Safe and Secure Computing

Brian Kellogg – SBU Network Manager

Mike Hoffman – SBU Executive Director for Information Technology

Recent History of Computer Security

- Hackers
- Viruses
- Worms

- - Generally nuisance or destructive

Today’s Threats

- Malware
  - from the words malicious and software, is software designed to infiltrate or damage a computer system without the owner's informed consent.
- Adware
  - any software package which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used.
- Phishing
  - the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.
- Spyware
  - computer software that is installed surreptitiously on a personal computer to intercept or take partial control over the user's interaction with the computer, without the user's informed consent.
- Bots
  - are software applications that run automated tasks over the Internet.
- Rootkits
  - Malware which consists of a program (or combination of several programs) designed to take control of a computer system, without authorization by the system's owners and legitimate managers.

- Major difference – today’s threats are almost always difficult to detect
- New Motive – Money $$$$$$

Today’s Threats

- Who is responsible for these threats?
  - Organized crime
  - Unscrupulous individuals
- What do they want?
  - Identity – identity theft
  - Computing power
    - Using your computer to perpetrate attacks on others
- Social engineering - the act of manipulating people into performing actions or divulging confidential information.
  - The weakest point in any security policy is people
  - Shoulder surfing
  - Impersonation
- P2p – Peer to Peer networks
  - Kazaa, Gnutella, …
  - Using many p2p applications greatly increases your security and legal risks

How can you Protect Yourself?

- Anti-Virus
- Anti-Spyware
- Operating System Updates (windows updates)
  - Make sure all three of these are kept up to date, check at least once a month
  - Enable automatic updates on your computers
- Passwords
  - The backbone of almost all security, strong passwords are vital
    - Strong Passwords – password that isn't easily guessed or broken
    - Passwords should be Reasonable and Functional, but at the same time be strong

Passwords

- How are passwords "cracked"?
  - Guessing, dictionary attack, brute-force attack, social engineering
- Weak Password – Examples
  - Dictionary word – automobile
  - Number Substitutions – aut0m0b1le
  - Doubled words – automobileautomobile
  - Anything easily known or guessed (birthday, ect.)
- Strong Passwords – password that isn't easily guessed or broken
  - Passwords should be Reasonable and Functional, but at the same time be Strong
  - Longer, more complex passwords are exponentially more difficult to "crack".
    - A six character lower-case letter password has 308 million possible combinations
    - A seven character password utilizing lower case, upper case, and numbers has 3.5 trillion possible combinations

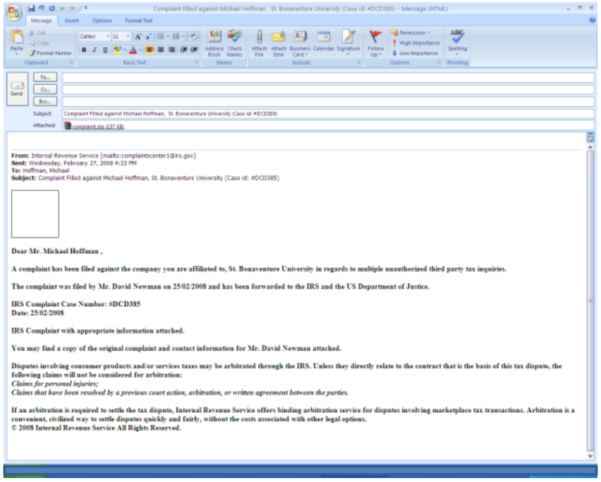
Passwords cont.

- Passphrase
  - Use a phrase as your password, ?Eye love Tech Services, easy to remember and relatively hard to crack (although not a good choice for me ☺)
  - Should be easy to remember and type, but not a famous quote or something that could easily be guessed
- Convert your Passphrase to a Password
  - I Love Tech Services at St. Bonaventure University
    - LTSaSBU
  - Add some punctuation:
    - ?ILTSaSBU!
- Recommendation
  - A password at least 10 characters long, containing upper & lower case letters, numbers, and symbols
  - Test your password: http://www.microsoft.com/protect/yourself/password/checker.mspx

Phishing

- Attempting to acquire sensitive information such as usernames & passwords by masquerading as a legitimate entity.
- Very creative
  - Banks, Ebay, Federal/State Govt., etc.
  - SBU Example
- How do you defend yourself?
  - Google is your friend
  - Visit the legitimate site, DON'T click the link or open the attachment

Phishing Example



Complaint Filed against Michael Hoffman, St. Bonaventure University (Case id: #DCD385) - Message (HTML)

Subject: Complaint Filed against Michael Hoffman, St. Bonaventure University (Case id: #DCD385)

Attached: complaint.zip (137 KB)

From: Internal Revenue Service [mailto:complaintscenter1@irs.gov]
Sent: Wednesday, February 27, 2008 4:23 PM
To: Hoffman, Michael
Subject: Complaint Filed against Michael Hoffman, St. Bonaventure University (Case id: #DCD385)

Dear Mr. Michael Hoffman ,

A complaint has been filed against the company you are affiliated to, St. Bonaventure University in regards to multiple unauthorized third party tax inquiries.

The complaint was filed by Mr. David Newman on 25/02/2008 and has been forwarded to the IRS and the US Department of Justice.

IRS Complaint Case Number: #DCD385
Date: 25/02/2008

IRS Complaint with appropriate information attached.

You may find a copy of the original complaint and contact information for Mr. David Newman attached.

Disputes involving consumer products and/or services taxes may be arbitrated through the IRS. Unless they directly relate to the contract that is the basis of this tax dispute, the following claims will not be considered for arbitration:
Claims for personal injuries;
Claims that have been resolved by a previous court action, arbitration, or written agreement between the parties.

If an arbitration is required to settle the tax dispute, Internal Revenue Service offers binding arbitration service for disputes involving marketplace tax transactions. Arbitration is a convenient, civilized way to settle disputes quickly and fairly, without the costs associated with other legal options.
© 2008 Internal Revenue Service All Rights Reserved.

2 Factor Authentication

- An authentication factor is a piece of information and process used to authenticate or verify a person's identity for security purposes.
- Something a person knows, Something a person has, and Something a person is
  - Bank example
- Is being investigated at SBU
- Security is always a balancing act between cost, intrusiveness, and risk.
- 2 factor authentication is more secure, but is also considerably more costly and relatively more intrusive.

Encryption

- What is it?
  - The encoding of information in such a way as to make it unreadable by everyone/everything except for the source and destination.
  - Example – Simple Substitution
    - boot - substitute x for b, z for o, and 5 for t
    - boot becomes xzz5
    - Encryption has been in use for thousands of years (used by the Romans)
- SBU VPN and Faculty and Staff wireless uses encryption to protect all traffic
- Most SBU server backups are encrypted so that if anyone stole our backup tapes the data would be unusable
- Hard drive encryption is being looked into

Encryption

- How can you use encryption to protect your information?
  - Secure websites use encryption, check for the lock icon to ensure the website is encrypted
  - Use a file compression utility such as WinZip to compress and encrypt your file, allowing it to be safely transmitted via email (but don’t send the password).

Wireless Security

- Wireless is a shared medium – anything a computer or Access Point transmits or receives can be viewed by anyone else in proximity with the right tools. Thus why we use encryption to protect the transmission here at SBU.
- Best Practices:
  - Change default administrator passwords for your Access Point and your computers
  - Turn on WPA encryption. ONLY USE WEP ENCRYPTION IF THAT IS YOUR ONLY OPTION. Better to buy a new Access Point and wireless card if WEP is your only option.
  - Change the default SSID. The default SSID and AP admin password are readily available on the internet.
  - Disable SSID broadcast for your AP at home
  - Enable firewalls on all of your computers and APs
  - Do not auto connect to open Wi-Fi networks

SBU Wireless Networks

- Student Network
  - Authenticated and un-encrypted
- Fac/Staff Network
  - Authenticated and encrypted
- There is a student encrypted wireless network as well, but it requires some manual configuration on the users end so we do not advertise it.

General Tips

- Shopping online? Use a credit card – not a debit card.
- If you are given the option on the website to save your credit card information – DON’T
- Don’t open attachments sent from strangers
- Lock your computer, at work or at home
- Screensaver password – get one
- Recognize the risks, only risk-free computer is one that is turned off.

Questions…