Internet (In)Security

Don Orifice, CISSP

February 20, 2004

Internet (In)Security

- Agenda
  - Identity Theft
  - Email
    - SPAM and Scams
  - Viruses, Trojans and Worms, Oh My!
  - Security Today

Internet (In)Security

- Identity Theft
  - Your money AND your life
- What is it?
  - Theft of personal info for fraudulent use
- Who does it affect?
  - Over 5 million people annually and growing
- How serious is it?
  - Possible loss of job or credit, even arrest

Internet (In)Security

- How can you prevent Identity Theft?
  - Manage and Protect Your Personal Information
- How is it typically done?
  - Company employees
    - Bribes, hacking, trickery
  - Dumpster diving
  - Improper use of credit reports
  - Stolen credit card numbers (skimming)
  - Stolen wallets, purses and mail
  - Social engineering
    - Read *The Art of Deception* by Kevin Mitnick

Internet (In)Security

- But what can they do with this info?
  - Spending spree
  - Open a new charge account
  - Change your mailing address
  - Take out an auto loan
  - File for bankruptcy
  - Counterfeit checks and debit cards
  - New bank account
  - Use your name when arrested

Internet (In)Security

- How can you tell you are a victim?
  - Failure to receive bills or other mail
  - Receiving unsolicited credit cards or bills
  - Credit denial
  - Collection calls from debt collectors

Internet (In)Security

- How can you reduce your exposure?
  - Use passwords on all of your accounts
  - Use strong passwords that:
    - Use letters, numbers AND symbols if possible
    - Are a minimum of 6 characters, or better 8
    - Are not a dictionary word, name or sequence of #s
  - Keep your information secure
    - Consider roommate(s), cleaning crews, services
  - Find out about access and disposal at work
    - Dumpster diving is still alive and well

Internet (In)Security

- Other means of protection
  - Don’t give personal info unless you place call
    - Social engineers are very good at what they do
  - Confirm identity of callers by call back
    - But don’t use the number they tell you!
  - Guard mail by using Post Office or mailbox
  - Use vacation hold at Post Office

Internet (In)Security

- ♦ Other ways to protect your information
  - – Shred all private information such as:
    - Charge receipts
    - Credit applications
    - Insurance forms
    - Checks and bank statements
    - Expired charge cards and ID cards
    - Medical statements

Internet (In)Security

- Other ways to prevent abuse
  - Before revealing information, ask how it will be used – it may not be necessary
  - Stop using your SSN for identification
  - Limit how many cards you actually carry

Internet (In)Security

- Secure Your Computer
  - Use Antivirus Software
    - eTrust, AVG, Symantec, McAfee, Sophos
  - Keep antivirus software up to date
    - Update at least once or twice a week or even daily
  - Update your operating system regularly
    - Second Tuesday of each month (Microsoft)
  - Don’t download files from anyone!
    - Especially friends
  - Use a firewall or two
    - Personal firewall for your computer
      - ZoneAlarm, BlackICE, McAfee, Symantec
    - Hardware firewall for the network
      - Linksys, Dlink, Sonicwall

Internet (In)Security

- Computer Security
  - Practice Secure Browsing
    - Look for the lock icon on browser
  - Minimize storage of personal information
    - Consider what the loss of your computer would do
  - Use strong passwords and change them
    - Letters (UPPER & lower), numbers and symbols
    - Minimum 6 characters long, 8 is better
    - No dictionary words, names or sequence of numbers
    - Example: use first letters of easy to remember phrase
      - Then change some letters to numbers – E to 3, S to 5, etc.

Internet (In)Security

- Computer Security
  - Consider changing operating systems
    - Windows 95, 98, ME all wide open
    - Windows 2000, XP allow security & encryption
  - Don’t use automatic login
    - Especially for laptops and remote access
  - Use a WIPE program before disposal
    - But please send disks with your donation
  - Pay attention to Web site privacy policies

Internet (In)Security

- What to do if you suspect Identity Theft
  - Place a fraud alert with the 3 credit bureaus
    - Equifax – www.equifax.com
    - Experian – www.experian.com
    - Trans Union – www.transunion.com
  - Close any accounts that have been abused
  - File a police report immediately
  - File a complaint with the FTC
    - 1-877-ID-THEFT

Internet (In)Security - Email

- SPAM (aka UCE)
  - AOL claims to block 1.5 billion messages a day
  - As much as 40% of legit emails go undelivered
  - SPAM filters must be monitored
    - Any false positive is unacceptable
    - Who is checking? Raises privacy issues…

Internet (In)Security - Email

- Examples of Scams
  - Nigerian (and other African ruses)
  - Beware of “Phishing” expeditions
    - PayPal, Amazon, eBay, FDIC, etc.
  - Microsoft system updates
    - No company will ever send software updates!
    - Repeat the above until you remember it!
  - Hoaxes
    - Check out www.snopes.com to debunk

Internet (In)Security - Viruses

- Viruses, Trojans and Worms, Oh My!
  - All are forms of Malware
    - Virus – attached to something else
    - Trojan – disguised as something else
    - Worm – self spreading using security flaw

Internet (In)Security - Viruses

- Viruses
  - Keep your antivirus software up to date
  - Don’t open attachments!!!!!
    - Call or email the sender to confirm
    - Even then, make sure your AV software is current
  - Quarantine the attachments
  - Turn off the preview pane until offline

Internet (In)Security - Trojans

- Trojan Programs
  - Beware the hidden agenda
  - Spyware falls in this category
    - Use Ad-aware or Hijack This or SpyBot (or all)
  - Block executables at the external firewalls
    - Only practical on corporate networks, not home
  - Don’t run any program unless absolutely sure
  - Use a personal firewall program
    - Beware of XP – only protects against incoming

Internet (In)Security - Worms

- Worms are self spreading
  - No action required – can be devastating
  - Keep your operating systems up to date
  - Use firewalls (personal and hardware)
  - Minimize Instant Messenger use
    - Lock it down
    - Prevent incoming programs
    - Connect only with known people
  - Block Windows messenger service

Internet (In)Security - Firewalls

- Personal Firewalls
  - Software, host based
  - Protect from outside in AND inside out
    - Windows XP only protects from outside in
  - Monitor all program and process activity
    - Report when unusual activity occurs
    - Must usually be “trained”
    - Without external (hardware) firewall, very noisy
  - Can be disabled by some trojans and worms

Internet (In)Security - Firewalls

- ♦ Why use a Hardware Firewall?
- ♦ Is a Router a Firewall?
- ♦ What exactly is NAT & how does it work?
  - – Network Address Translation
  - – Hides internal devices behind router
  - – Usually many addresses inside, one outside
    - • This protects inside from uninitiated contact
    - • But not if your computer starts the conversation
    - • This is a problem for certain applications

Internet (In)Security - NAT

192.168.1.25 – Your computer

|||

192.168.1.1 – Router inside address ←→ Router outside address– 20.24.15.3

|||

Destination 173.35.67.8

Internet (In)Security – NAT

192.168.1.25 – Your computer
192.168.1.30 – Your other computer(s)
|||
192.168.1.1 – Router inside address ←→ Router outside address– 20.24.15.3
|||
Destination 173.35.67.8

Internet (In)Security

- Security Today
  - Practice Security in Depth
    - Layers are important in security AND cold weather
  - Keep your head out of the sand

Internet (In)Security

- So, anyone here still think they are secure?
- There are risks, but with awareness and reasonable care, they can be controlled
- Think twice (or thrice) before you act

Internet (In)Security

Questions?

Contact information:

Don Orifice, CISSP
dono@northshore.org
888-955-NSCS (6727)