NEWS RELEASE

Air Gap Attacks – What You Need to Know

Free September 14 "Hacking the Human" webinar to provide tips for avoiding deceptive hacking tactic

PHOENIX, Ariz. (August 29, 2017) – It may sound like science fiction, but air gap attacks are real. Criminals have invented ways to affect your computer without ever actually touching it - even if it isn't connected to the internet or another network.

"This type of attack is called an 'air gap' attack because the attack is designed to jump the 'air gap' between the source and the target machine that isn't connected to anything," said Michael Cocanower, president and CEO of Phoenix-based itSynergy.

Cocanower, who has been recognized nationally and locally for his IT expertise, will conduct a free, 15-minute "Air Gap Attacks" webinar on Thursday, September 14 at 11:30 a.m. Interested participants should register at http://www.itsynergy.com/webinar.

The most famous example of an air gap attack was the Stuxnet virus, which many refer to as the world's first digital weapon. It was first discovered in 2010, but it had been silently sabotaging centrifuges at Iran's Natanz nuclear plant for close to a year. Because the computers that controlled the centrifuges were not connected to the internet, the attackers designed their weapon to spread via infected USB flash drives.

"The obvious question is how did the attackers get the virus on to their target air-gapped computer system?" Cocanower said. "Once again, people were the weakest link. The hackers targeted five outside companies that were believed to be connected to the nuclear program and infected their systems. Their employees became unwitting carriers who helped to transport and spread the virus via flash drives that they delivered to the protected facility."

Once the target computer system is infected, the hackers can use several types of receivers to control or remove data.

"I've seen examples at research labs where a drone flew outside near a window and was able to receive data from the infected computer. Some receivers can use sound, lasers and other radio frequencies from nearly a mile away to receive the data," Cocanower said.

The "Hacking the Human" webinars take place at 11:30 a.m. on the second Thursday of each month. The webinars are geared towards non-technical end users in business at any level in the company. Each webinar provides useful tips to ward off cyberattacks and more complex social engineering schemes that result in theft and corporate espionage.

The schedule of webinars after September include:

October 12 – Two Factor Authentication

One of the best ways to defeat any attack involving compromise of a password is to utilize two factor authentication. This month we'll teach you what two factor authentication is and why it helps to defeat attacks. We'll then discuss many locations where it is available, and how to turn it on and use it. You'll leave armed with the knowledge of how to make settings changes that will protect some of your most frequently visited and most valuable online assets such as email, file sharing sites, banking sites, and more.

- Learn what two factor authentication is
- See various common methods that can be used for two factor authentication
- Learn the types of attacks that can be thwarted using two factor authentication
- See a list of many common websites and services that have two factor authentication available, and learn how to enable it

November 9 – Your Phone - Hacker's Friend?

When you think about hacking, do you think mostly about your computer? What you may not realize is that more and more, thieves are targeting your phone just as much as any other device. Because your defenses may be a bit lower when it comes to your phone, these attacks can be very successful. Join us to learn about what you need to be aware of when it comes to potential attacks on your phone, and how you can protect yourself.

- What types of attacks are launched by criminals against your phone?
- What physical measures do you need to take to protect your phone from being hacked?
- What can the bad guys get by targeting your phone?
- Learn the steps you need to take to recognize an attack and protect yourself

December 14 – ATM Security

Out shopping for the holidays? Decided to stop at an ATM for a bit of extra cash? How can you protect yourself from getting hacked at the ATM? Join us to learn how to leave the ATM with just cash, and not as the victim of a newly stolen identity or theft victim whose accounts will shortly be trained of cash.

- What techniques do criminals use at an ATM to 'get you'?
- What happens once your information has been stolen from a compromised ATM?
- Learn what to look for when approaching/using an ATM to help ensure it hasn't been compromised
- Understand how to select an ATM with the lowest probability of criminal exploit

For more information, call itSynergy at (602) 297-2400 or visit www.itsynergy.com.

###

About Michael Cocanower, President and CEO of itSynergy

He has his black belt in the Kung Sul division of Hwa Rang Do, a Korean martial art, so it's fitting that Michael Cocanower's passion is helping small and medium-sized businesses defend themselves against malicious cyber intruders. A Phoenix native, Cocanower founded itSynergy in 1997, and under his leadership, the company has experienced exponential revenue growth. A long-standing

Microsoft Partner, itSynergy provides strategic technology management services for small and mid-sized organizations on a fixed monthly fee. Cocanower has received numerous awards and widespread industry recognition throughout his career, including being named one of 20/20 Visionaries in *Channel Pro Network* magazine's May 2016 issue. The magazine regularly turns to him for input on current IT trends, and called him a "shrewd and articulate observer of the SMB market." In addition, the Arizona chapter of Entrepreneurs' Organization (EO) recently appointed Cocanower to the board of directors as membership chair.

Media Contact:
Sue Kern-Fleischer, PublicizeThis!, (602) 810-1404, sue@publicizethis.com