



THE SPYWARE EPIDEMIC

Protecting Your Member Information and Confidence



Presented by:
Jim Soenksen and Ed Sale

You Will Learn:

- What is Spyware and How it Spreads
- How Spyware Can Affect Business
- Regulatory Compliance and Your Responsibilities
- Legal Recourse
- How to Know and What to Do if Your Credit Union is Infected with Spyware
- How to Protect Your Credit Union from Spyware
- Anti-Spyware Solutions
- Reference and Help Sites

What is Spyware?

- *Spyware* is a type of software that usually installs itself without a user's permission and collects data on a user's activities and from his computer
- *Adware* is a type of software that is also installed with or without permission that presents advertisements and controls where users may surf the Internet

Who Installs Spyware?

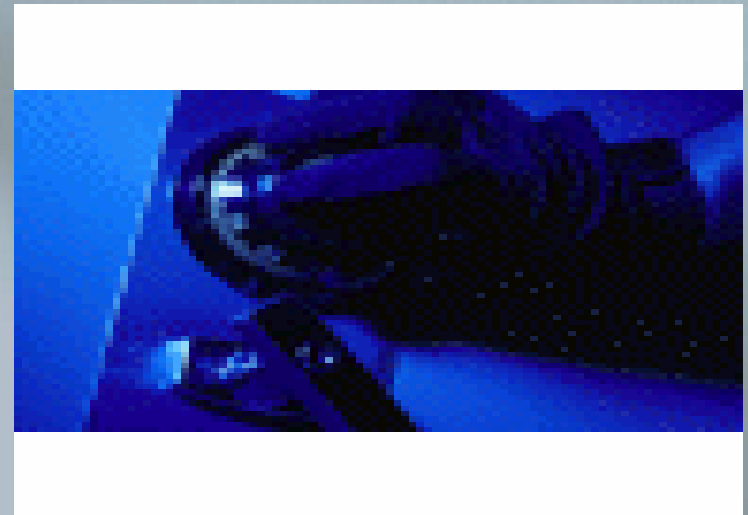
- Legitimate Companies, like:
Sony, BellSouth, Kodak
- Hacker Marketers
- Organized Crime

Recent Spyware Incidents



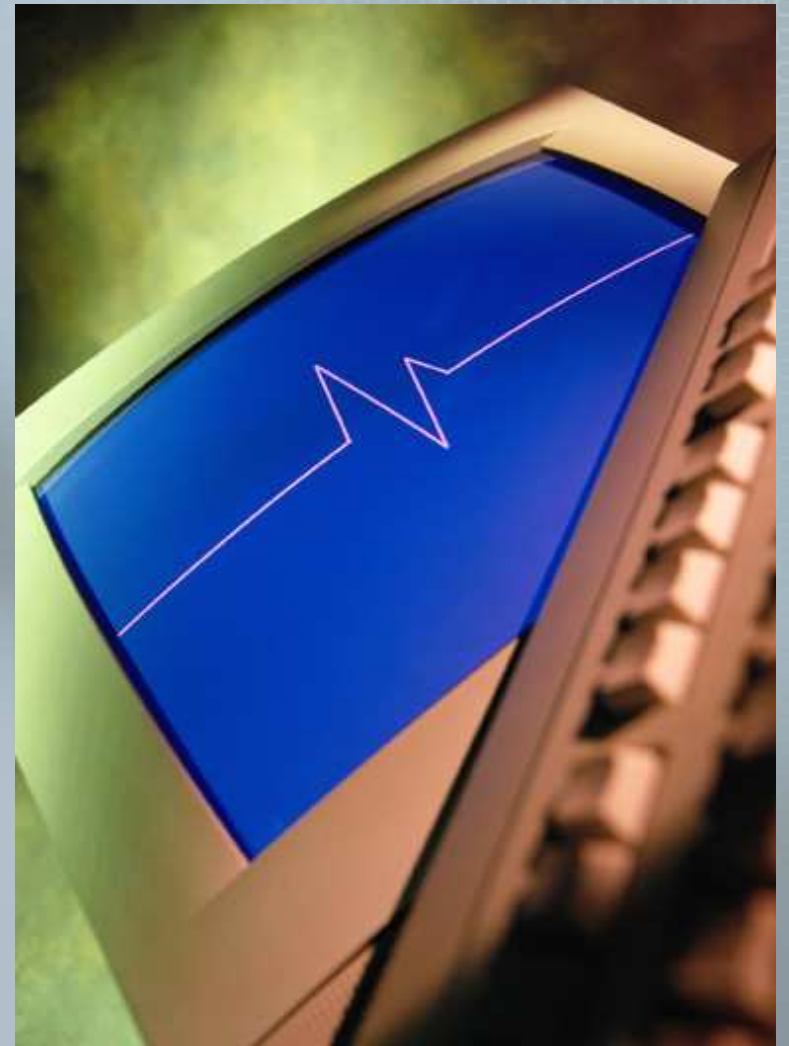
■ Web Mob

■ ID Theft



Negative Effects of Spyware

- Reduced System Performance
- Reduced System Security
- Directed Web Browsing
- Unwanted Pop-Up Advertising
- Loss of Privacy
- Identity Theft



What to Expect if You Do Have Spyware

- Most Symptoms are Curable *IF* Treated in a Timely Manner
- Some Possible Lingering Effects:
 - Loss of Confidential Information
 - Fraud
 - ID Theft
 - Damage to Reputation
 - Quantifiable Damages - \$

Regulatory Compliance Responsibilities

- Reg 748 Part A & B
- Protect Member Information
- Incident Response Program



According to Current Legal Precedents, You are Liable if...

- You have Violated Company Policy
- You had Negligent or Malicious Intent
- You did not Mitigate Damages
- There are Quantifiable Monetary Damages
- You have Ruined a Reputation

If Spyware Happens to You, Your Legal Recourse Options are:

- Prove and Quantify Damages
- Prove Negligence or Malicious Intent
- Find Perpetrator (often difficult)
- Use Law Enforcement Assistance for Damages Over \$25,000

Questions to Ask if You Think Your Network is Infected

- Are You Missing Any Security Updates?
- Have You Installed Any Free Software Lately?
- Have You Shared Music, Files, or Photos?
- What are the Pop-Ups Advertising?
- Spyware on an Infected System can:
 - Gather Data, Monitor Surfing Habits
 - Log Keystrokes
 - Modify or Direct Web Surfing
 - Execute Malicious Code
 - Extract Data

Nuisance...to Pest...to Threat!!!

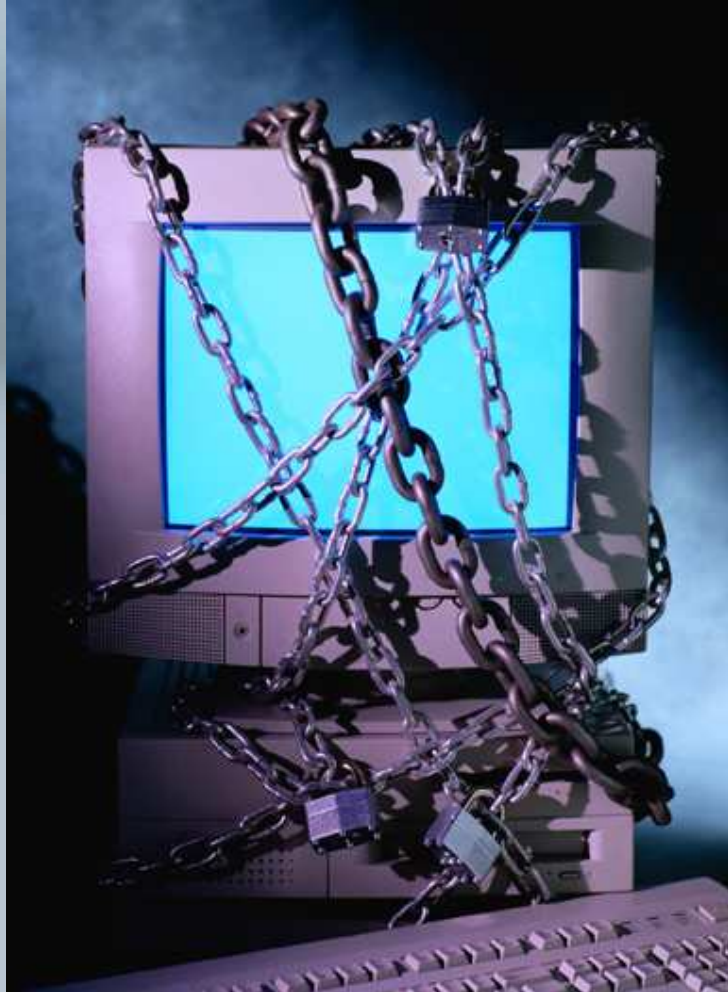
How Spyware Spreads

- Browse an Infected Site
- Download Infected Freeware
- Receive Infected E-mail

- Threats Double Every 12 Months
- Universities Teach How to Build Spyware
- Over 50% of Corporate America does Nothing
- Over 90% of All Computers have Spyware
- Average of 28 Infections per Computer

- No Policies or Procedures in Place
- No Education or Training Performed
- No Defense or Monitoring Technology

Now You Need To...



- Identify, Stop, Remove, and Immunize
- Take Inventory of Damages
- Notify Appropriate Parties
- Implement Best Security Practices

Spyware Detection and Prevention

- Layered Technology Defense
- On-Going Monitoring, Scanning, Removal, and Updates
- Policy and Procedures
- Education
- Active Security Program
- Independent Audit and Assessment

look, plan, act, repeat

Anti-Spyware Solutions

- Freeware
- Personal / Enterprise
- Appliance
- Administrative

Freeware Solutions

Products

AdAware, SpyBot, SpywareData SSI

- Good for Home Users; Lacking for Organizations
- Targeted Solutions, not Part of Software Bundle

Personal / Enterprise Solutions

Products

SpySweeper, CounterSpy, Norton, McAfee, Trend, Microsoft

- Allow Central Management, Monitoring, and Reporting
- Some Targeted, Some Bundled
- None 100% Effective
- Using Multiple Tools is Most Effective

Appliance Solutions

Products

McAfee *Secure Web Gateway*

Trend Micro *OfficeScan 7*

Finjan *VSA NG-5000*

- Attempt to Stop Attacks in Network Appliance for an Entire Enterprise
- Bundled with Other Types of Protection
- Good to Use Along with a Targeted Enterprise Solution

Administrative Solutions

From article by Ed Skoudis

Information Security July 2005

1. Create DNS Black Holes
2. Restrict User Privileges
3. Use AD Group Policy Objects (GPOs)
4. Use Alternative Browser
5. Use Network IPS
6. Use Web Proxy
7. Spyware Detection/Removal at Startup

Reference and Help Sites

- www.stopbadware.com
- www.benedelman.org/news/040406-1.html
- www.spywareguide.com
- www.spywaredata.com
- www.bleedingsnort.com
- www.intelguardians.com
- informationsecurity.techtarget.com
- buyersguide.eweek.com
- www.sans.org
- www.pivotgroup.net
- www.infragard.net
- www.microsoft.com
- www.us-cert.gov
- www.webroot.com



THANK YOU

from Jim Soenksen and Ed Sale

O:404-419-2163 jsoenksen@pivotgroup.net

look, **plan**, **act**, **repeat**



Questions and Answers