# Internet Safety & You

Tri-County Chapter of IAAP

March 11, 2008

# Gregory C. Pickett

- University of Georgia, ‘92 (ABJ)
- Ten Years experience in Information Technology (IT), focusing mainly on web development
- Earned J.D. / MBA (Univ. of Balt.) and passed Maryland State Bar in 2003
- Currently working in IT department for Wicomico County, Maryland

# There are agents even now working against you…

# Danger, Danger…

# What will we discuss?

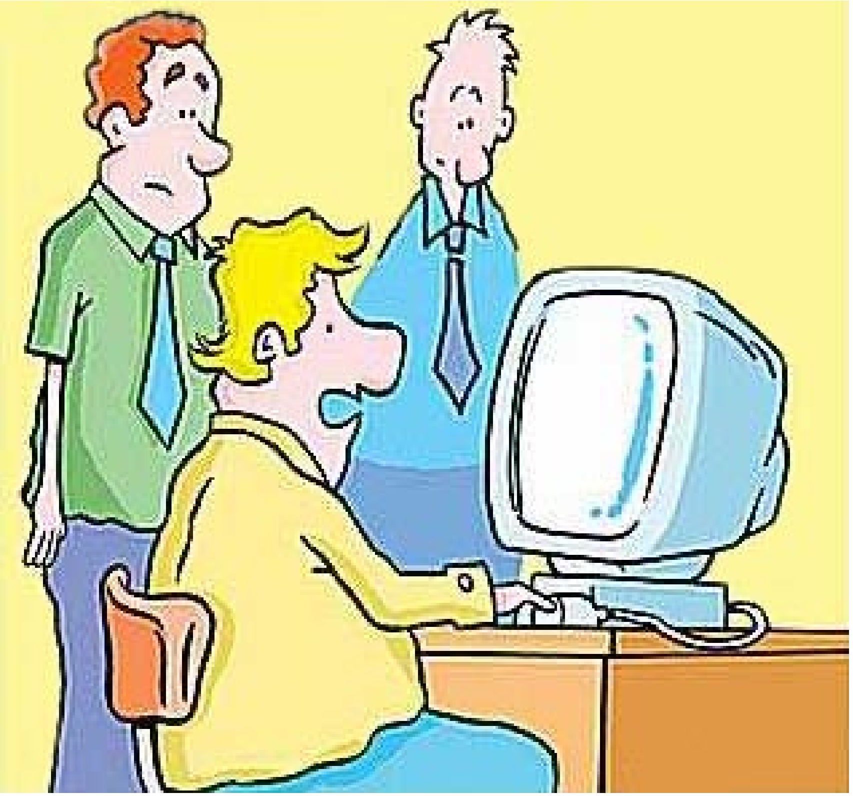
- Malware
- Identity Theft & Online Fraud
- Detection & Prevention

# 1) Malware

- “Malware” is short for malicious software and is typically used as a catch-all term to refer to any software (whether it’s a virus, spyware, etc.) designed to cause damage to:
  - single computer
  - server
  - computer network

http://www.microsoft.com/technet/security/alerts/info/malware.mspx

# “This is definitely a stealth polymorphic macro virus …”



# Types of Malware

- Virus
- Trojan Horse
- Adware
- Worms
- Spyware
- Rootkit

# Virus

- Viruses are computer programs or scripts that attempt to spread from one file to another on a single computer and/or from one computer to another, using a variety of methods, without the knowledge and consent of the computer user

# Virus

- Even … a simple virus is dangerous because it [can] quickly use all available memory and bring the system to a halt

http://www.webopedia.com/TERM/v/virus.html

# Virus

- [I]n March 1999, the *Melissa* virus was so powerful that it forced Microsoft and a number of other very large companies to completely turn off their e-mail systems until the virus could be contained

# Worm

- A worm is a specific type of virus that propagates itself across many computers, usually by creating copies of itself in each computer’s memory
- Experts estimate that the *Mydoom* worm infected approximately a quarter-million computers in a single day in January 2004

# Trojan Horse

# Trojan Horse

- A Trojan Horse … attempts to infiltrate a computer without the user’s knowledge or consent
- A recent example of … a Trojan Horse is the recent e-mail version of the *Swen* virus, which falsely claimed to be a Microsoft update application

# Spyware

SPY VS SPY 2
THE JOKE AND DAGGER FILES
MORE MAD MISSIONS OF MADNESS
BY DAVID SHAYNE
FOREWORD BY J.J. ABRAMS

# Spyware

- Spyware is a program that runs on your computer and … tracks your Internet habits ...
- Spyware sends personal information to a 3rd party without your permission or knowledge

http://www.microsoft.com/windowsxp/using/security/expert/honeycutt_spyware.mspx

# Spyware

- This information can include …
  - Web sites you visit
  - Your user name and password
- [C]ompanies often use this data to send you unsolicited targeted advertisements

# Adware

- Adware is software that displays advertisements on your computer
- These are ads that inexplicably pop up on your … screen, even if you’re not browsing the Internet
- Some companies provide “free” software in exchange for advertising on your [screen]

# Rootkit

- A rootkit is a collection of tools (programs) that enable administrator-level access to a computer or computer network

http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci547279,00.html

# Rootkit

- Typically, a [hacker] installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or ‘cracking’ a password
- Once the rootkit is installed, it allows the attacker to:
  - mask intrusion
  - gain root or privileged access to the computer
  - possibly gain access to other network machines

# Rootkits…

- monitor traffic and keystrokes
- create a “backdoor” into the system for the hacker's use
- alter log files
- attack other machines on the network
- alter existing system tools to escape detection

# Rootkit

- If a rootkit is detected, however, the only sure way to get rid of it is to completely erase the computer’s hard drive and reinstall the operating system

# 2) Identity Theft & Online Fraud

- Phishing
- 419 Fraud
- IRS Notification Fraud

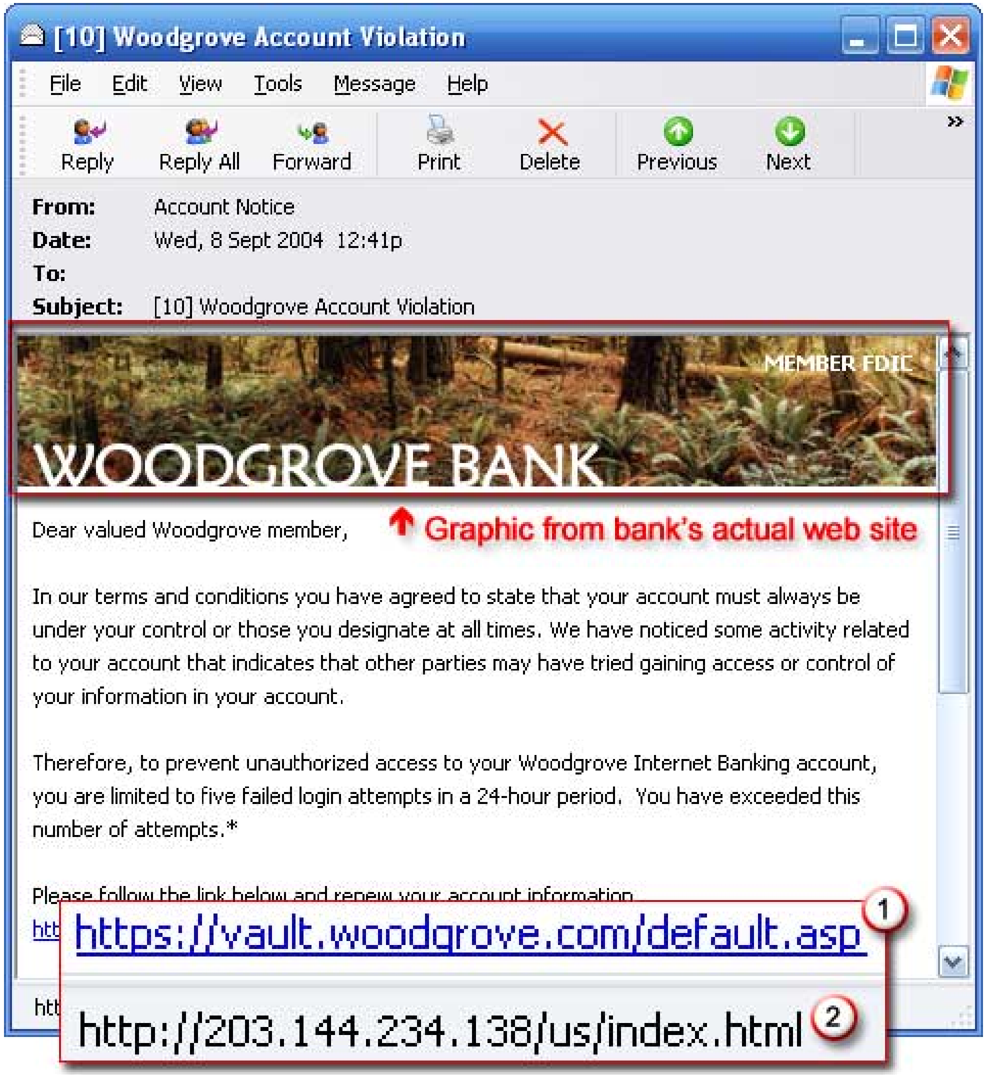
# Phishing

# Phishing

- Phishing is a type of deception designed to steal your valuable personal data, such as:
  - credit card numbers
  - passwords
  - account data
  - other information

http://www.microsoft.com/protect/yourself/phishing/identify.mspx

# Phishing



**From:** Account Notice
**Date:** Wed, 8 Sept 2004 12:41p
**To:**
**Subject:** [10] Woodgrove Account Violation

Graphic from bank's actual web site

Dear valued Woodgrove member,

In our terms and conditions you have agreed to state that your account must always be under your control or those you designate at all times. We have noticed some activity related to your account that indicates that other parties may have tried gaining access or control of your information in your account.

Therefore, to prevent unauthorized access to your Woodgrove Internet Banking account, you are limited to five failed login attempts in a 24-hour period. You have exceeded this number of attempts.*

Please follow the link below and renew your account information.

htt

1 https://vault.woodgrove.com/default.asp

htt

2 http://203.144.234.138/us/index.html

# Phishing

- To make these phishing e-mail messages look even more legitimate, the scam artists may place a link in them that appears to go to the legitimate Web site but:
  - actually takes you to a phony scam site; or
  - takes you to a pop-up window that looks exactly like the official site

# Phishing “Bait”

- “Verify your account” (Not with email)
- “If you don't respond within 48 hours, your account will be closed” (Hurry!)
- “Dear Valued Customer” (No name)
- “Click the link below to gain access to your account” (link is fraudulent)

# Phishing

- Fradulent Uniform Resource Locators (URLs) are also used to trick users to go to a disreputable website:
  - – http://www.mi**c**osoft.com (no ‘r’)
  - – http://www.infomation.com (no ‘r’)

# Phishing losses in $$$

- It is estimated that between May 2004 and May 2005, approximately 1.2 million computer users in the United States suffered losses caused by phishing, totaling approximately $929 million

http://www.thesecryption.com/email-encryption/Phishing.html

# 419 Fraud (Nigerian Letter)

- a letter / email, mailed from Nigeria, offers the recipient the “opportunity” to share in a percentage of millions of dollars that the author, a self-proclaimed government official, is trying to transfer illegally out of Nigeria

http://www.fbi.gov/majcases/fraud/fraudschemes.htm

# 419 Fraud (Nigerian Letter)

- The recipient is encouraged to send the following information to the author [via] a facsimile number provided in the letter:
  - – blank letterhead stationery
  - – bank name
  - – account numbers
  - – other identifying information

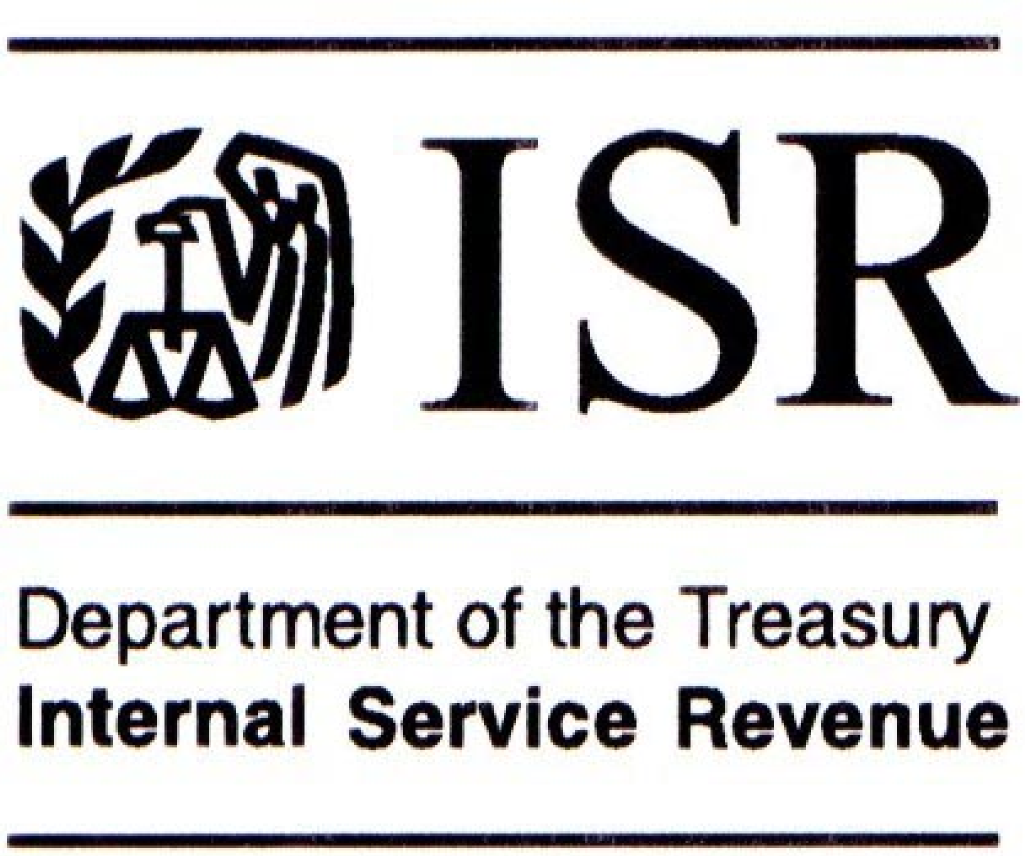
# 419 Fraud (Nigerian Letter)

- Payment of taxes, bribes to government officials, and legal fees are often described in great detail with the promise that all expenses will be reimbursed as soon as the funds are spirited out of Nigeria
- In actuality, the millions of dollars do not exist and the victim eventually ends up with nothing but a loss

# 419 Fraud (Nigerian Letter)

- The schemes themselves violate section 419 of the Nigerian criminal code, hence the label “419 fraud”
- Subculture now exists – scam the scammers:
  - http://www.419eater.com/
  - http://scambuster419.co.uk/

# IRS Notification Fraud



ISR

Department of the Treasury
Internal Service Revenue

# IRS Notification Fraud

- Example 1: e-mail scam intended to fool people into believing they are under investigation by the IRS's Criminal Investigation division

  http://www.irs.gov/newsroom/article/0,,id=170894,00.html

# IRS Notification Fraud

- e-mail purporting to be from IRS Criminal Investigation falsely states that the person is under a criminal probe for submitting a false tax return to the California Franchise Tax Board
- e-mail seeks to entice people to click on a link or open an attachment to learn more information about the complaint against them

# IRS Notification Fraud

- The IRS warned people that the e-mail link and attachment is a *Trojan Horse* that can take over the person’s computer hard drive and allow someone to have remote access to the computer [to steal financial data]
- <u>Example 2</u>: Similar e-mail variations suggest a customer has filed a complaint against a company and the IRS can act as an arbitrator

# 3) Detection & Prevention

- Is computer running abnormally slow?
- Will your computer not turn off?
- Are you getting pop-ups frequently?
- Are you getting more spam recently?
- Are applications crashing or is system functionality limited?
- Are you finding mysterious files on hard drive?

# Anti-Virus Tools

- Norton Internet Security (http://www.symantec.com/norton/products/)
- McAfee VirusScan (http://www.mcafee.com/)
- AVG Free Advisor (http://free.grisoft.com/)*
- Avira AntiVir (http://www.free-av.com/)*

* Freeware

# Anti-Spyware Tools

- Adaware (http://www.lavasoftusa.com/)*
- Spybot (http://www.safer-networking.org)*
- Windows Defender (http://www.microsoft.com/athome/security/spyware/software/default.mspx)

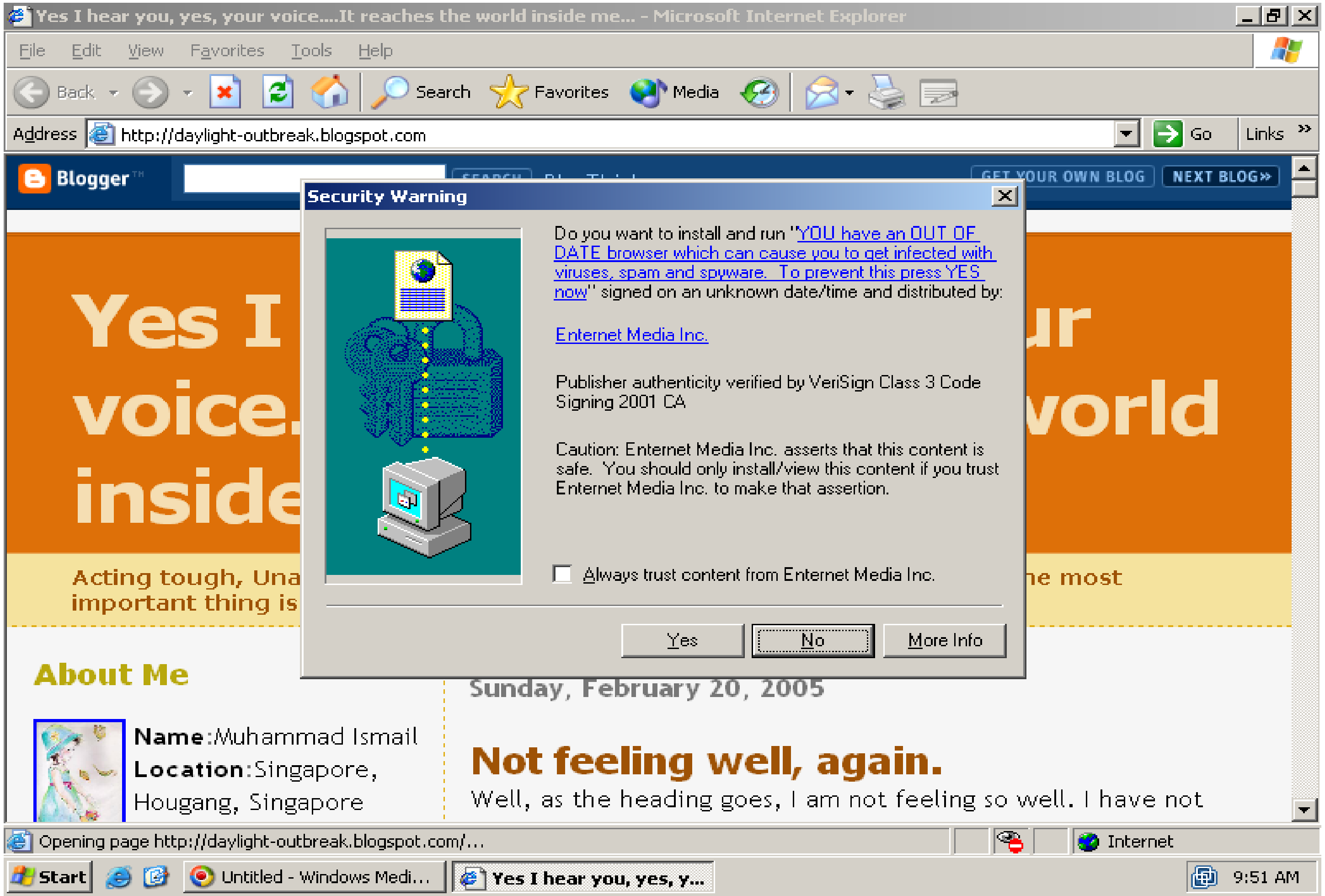
* Freeware. (Windows Defender requires certified Windows license)

# Be Active in Prevention

- Windows Update (http://www.update.microsoft.com/)*
- Up-to-date browser: IE 7 or Firefox 2
- Windows XP, Vista: Firewall on
- Visit only trusted, reputable websites
- Don't open unsolicited emails

*Requires Internet Explorer (IE) 5 or later

# Don’t click on pop-ups or ‘alerts’



Yes I hear you, yes, your voice....It reaches the world inside me... - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://daylight-outbreak.blogspot.com
Go Links
Blogger
GET YOUR OWN BLOG
NEXT BLOG»
Yes I ... ur
voice. ... vorld
inside
Acting tough, Una ... he most
important thing is
About Me
Name:Muhammad Ismail
Location:Singapore, Hougang, Singapore
Sunday, February 20, 2005
Not feeling well, again.
Well, as the heading goes, I am not feeling so well. I have not
Opening page http://daylight-outbreak.blogspot.com/...
Internet
Start
Untitled - Windows Medi...
Yes I hear you, yes, y...
9:51 AM

Security Warning

Do you want to install and run "YOU have an OUT OF DATE browser which can cause you to get infected with viruses, spam and spyware. To prevent this press YES now" signed on an unknown date/time and distributed by:

Enternet Media Inc.

Publisher authenticity verified by VeriSign Class 3 Code Signing 2001 CA

Caution: Enternet Media Inc. asserts that this content is safe. You should only install/view this content if you trust Enternet Media Inc. to make that assertion.

□ Always trust content from Enternet Media Inc.

Yes | No | More Info

# Be Active in Prevention

- Update anti-spyware / anti-virus definitions daily
- Run anti-spyware / anti-virus tools frequently
- Research security threats in periodicals / websites on

# Be Active in Prevention

- Careful when installing freeware games or utilities
- Run file sharing programs at your <u>own risk</u>
- Create separate email accounts for online orders, blogging, and personal use

# Be Active in Prevention

- Password protect computer
- Do not logon as ‘Administrator’ unless installing software or doing administrative tasks
- Back-up (old computer -> data server)
- Turn off / log off computer
- Reinstall Windows annually

# Guard Identity & Avoid Fraud

- Phishing
  - Guard your account information carefully
  - Never send, via the web, money or give out the following personal information to unfamiliar companies or unknown persons:
    - credit card numbers and expiration dates
    - bank account numbers
    - dates of birth
    - social security numbers

# Guard Identity & Avoid Fraud

- Phishing
  - Reconcile your bank account monthly and notify your bank of discrepancies immediately
  - Report unauthorized financial transactions to your bank, credit card company, and the police as soon as you detect them

http://www.fbi.gov/majcases/fraud/fraudschemes.htm

# Guard Identity & Avoid Fraud

- Phishing
  - Review a copy of your credit report at least once each year.
  - Notify the credit bureau in writing of any questionable entries and follow through until they are explained or removed
  - Don’t buy from an unfamiliar company; legitimate businesses understand that you want more information about their company and are happy to comply

# Guard Identity & Avoid Fraud

- 419 Fraud (Nigerian Letter)
  - If you receive a letter from Nigeria asking you to send personal or banking information, do not reply in any manner. Send the letter to:
    - U.S. Secret Service
    - Your local FBI office
    - U.S. Postal Inspection Service

# Guard Identity & Avoid Fraud

- 419 Fraud (Nigerian Letter)
  - Be skeptical of individuals representing themselves as Nigerian or foreign government officials asking for your help in placing large sums of money in overseas bank accounts
  - Do not believe the promise of large sums of money for your ‘cooperation’

# Guard Identity & Avoid Fraud

- IRS Notification Fraud
  - The IRS does not send out unsolicited e-mails or ask for detailed personal and financial information
  - [T]he IRS never asks people for:
    - PIN numbers
    - Passwords
    - Other secret access information for their credit card, bank or other financial accounts

# Guard Identity & Avoid Fraud

- IRS Notification Fraud
  - Recipients of questionable e-mails claiming to come from the IRS should not open any attachments or click on any links contained in the e-mails. Instead, they should forward the e-mails to phishing@irs.gov

# The End

Gregory C. Pickett
gdawg1992@yahoo.com