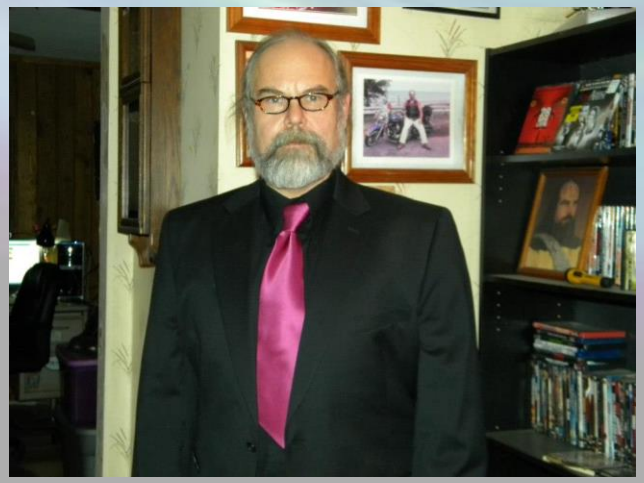
Protecting Your Privacy Online:

Some Practical Tips



Dr. Gerald M. Santoro
College of IST
Penn State University
24-October-2013

Introduction

The emerging era of Information/Communication technologies has resulted in much human activity going online

Or being stored in networked computer systems

The net result has been an increasing threat to our personal security and privacy.

Introduction

The goal for this talk is to discuss the multitude of threats

- And to provide a number of practical tips and resources to enable the individual to, as much as possible, secure their information and communications

The accompanying Web site will contain links to many resources

http://www.personal.psu.edu/gms/privacy/privacy.htm

Introduction

Despite what you read in the 'news' the greatest threat to your security and privacy is from cyber criminals

According to GoGulf.com:

- **there are 556 million victims of cyber-crime each ye**
  - **1.5 million per day or 18 per second**
- **232.4 million result in identity theft**
- **50% of cyber-attacks involve malware or spyware**
- **22% of cyber-attacks involve phishing**
- **17% of cyber-attacks involve social engineering**
- **38.9% of data breaches involve healthcare**
- **35.1% of data breaches involve business**

Introduction

According to GoGulf.com:

- **40% of cyber-attacks are motivated by theft**
- **50% of cyber-attacks are motivated by hacktivism**
- **the top country of origin for cyber-attacks is Russia**

http://www.go-gulf.com/blog/cyber-crime/

Introduction

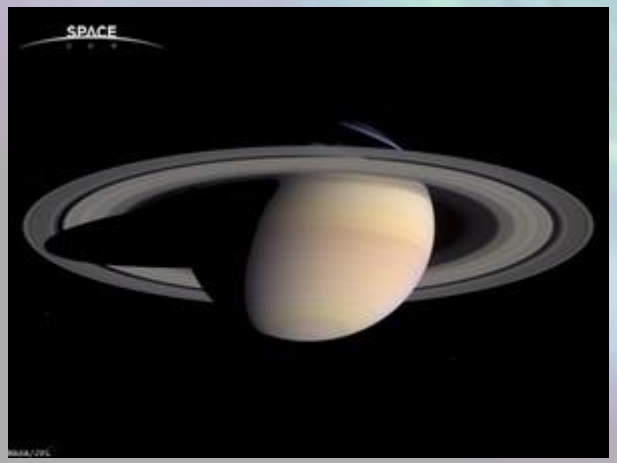
The rest of this presentation will describe practical steps the individual can take to protect their information and communications from cyber-attack, and thereby heighten their security and privacy

The practical steps are in two categories:

- **Hardening – Steps to make your computer-based information resistant to theft, compromise**

- **Methods and Strategies – To make your communications and Web activity resistant to eavesdropping**

Systems Hardening



Tip 1 – Have good anti-malware, keep it current, run it often

- as noted above, 50% of cyber attacks involve malware
- much malware today has the goal of stealing user files and private information such as SSN and credit-card accounts
- although anti-malware software is not perfect, if kept current and run regularly it can provide significant protection
- there are many types of anti-malware software – ranging from simple scanners (often free) to complete suites with real-time and Web protection (often require subscription)

Systems Hardening

Special note for mobile devices:

- **malware on mobile devices is the hot area today**
- **Android is especially vulnerable, but no device is safe**

- **Do NOT jail-break or root your mobile device!**
- **Obtain good anti-malware software for your device – keep it current and run it often**
- **Only obtain applications from the official app store**
- **Do not enable side-loading**

Systems Hardening

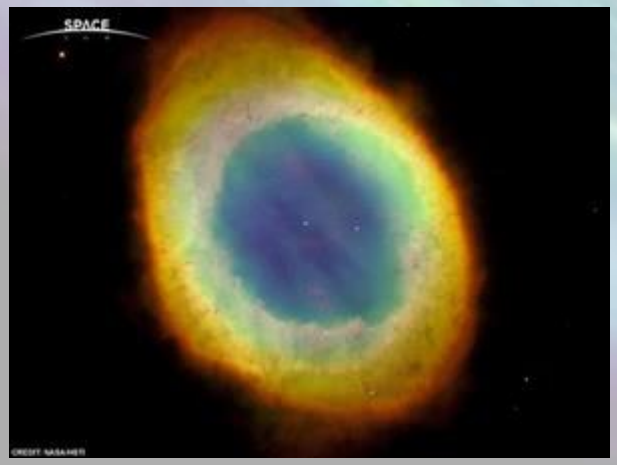
Tip 2 – Have good anti-spyware software, keep it current and run it often

- many anti-malware programs do not scan for spyware (although some do)
- spyware can violate your privacy by recording Web sites you visit, who you communicate with (including contents of communications) and more
- many anti-spyware programs also allow you to manage cookies – short bits of text stored on your computer that preserve information on prior online activity
    - note – many online stores require use of cookies to enable a 'shopping cart'

Systems Hardening

Tip 3 – Have, and properly configure, a good firewall

- most personal computer operating systems come with firewall software installed
    - you only need to enable it (which may be the default setting)
- home cable and DSL modems also provide firewall protection via NAT (network address translation)



Systems Hardening

Tip 4 – Use a Least-Privilege Account (LPA)

- This is when you only use accounts that do NOT have administrator privileges
  - this is because Web sites can inject scripts into your browser – and those scripts execute with the privileges of the current user
- Keep the administrator account separate – only use it when absolutely needed!

- according to Microsoft, 64% of all vulnerabilities during 2009 could have been prevented by use of a LPA

http://www.zdnet.com/blog/security/report-64-of-all-microsoft-vulnerabilities-for-2009-mitigated-by-least-privilege-accounts/5964

Systems Hardening

Tip 5 – Ensure that your OS and Applications have current security patches applied

- OS patches can be automatically installed for Windows and Mac
- Application patches are more problematical
  - in some cases the software checks for patches and alerts the user to download and install them
  - in some cases the patches are automatically installed
  - in some cases it is up to the user to determine if a patch is needed

- vulnerability scanners (such as Secunia PSI) and services (such as CERT) can help

Systems Hardening

Tip 6 – Use encryption for important files in storage

- Encrypted files, folders and devices offer an extra layer of security
  - even if a criminal obtains the file, folder or device, the data will be unavailable to them
- Many programs (some free) exist for file, folder and device encryption
  - do not lose the encryption password
  - do not select a simple encryption password
- many organizations advise full-disk encryption of laptops and other mobile devices, to protect your information in case of loss or theft of the laptop
- of course you can always keep sensitive files on removable media and lock it away when not using it

Systems Hardening

Tip 7 – Protect your home Wi-Fi network

- many users install home Wi-Fi nets with factory settings and no security
  - in 2009 the SRA Club did a war-driving exercise – out of 9,000 networks 1/3 were completely unprotected
- indeed, the trained hacker can easily overcome WEP and WPA (WPA2 is harder)
  - so you may consider also running a VPN – which will be discussed later

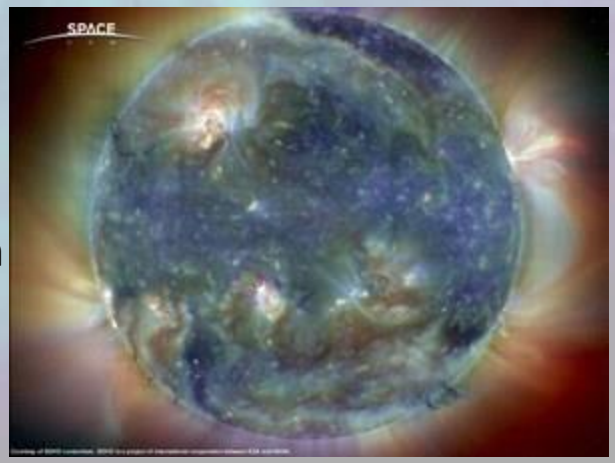
Methods and Strategies

Tip 8 – Use a VPN when in a public hotspot or accessing sensitive services

- makes any ‘man-in-the-middle’ attack much harder

- many organizations provide VPNs for access to internal networks or servers
- personal VPNs are available – encrypt communication from client to VPN host

- using a personal VPN from home will also protect you from man-in-the-middle attacks on your home network



Methods and Strategies

Tip 9 – Use a secure browsing suite, such as TOR or MaskMe

- **web ‘portals’ that mask your IP address by forwarding requests and responses**
- **note that some services like this maintain logs for a short time**
- **some provide additional services such as masked email addresses, temporary inboxes, strong password generation, and iOS and Android support**
- **delete your browsing history!**

Methods and Strategies

Tip 10 – Use a secure search engine, such as DuckDuckGo, Ixquick, or Gigablast

- search engines that do not maintain logs with user IP address (sometimes deleted after a specified time)

- can avoid biased results – search transparency

Methods and Strategies

Tip 11 – Use an encrypted e-mail service

- some security suites (such as Symantec) provide this
- some are free, some require payment
- note – some encrypted e-mail services have shut down recently (Tor Mail, Lavabit and Silent Circle are examples)
- note 2 – use of encryption in e-mail can raise red flags – be careful!

Methods and Strategies

Tip 12 – Never use company networks or computers for personal purposes

- they have every right to use forensics to uncover anything done with their networks or systems
- even if you work from home – use separate computers
- If involved in BYOD – purchase separate systems

Methods and Strategies

Tip 13 – Never reveal personal information online

- **If you do use social networking – such as Facebook – become very familiar with privacy controls and NEVER TRUST THEM!**

- **note that the agreement you sign often gives the provider copyright control over everything you publish**

- **Your birth date and place of birth can often be used to calculate your SSN**

http://arstechnica.com/science/2009/07/social-insecurity-numbers-open-to-hacking/

Methods and Strategies

Tip 14 – If you are asked security questions – lie and remember the lie

- **It is possible to do a bit of research and find out a persons maternal grandmother's name, place of birth of eldest child, etc.**

- **so lie, state that your maternal grandmother was Lucille Ball and then remember the lie**

Methods and Strategies

Tip 15 – Select strong passwords, and never use the same userid/password set for multiple services

- **Strong passwords should be 8 or more characters, and have a mixture of special characters and case**

- **pick an algorithm for password selection – such as the first character of every other word of lyrics of a favorite song – with some special characters.**

“Lady Madonna, children at your feet, wonder how you manage to make ends meet?”

Becomes:

“LMc@yf-whUm2m3m”

Methods and Strategies

Tip 16 – Learn to manage your cookies

- Cookies are text strings stored on your computer – used for shopping carts and directed ads

- add-ons can alert you when cookies are set in your browser

- system cleaners (in next slide) can eliminate unwanted cookies

Methods and Strategies

Tip 17 – Use a system cleaner

- system cleaners (such as Ccleaner) remove tracks from programs you run, erase temporary files, empty the recycle bin, and clean your Registry

- frequent use of system cleaners can also help to speed up computers that are performing slowly

Methods and Strategies

Tip 17 – Use a secure file eraser

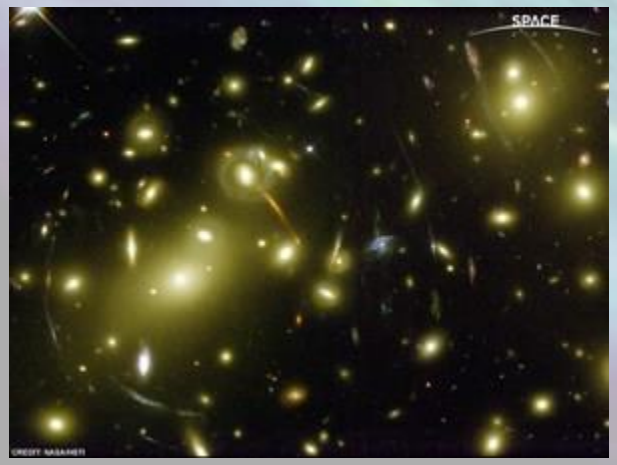
- **secure file erasers overwrite deleted files multiple times to prevent forensic discovery**

Methods and Strategies

Tip 18 – Keep a 'clean' e-mail addess

- **this is a separate e-mail address that you can use when posting to newsgroups, mailing lists, chat rooms, etc.**

- **it is separate from your preferred e-mail address**



Methods and Strategies

Tip 19 – Be aware of social engineering attacks

- **beware of any e-mail or Web site that offers a reward or prize for contact information or other personal details**
- **if an offer appears too good to be true it is!**
- **do not reply to spammers – ever!**
- **seek confirmation**
- **do not follow links sent to you in email – even if they appear to be from a friend**
- **if you want to send a link to a friend – include information only they would know – possibly send a second e-mail explaining why you sent the link**

Methods and Strategies

Tip 20 – Keep children safe online

- children could innocently give away private information
- use a protection program such as ‘net-nanny’
- have clear rules for when children may go online and what they may do
- keep a family computer in a public area (like a family room) and monitor their usage
- if you give a child a cell phone consider a limited phone such as jitterbug

Summary

Online security is each person's responsibility!

Do not count on technical solutions – exercise judgment and caution.

Do not break the law!

Questions?