while many hackers are doing everything they can to use technology against us, you can use it against them too. Work with a dedicated and experienced IT security firm.





Tell them your business's network security needs and they'll go to work fighting the good fight against the bad guys.

# Security Awareness Training and Simulated Phishing Platform

Helps you manage the ongoing problem of **social engineering**

## KnowBe4 Security Awareness Training

Old-school security awareness training doesn't hack it anymore. Today, your employees are frequently exposed to sophisticated phishing and ransomware attacks.

-  **Baseline Testing**  
We provide baseline testing to assess the Phish-Prone™ percentage of your users through a free simulated phishing attack.
-  **Train Your Users**  
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.
-  **Phish Your Users**  
Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.
-  **See the Results**  
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!



KnowBe4 is the world's largest integrated Security Awareness Training and Simulated Phishing platform with over 30,000+ customers. With world-class, user-friendly new-school Security Awareness Training, KnowBe4 gives you self-service enrollment, and both pre-and post-training phishing security tests that show you the percentage of end-users that are Phish-prone. KnowBe4's highly effective, frequent, random Phishing Security Tests provide several remedial options in case an employee falls for a simulated phishing attack.

Gauge the security awareness proficiency of your users and measure your organization's overall security culture posture with KnowBe4 Assessments. These two science-based assessments help you tailor training to address proficiency gaps and weaknesses, as well as monitor the impact your security awareness training program has on improving your users' knowledge and sentiment to security awareness over time. Contact us to implement these services today! Visit [www.hitechhui.com/securityawareness](http://www.hitechhui.com/securityawareness) for more information on KnowBe4.

### OUR SOLUTIONS

**Cyberuptime**

**FIREEYE™**

**SOPHOS**

**Fidelis™**  
Cybersecurity

**BlackBerry.**

**CYLANCE.**

**JUNIPER.**  
NETWORKS

**proofpoint.**

**datto**  
backupify

**DEMISTO**

**thycotic**

**CISCO**

**Microsoft 365**  
Business

**bitglass**

**Qualys.**

**paloalto**  
NETWORKS

**DUO**

**KnowBe4**

Call us at  
**808.206.8549**  
or email us at  
[info@hitechhui.com](mailto:info@hitechhui.com)

## INSIDER SCOOP

This month we had the honor of Auntie Angel blessing our newest office. Auntie is a genuine healer, is extremely practiced and sought out in traditional Hawaiian blessings, and is considered part of our o'hana. We're grateful she was able to visit our office and guide us in praying and asking for Queen Lili'uokalani's permission to receive blessings towards helping Hawaii businesses and allowing our business to flourish. Having Queen Lili'uokalani's mural on the side of our office building, being able to look her in the eyes and connect with our request, made the moment incredibly special to us.



## OUR OHANA IS GROWING!



**CANDACE TAGAWA**  
Creator of Opportunities

Candace is a sales professional with extensive experience in the telecommunications industry. She has worked as a sales executive handling large enterprise clients as well as national and international carriers. When not working, Candace enjoys spending time with her family, watching UH football and traveling.

**LIAM WESLEY**  
SOC Analyst

Liam Wesley is an Offensive Security Wireless Professional (OSWP) and an Offensive Security Certified Professional (OSCP) and a Linux veteran of over 20 years. He enjoys playing piano and spending time with his wife and daughter when not studying technical manuals. Having been raised in Japan for a large portion of his youth and later living in Japan as an adult, he can also speak Japanese fluently.



## WE NEED YOUR HELP!

Help us Keep Candace Busy. She Needs Your Referrals.



All you need to do is send us an email to [info@hitechhui.com](mailto:info@hitechhui.com).

**Subject:** Referral for Candace

Let us know the name of the fellow business owner who might benefit from our services.

The more qualified referrals you send our way, the more entries you get!

**Samsung - 49" - QLED - 4K UHD TV**  
**Smart TV - LED - with HDR**

Contest ends October 31, 2020.

Referrals must be qualified to enter giveaway.  
If referral turns to customer, 5 BONUS entries!

