NEWS RELEASE

How Much is Spam Costing Your Business?

Free July 13 “Hacking the Human” webinar to provide tips for combating spam

PHOENIX, Ariz. (June 27, 2017) – Email spam is not only annoying, it’s costly. In fact, some researchers believe the total cost of spam for businesses is on track to exceed $257 billion per year. Another report reveals that for every dollar spammers create, they destroy $100 in the overall economy.

“Beyond inconvenience, spam hammers your email accounts in hopes of taking information from you,” said Michael Cocanower, founder and president of Phoenix-based itSynergy. “For businesses, not only does it translate to decreased productivity, but it can hurt the bottom line by increasing infrastructure costs, bogging down your Internet connection, and creating an increased demand for storage.”

Spam has exploded over the past four decades. Internet folklore dates the first spam e-mail to 400 recipients in 1978. Spam filters were introduced in the 1990s, but that hasn’t stopped the spammers. Today, an estimated 269 billion emails are sent daily, with spam messages accounting for 56.87 percent of email traffic worldwide.

Cocanower, who has been recognized nationally and locally for his IT expertise, will conduct a free, 15-minute “Combating Spam” webinar on Thursday, July 13 at 11:30 a.m. The webinar, part of a monthly “Hacking the Human” series, will provide participants with tips for controlling shareable data through smart tools that keep sensitive information secure. Interested participants should register at http://www.itsynergy.com/webinar.

“We’ll be discussing different kinds of spam that exist and prevention methods. In addition, we’ll show you spoofing examples and explain how technical pros determine whether a message is real or not. We’ll also address false positives – when legitimate email gets stuck in your spam folder,” 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 July include:

August 10 – Protecting Your Privacy Online

It seems every day there is a new news story about online privacy. Information about you, your family, and your online activities is very valuable, and a large number of companies are vying to get that data from you and turn it into profit, starting with your Internet provider. If these existing efforts weren't bad enough, Congress recently passed and the President signed into law a repeal of Obama-era regulations that would prevent ISPs from selling your data. Join us to learn about how to be aware of what you are exposing online, and then use that information to make intelligent decisions about what to share and what to keep private.

- Learn how to take inventory of exactly what you are giving away online
- Review common sites (Facebook, LinkedIn, etc.) to understand where to find privacy settings and how to set them to your liking
- See how to use some simple techniques to hide your identity in certain situations
- Leave knowing that you are in control of information and whatever is being shared is done only because you have made a conscious decision to do so

September 14 – Air Gap Attacks

Did you know 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. Join us to learn about the types of air gap attacks and what you need to be on the lookout for to avoid them.

- Learn the various types of air gap attacks that have been used
- Get tips on what to be aware of in your surroundings to avoid being the victim
- Steps you can take to help protect yourself from an air gap attack
- The types of things attackers can do once you have been compromised via an 'air gap' attack

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, Founder and President 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