



*Information Systems
Audit and Control
Association®*

Hudson Valley Chapter

December 2005 – January 2006 Newsletter

In this issue:

- [President's Message](#)
 - [Member Articles](#)
 - [CISA and CISM News](#)
 - [Membership](#)
 - [Certification Seminar](#)
 - [Technology Conference Update](#)
 - [ISACA International News](#)
-

President's Message

Wow! That was quick! Here it is the holiday season already. Time for the hustle and bustle (I love that word!) of holiday shopping, planning for travel to visit friends and family, preparing special meals and parties, and for recalling all of the events that have taken place over the year(s). Barely leaves enough time for work!

But to some, the holiday season is a time to really increase their work, as it presents a great opportunity to reach an extended customer base. Yes, I'm referring to spammers and phishers; those unscrupulous individuals that use the Internet and email to gather valuable information and acquire territory. Traditionally, there has been seasonal increases in spam and phishing attempts, thought to be due to an increase in computer usage due to on-line holiday shopping and email correspondence with distant family members. And recent news articles have identified a significant increase in email-transmitted viruses, citing a version that appears to come from the FBI or CIA, with a subject that implies that Internet usage is being monitored by these federal organizations in an attempt to trick the recipient into activating links within the email and installing the virus. With that in mind, Wes Moore's article in this newsletter should be especially helpful.

Luckily (at least for me) December's Holiday luncheon was very helpful in dealing with the stressful situations (like increased spam) that always arise with the season. Dr. John Pelizza provided some excellent advice and examples for coping with stress in our lives, both the seasonal and day to day stressors. Now, all we need to do is follow through on this timely advice.....

And, with the passing of the holiday season, it's time to start thinking of registering for the June CISA or CISM exams. This year, the exam will be on June 10, with the deadline for registration on April 5. The early registration deadline is February 8, and additional savings can be obtained by registering for the exam online. We are still evaluating whether there is sufficient interest in holding an exam preparation course, so if you are considering taking the exam and are interested in attending such a course, please contact Mark Ren.

Best of holiday wishes to each of you. And hope you all remain safe and secure.

Mike Farrar

Chapter President



Analysis of a Computer Crime: Phishing for Your Data

By Wes A. More

Introduction

Sending email spoofed to look like it came from a legitimate source combined with fraudulent websites modeled after the actual site they mimic is the foundation of a phishing attack. The catch these “anglers” are looking for includes an unsuspecting user’s financial data such as credit card numbers, account user names and passwords, social security numbers and other personal sensitive information.

The Anti-Phishing Work Group (APWG) counted over 3600 phishing attacks from April to June of 2004. For a breakdown of attacks by week and cumulative for this period, please see their site (1). Phishing attacks are growing steadily and may be the number one attack against consumers utilizing computers today.

Phishing for AOL user’s data

This paper will analyze a phishing attack using common language as described by Howard and Meunier (2). The spoofed organization in this instance was AOL. The scam was a statement that a billing to the target was not validated by the credit card company. The phish(3) (goal) was the user’s e-bay username/password, credit/debit card information, social security number, ATM pin number and other sensitive information.

The event begins by the perpetrator designing a web page(s) that looks like the authentic web page of the organization spoofed. In this case (4), AOL was the organization spoofed. The page was designed to look like the user was at the AOL Billing Center. As you will see, the spoofed organization is not the real target.

The next step in the attack is to design an email to send to a list of the spoofed organization's clients. This email, combined with the spoofed website, is the tool used in the phishing attack. The email informs the "client" that the spoofed organization attempted to bill their credit card and the credit card was not validated. There is no attempt to identify the credit card company or the card itself. The client is also informed to update the account information within 24 hours or they will be forced to terminate the user's account with them.

To facilitate the information exchange, a link identified as the spoofed organization's service center is included in the email. When clicking the link to the phish site, a pop-up window shows up. The pop-up window welcomes the client to the spoofed organization's site, reiterates the issue with the account and prepares the client by requesting the billing, credit and relevant information.

Clicking through the pop-up window takes us to the actual phish site. This is where we begin to see the actual target. The spoofed site contains the logo of the spoofed organization, logos of the popular credit and debit cards and hints on where certain information can easily be found by the client. Information must be from the cardholder or someone authorized to use the card.

The information requested on the spoofed page includes the client's name and address. Additionally, the client's phone number, mother's maiden name, social security number and date of birth are requested. Also, credit or debit card information including card number, expiration, and name on card, control number and user's pin number are asked for.

To make the phishing site look more authentic the page includes a text box for comments and suggestions. The obligatory submit button is also present. To complete the authentic look there is a statement at the bottom of the page indicating that the data submitted is being sent encrypted using AOL SSL security.

As we can now see, the target here is the user's sensitive data. By tricking the user into providing this sensitive information the attacker gains the unauthorized result of disclosure of information. With this data the attacker could use the credit or debit card information fraudulently. Additionally, the attacker has gained enough data to perpetrate an identity theft.

The final step in this incident is the attacker's objective. Phishing attacks are generally perpetrated by professional criminals. Typically the objective of professional criminals is financial gain. A successful phishing attack such as we have discussed will result in gaining the necessary data to achieve the objective of financial gain.

Protection Measures

There are steps we can take to protect ourselves from phishing attempts. First, your bank or other organizations that have sensitive personal information should never ask for updates via email. Tips to help protect you from phishing attempts are:

Never click on a link in an email asking you to update sensitive information

If you need to update account information with your bank, online auction site, online gambling site, etc. Always type the organization web address into your browser or contact them via phone or regular mail.

Make sure you are using one of the latest Operating System (OS) versions

Ensure that your systems are kept up to date with fixes provided by your OS vendor

If you desire there are vendors providing software designed to protect you from phishing attacks.

Remember that these attacks are designed to take you to a web site that looks exactly like the web site you are anticipating going to. Even the lock symbol in your browser will show. This is an indication that the traffic to the site is encrypted but not an indication that the site is legitimate.

- (1) [http:// www.anti-phishing.org](http://www.anti-phishing.org)
- (2) Howard, John D. and Meunier, Pascal: Using a "Common Language" for Computer Security Incident Information; Computer Security Handbook, Chapter 3; John Wiley & Sons Inc.
- (3) Dragon, Alice: Fighting Phish, Fakes, and frauds; CIO Magazine – September 1, 2004 – pg. 38
- (4) [http://www.anti-phishing.org/phishing_archive/08-06-04:AOL_\(Urgent_Message_from AOLmember_services\).html](http://www.anti-phishing.org/phishing_archive/08-06-04:AOL_(Urgent_Message_from_AOLmember_services).html)
- (5) National Research Council (NRC), Computers at Risk: Safe Computing in the Information Age (Washington DC: National Academy Press, 1991), p.301; and Amoroso, Fundamentals of Security Technology, p. 2

CISA and CISM[®]

You can now register for the June 2006 CISA and CISM exams at www.isaca.org. Bulletins of Information for each exam are available on ISACA's website. The early registration period ends February 8th. You can save \$50 by registering early, and save another \$35 by registering online. The following CISA and CISM study aids from ISACA are now available for the upcoming June exams, or will be available soon (as denoted in parenthesis):

- *CISA Review Manual 2006* (Available now)
- *CISA Review Questions, Answers & Explanations Manual 2006* (Available now)
- *CISA Review Questions, Answers & Explanations Manual 2006 Supplement* (Available now)
- *CISA Review Questions, Answers & Explanations CD-ROM 2006* (English edition, available December 2005)
- *CISM Review Manual 2006* (English, available December 2005)
- *CISM Review Questions, Answers & Explanations Manual 2006* (English edition, available December 2005)
- *CISM Review Questions, Answers & Explanations Manual 2006 Supplement* (English edition, available January 2006)

Please contact Mark Ren at either 408-4288 or mren@osc.state.ny.us if you are interested in the CISM review course the Chapter plans on sponsoring, or in obtaining the Micromash CISA review software the Chapter will help pay for.

From the Desk of Membership

We would like to introduce two new members of the Hudson Valley Chapter:

- Gauray Dhawan
- Laura Iwan

Please join me in welcoming both of them! The Hudson Valley Chapter now stands at 169 members strong!

Professional Certification Information Seminar

Cosponsored by the local chapters of the ACFE, AGA, NYSSCPA, IIA, IMA & ISACA

Date: Thursday, February 2, 2006
Time: 8:00 am – 8:30 am – Registration, Coffee and Pastries
8:30 am – 10:00 am - Seminar
Location: Holiday Inn TURF, 205 Wolf Rd., Colonie, NY
Cost: Free, but you must pre-register
CPE: One (1)
Guest Speakers: Mary Peck, CIA, CCSA, CGAP
Robin MacGowan
Amy Harlow
Charles Norfleet, CFE
Jill Flinton, CPA, CGFM
Mark Ren, CISA
CPA rep.
Registration: Online: www.aganycap.org or contact Karen Lydon at Registrar@aganycap.org – (518) 286-2622 ex. 100

Attend the **Professional Certification Information Seminar** to learn about the:

- Various certifications available to government, finance, accounting, auditing, IT and fraud professions.
- Benefits of the professional certifications
- Requirements for applying and earning the professional certifications
- Exam details
- Maintenance requirements

The seminar will give you a quick overview of the following certifications:

- Certified Fraud Examiner (CFE)
- Certified Government Finance Manager (CGFM)
- Certified Information Systems Auditor (CISA)

- Certified Internal Auditor (CIA)
- Certified Public Accountant (CPA)
- Certified Management Accountant (CMA)
- Certified in Financial management (CFM)

Following a general discussion about the benefits of obtaining a professional certification, representatives from each of the certification sponsoring organizations will provide a brief overview of their professional certification. For the remainder of the session, attendees can visit with representatives, ask questions and obtain written information and publications regarding each certification.

6th Annual Technology Conference

The local chapters of the AGA, IIA, and ISACA will again join forces to present this must attend conference on technology issues affecting everyone, including the non- technical among us.

The theme this year is **DATA – the GOOD, the BAD and the UGLY**. We will focus on how data can be used, and abused. We will examine stories right out of recent headlines, including Medicaid fraud and personal identity theft, as well as, how these and other improper activities can be identified and prevented. We will look at how huge amounts of data can be effectively analyzed, how it can be compromised, and how it can be protected while in your possession. We will also look closely at New York State's Information Security Policy, the role of an entity's Information Security Officer (ISO), and how the ISO and auditor interact.

Speakers

Todd Holowchak - ACL
Yehuda Scheff - NYS Attorney General's Office
Officer Steve Heieder – Colonie Police Department
Laura Iwan- NYS Cyber Security and Critical Infrastructure Coordination
Ramon Rodriguez – NYS Office of the State Comptroller
Lynn Humiston – State Education Department

January 25, 2006

CPEs - 7

7:45 am – 8:15 am Registration

8:15 am – 4:15 pm Seminar (including lunch, continental breakfast and breaks)

\$75 for AGA, IIA, and ISACA members

\$125 for all others

\$25 discount for early registration (by January 18, 2006)

Location: Century House, Latham NY

Registration

You can register for this event on-line. You can also register by calling Karen Lydon directly at (518) 286-2622 Ext 100 or e-mail her at registrar@aganycap.org. If using e-mail, please be sure to include all of the information called for in the registration form. If you have any problems with on-line registration, please call or write Karen.

ISACA International News

Webcast From International President

To learn about the recent activities of ISACA and ITGI, as well as the organizations' strategic plan, visit www.isaca.org/board to view a webcast from International President Everett Johnson (the link to the webcast can be found at the end of Johnson's biography). The webcast, which takes approximately 20 minutes to view, describes Johnson's plans and aspirations for ISACA's future and covers:

- ISACA's recent achievements
- Recent ISACA and ITGI activities and upcoming deliverables
- A five-year strategic plan for ISACA and ITGI

Computer Security Day on 30 November Urges Organizations to Protect Their Information and Promote Security Awareness

Rolling Meadows, IL, USA (17 October 2005)—An organization's information security is the responsibility of all employees, regardless of the position they hold. To help people recognize their responsibilities and promote stronger security, the Information Systems Audit and Control Association® (ISACA®) is co-sponsoring Computer Security Day on 30 November.

Computer Security Day was started in 1988 by the Association for Computer Security Day to help raise awareness of computer-related security issues and to remind people how important it is to protect their computers and information.

The Association for Computer Security Day suggests more than 50 ways for companies to recognize Computer Security Day, including:

- Display computer security posters (available at www.computersecurityday.org).
- Offer a training session to provide all computer users with a basic understanding of computer security.
- Encourage password changes.
- Check for computer viruses.
- Back up data (after ensuring that the information is virus-free).
- Delete unnecessary files.
- Publicize the existing computer security policy or issue a new and improved computer security policy.
- Declare an amnesty day for computer security violators who wish to reform.
- Install and inspect power surge protection as appropriate.
- Install fire/smoke detection and suppression equipment in areas with computers.

To further assist organizations in strengthening their information security, ISACA recently released *Security Awareness: Best Practices to Secure Your Enterprise* (available at www.isaca.org/bookstore). The publication features 18 steps for creating a security awareness program and offers a self-assessment guide for evaluating the program.

"Information is among a business's greatest assets," said Everett Johnson, CPA, international president of ISACA. "It is crucial to make information security a high priority and to make employees aware of the important role they play in strengthening the organization's security."

About the Association for Computer Security Day

The Association for Computer Security Day (A4CSD) (www.computersecurityday.org)

coordinates the annual observance of Computer Security Day worldwide. Supported by sponsors and partners, the A4CSD produces and distributes posters and provides information that helps each participant focus attention on computer security at their own location. Computer Security Day began in 1988 and has official participants in more than 50 countries this year. Sponsors are Security Awareness Inc., ISACA, Symantec Inc., ACM/SIGSAC, ITAA, and ISSA.

Media Contacts

Kristen Bertholomey, +1.847.590.7455, kbertholomey@isaca.org

Deborah Vohasek, +1.847.590.7466, dvoasek@isaca.org