Issue # 8 Volume #15 August 2014

AaSys® Solutions are our Business

Solutions

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

MASQUERADING

What it is and how not to fall victim to it!

Banks have been called to task to provide better security for their customers...but banks have also been victims.

David Pollino, a fraud prevention officer at Bank of the West, has been doing intense research on a type of cyberfraud that he has called "masquerading." Masquerading is a combination of social engineering and a confidence scam. Basically, cyber criminals do not want to reinvent the wheel; they just want to change the players.

Masquerading involves a cybercriminal pretending to be an executive of a particular bank to try to perpetrate wire fraud. The fake CFO, CEO or executive gives instructions to the bank employees through what looks like a legitimate email (or even through a phone call) and requests a confidential wire transfer to another institution.

Although most banks have checks and balances in place to prevent fraud, if your employee believes the email or phone call request is valid, he or she will allow the transaction to go through.

Fourteen percent of businesses experienced wire fraud last year, up from 11% the prior year, according to the Association for Financial Professionals' 2014 AFP Payments Fraud and Control Survey.

But David Pollino has a few ways that banks and companies can protect themselves.

1. ***Confirm the wire transfer request is a valid request from an authorized individual within your organization.***

2. ***Double check the email address the request is coming from.*** Sometimes the criminal will alter the email address slightly to not draw any attention that it could be fraud. By replacing the "w" in the company's name with a double "v," for example, a masquerader could send emails from Bankofthevvest.com.

3. ***Establish an approval process that requires multiple signatures over a certain dollar amount.*** An email request should never be enough to get a large dollar amount wire transfer initiated.

4. ***Take your time.*** Many jump into action when executives make a request. But moving too fast and not following proper procedures can lead to mistakes that can be costly. If you have questions about the request, contact your manager or the person making the request directly or in person.

Source: Pollino,David "6 tips to Protect Against new cyber threat" Bank of the West July 26, 2014 http://blog.bankofthewest.com/6-tips-protect-new-cyber-threat-masquerading/

AaSys Group, Inc. will be closed Monday, September 1, 2014 in honor of the Labor Day holiday.

Inside this issue:

Backoff Malware

Backoff Malware is a new point of sale malware affecting many big retailers and smaller shops. The government has been tracking this malware as far back as 2013, but recently the malware has been more aggressive. The malware consists of four capabilities:

1.Scraping memory for tracking data,
2. Logging keystrokes,
3. Command & Control (C2) communication, and
4. Injecting malicious stub into explorer.exe.

This malware normally attacks several merchants at the same time through the exploit of a remote-access or third-party vulnerability. It has been reported that that more than 1,000 retailers have been affected so far. Federal authorities say their investigations have determined that hackers used available tools to locate businesses that use remote desktop applications such as LogMeIn Join.me, Microsoft's Remote Desktop, Apple Remote Desktop, Chrome Remote Desktop, Splashtop 2 and Pulseway to carry out their attacks.

Experts say banks need to manage their networks properly. While there is great benefit to having remote employees, you want to be sure to have a VPN that those employees log in to. Also important is using two-factor authentication and then from there, accessing the remote desktop.

Another way banks can be under fire is through an online banking user with a Windows 7, 8 or XP computer. These machines come with the Remote Desktop tool and the computer can be infiltrated that way. Back Off has the potential to record the keys strokes of the online user when they log into a bank site. While on that site, the hacker can send customized notifications instructing the user to divulge additional personal information.

Experts and the Department of Homeland Security recommend several steps to help organizations avoid being attacked, a few of which are listed below along with AaSys' response to the threat. For the full list please visit https://www.us-cert.gov/ncas/alerts/TA14-212A.

- Configure the account lockout settings to lock a user account after a period of time or a specified number of failed login attempts. This prevents unlimited, unauthorized attempts to login whether from an unauthorized user or via automated attack types like brute force.

AaSys Response: All AaSys customers are configured with proper account lockout settings.

- Define complex password parameters. Configuring an expiration time, password length, and complexity can decrease the amount of time in which a successful attack can occur.

- Require two-factor authentication (2FA) for remote desktop access.

AaSys Response: Because AaSys requires VPN access to remote desktops, all of our customers inherently use multifactor authentication. However, many of our customers are now using another level of authentication in the form of RSA/Vasco tokens or one time passwords on their VPN. If you would like more information on this, please ask your Account Representative for details.

- Use firewalls (both software and hardware where available) to restrict access to remote desktop listening ports.

AaSys Response: All AaSys customers' remote desktops sit behind a firewall and require VPN access.

Again, we may not always be able to prevent every single threat, but educating ourselves and our customers definitely helps improve our chances of us not falling victim to these schemes.

DID YOU KNOW???

Here are some fun facts that may help you out in your next Trivia or Jeopardy game!

⇒ **In 1984, MasterCard® was the first to use a hologram on its cards to deter fraud.**

⇒ **Martha Washington is the only woman whose portrait has appeared on U.S. paper currency.**

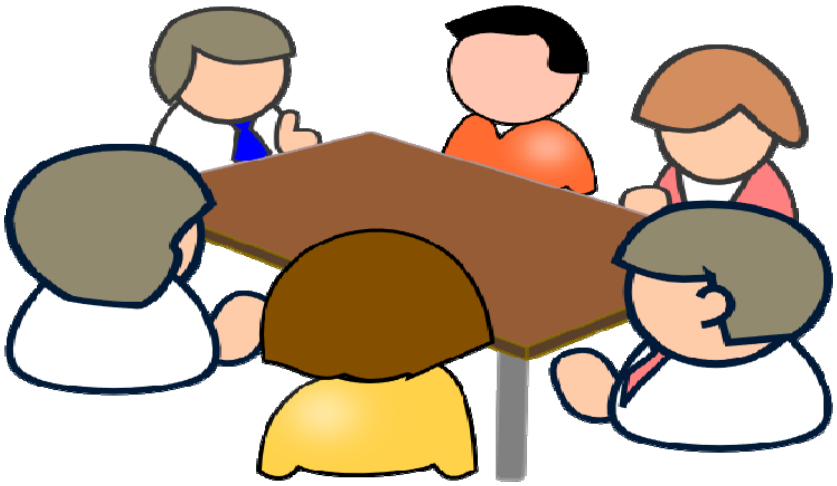
⇒ **Credit cards were first used in the United States in the 1920s.**

⇒ **The word "buck" came to mean a dollar because originally, a buck referred to a deerskin or buck-skin, which was commonly used as money.**

⇒ **Susan B. Anthony and Sacagawea are the two women who have appeared on the U.S. $1 coin**.

AaSys Upcoming ISO Meetings!

Great News! AaSys is pleased to announce that our first ISO Meeting in Sutton, WV on August 14, 2014 was a great success! We would like to thank everyone who was able to attend. We are thrilled to be able to work together to share resources & compare best-practices to improve the overall security structure of the financial sector. Below is a schedule of our upcoming ISO Meetings. We hope to see you there!



CULLMAN, AL

Topic: Cybersecurity Framework & Options for Implementation
Co-Hosted by Eva Bank

Date: Tuesday, September 9, 2014

Time: 10:30 am – 2:30 pm, lunch included

Location: Cullman Chamber of Commerce
301 2nd Ave SW
Cullman, AL 35055