Issue # 10 Volume #15 October 2014

AaSys® Solutions are our Business

Solutions

Tips for keeping your personal information safe, your family protected, and our national security intact.

Stop hackers from accessing your accounts — set secure passwords.

Stop sharing too much information — keep your personal information personal.

Stop — trust your gut. If something doesn't feel right, stop what you are doing.

Think about the information you want to share before you share it.

Think how your online actions can affect your offline life.

Think before you act — don't automatically click on links.

Connect over secure networks.

Connect with people you know.

Connect with care and be on the lookout for potential threats.

Securing one citizen, one family, one Nation against cyber threats.

www.dhs.gov/stopthinkconnect

National Cyber Security Month
Stop. Think. Connect.

October is the 11th Annual National Cyber Security Month! President Obama realized early on in his tenure that as a nation, we needed to increase dialog and education about protecting ourselves online. This resulted in Homeland Security creating an ongoing campaign called ***Stop. Think. Connect***. The campaign is geared towards empowering individuals, consumers and companies to take cyber security seriously and to be vigilant in protecting ourselves and each other.

Month after month, the AaSys Newsletter has provided our customers with the most updated information on new bugs, upcoming technologies and demonstrated best practices. We are committed and will continue to do everything we can to ensure our customers are well educated on cyber security and any emerging threats.

As we go into the fourth week of October, the Campaign will focus on what new and established businesses can do to protect their organization, customers, and employees. As seen in recent months, there is potential for significant financial loss and loss of consumer confidence when a cyber attack has been able to penetrate some of the largest and most trusted organizations. But there are some simple steps that we can all do on a regular basis to protect ourselves: set strong passwords, keep our operating system, software and browser updated, and most importantly, limit the amount of personal information we share online.

The reality is the internet is intertwined with every aspect of our lives. It has allowed us to be more efficient and productive than ever before, but like all things, it comes with risks. If we stay vigilant while we share information with friends, family and colleagues, we can make the Internet safer for all. For more information about the Stop. Think. Connect Campaign visit http://www.dhs.gov/stopthinkconnect.

STOP | THINK | CONNECT™

Are there subjects that you would like to have covered in future newsletters? We are always looking for topics of interest and we welcome all suggestions! To submit a topic, subscribe, or unsubscribe to our distribution list, please send an email to newsletter@aasysgroup.com

11301 N. US Highway 301, Suite 106
Thonotosassa, FL 33592
(800) 799-8699
www.aasysgroup.com

NOTICE!
The AaSys Help Desk will be closing at 5:00PM EST on November 28, 2014.

Happy Halloween!

Inside this issue:

This Poodle Bites

I know it's not the most sophisticated, "techy" name, and it actually sounds kind of comical. Unfortunately, the "Poodle" vulnerability is no laughing matter.

Here is the breakdown: SSL (Secure Sockets Layer) provides a secure connection while online, allowing data to be encrypted while being transmitted from a user to a website. What "Poodle" (aka ***Padding Oracle On Downgraded Legacy Encryption***) has been found to do is infiltrate the older version of SSL (called SSL 3.0 or SSLv3) allowing a hacker to highjack your browsing session, potentially gaining access to things like your email, online banking or any other online accounts. The silver lining is many have stopped using the SSL 3.0 version years ago and upgraded to TLS (Transport Layered Security), which is more robust. However, there are some that still use the older version making them very vulnerable to an attack. Experts don't believe Poodle is as harmful as Heartbleed or Shellshock because security researchers believe that the potential victim has to be actively online and physically close to the attacker (e.g., using the same Wi-Fi network). Despite this, they are still urging all users to take the necessary steps to protect their data.

So what do you do? As always ensure that all your software applications, browsers and operating systems are updated. If you are still using Microsoft Windows Explorer 6, you should upgrade as soon as possible. Most web browsers will remove support for SSL 3.0 in the near future. AaSys is in the process of disabling SSL 3.0 client support to all of our ROC (Remote Operations Center) customers and will continue to keep our customers abreast of any new developments.

The True Cost of Cyber Crime on Community Banks

Whether it's Poodle, Heartbleed or Bash, vulnerabilities all have the potential to cause major damage to community banks. Community banks have been the financial foundation for many communities, and when they are victimized by a cyber attack, the cost can be enormous. Financial institutions rank 5th among the top 10 industries for targeted attacks. We commonly relate losses to what has been stolen, but seem to forget the internal cost that also affects the banks. Long ago when someone physically robbed a bank, law enforcement was able to narrow down the potential suspects to maybe a handful of individuals. Now when dealing with a digital thief, they can basically be look at anyone on the planet with access to a computer as a potential suspect. Here is where a bank's expenses start to add up. Between investigations, potential civil and legal claims, regulatory fines and public relations costs, a bank can spend millions just trying to catch a cyber criminal. Then there is reputational damage. Most companies spend years building a trusted brand, especially banks. But with just one key stroke by a cyber criminal they can change how customers and potential customers feel about an organization, possibly causing more monetary damages. But most importantly, the perception of the organization in the community which can have lasting effects. All this to say the true cost of cyber threats can be enormous. In 2013, McAfee sponsored a study to show the economic impact of cyber crimes on the global economy. It showed that the annual global loss is about $300 billion to $1 trillion. And an estimated 500 thousand jobs are lost each year. As we close out National Cyber Security Month, it is imperative that financial institutions stay informed about the continuously changing forms of cyber threats and develop appropriate, cost-effective controls to safeguard their businesses customers and employees.