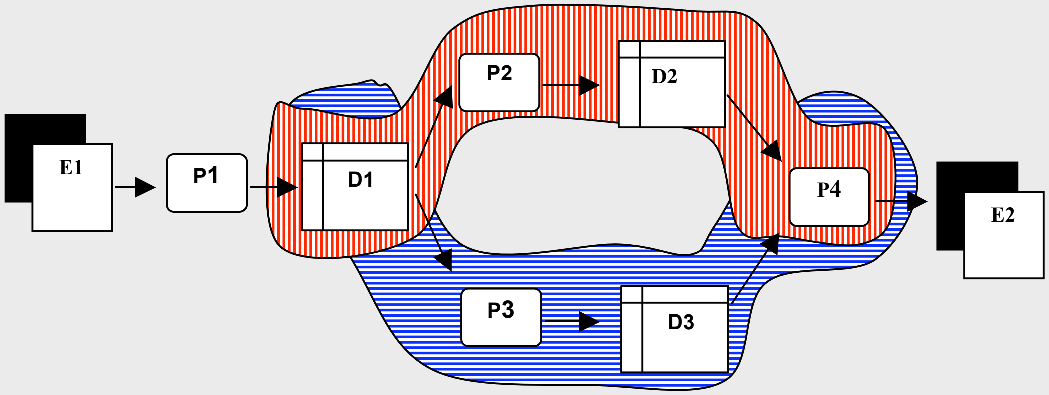
Personal Data Privacy and Information Security in Today's Digital World



Tom Ferrin, Ph.D.

Depts. of Pharmaceutical Chemistry and Biopharmaceutical Sciences
Resource for Biocomputing, Visualization, and Informatics
University of California at San Francisco

UCSF

Outline

- The digital world today
- Authentication - are you are who you say you are?
- Public key cryptography
- Passwords, passwords, everywhere passwords
- Malware and you
- Where to learn more

Intended Audience

This presentation focuses on data privacy and information security awareness for individuals and ways YOU can make your digital world a safer place.

Why focus on individuals?

Because if you are knowledgeable about information security it benefits both you and the University!

Today's Digital World can be mean, tough, and unforgiving!

Internet phishing scams

Trojan Horse malware

Destructive viruses

Deceptive Web sites that collect personal data or install malicious software

Insecure computer systems containing personal data

Open computer networks that are easily snooped

Identity fraud

Spyware

And on and on…

How Are Institutions Responding?

Organizational Practices:

- Creation of security and confidentially policies
- Creation of security and confidentiality committees
- Hiring information security officer
- Conducting education and training programs
- Imposing sanctions for violations
- Improving authorization forms

Technical Practices and Procedures:

- Individual authentication of all users
- Per-user access controls
- Audit trails (user accountability)
- Physical security and disaster recovery
- Protection of external electronic communication (encryption)
- Protection of remote access points (network firewalls)
- Protection from malicious software (malware)
- Authentication of data records
- Single sign-on
- Ongoing system vulnerability assessment

How Are Individuals Responding?

Outside of the institutional setting, most individuals are pretty much doing....

Nothing!

What can individuals do?

- Raise you awareness level and educate yourself about information security

- Take advantage of existing technology to improve your secure digital environment

- Get into the habit of always practicing safe information security

Authentication - Are you who you say you are?

Authentication can be based on one or more of:

- Something you know (e.g. a password or pin)
- Something you have (e.g. a "token" such as an ID card)
- Some physical attribute or "biometric" (e.g. fingerprint, retinal pattern, handwriting, voice identification, face recognition)

Potential problems:

- Someone else can know the same thing (e.g. shared or stolen password)
- Someone else can have the same thing (e.g. shared or stolen ID card)
- Someone else can masquerade as you (e.g. steal and then use the digital version of your fingerprint after the measurement is taken)

Improved Authentication using Dynamic Tokens

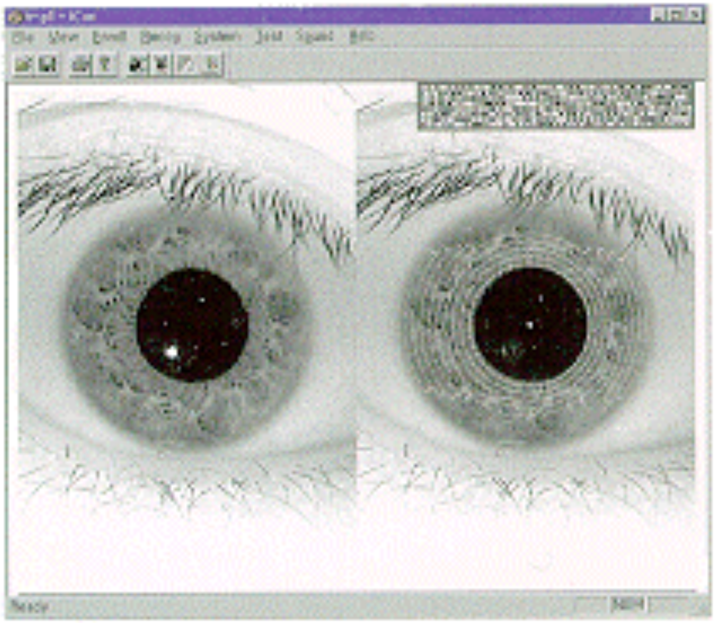
Pretty Good Authentication Example

Use password and dynamic token:

- Session #1 at 10:05am on 10/26/2005:
  - login: tef
  - password: mysecret
  - token: 032848
- Session #2 at 12:16pm on 10/26/2005:
  - login: tef
  - password: mysecret
  - token: 314159

Biometric Identification

- Fingerprints
- Palmprints
- Voiceprints
- Iris or retina scans
- Behavioral factors such as the way you sign your name (e.g. speed, path, & pressure of your hand stroke)



(Note that identification needs to be based on phenotypic features, not genotypic, since ~1% of the population has an identical twin.)

Note that once a biometric is stolen, you can't just get a new one issued.

Public Key Cryptography (PKC)

A method for two parties to communicate privately without pre-arrangement and over a communications link that may be monitored by a hostile third party.

- Based on the premise that a message can be encrypted with one key and decrypted with another (there are several algorithms to do this)
- Requires that the parties agree on the algorithm to use for encrypting messages and two “keys”, one private and the other public
- Each user publishes his/her public key in some easily accessible place (e.g. on their web site) for the other party to see, while closely guarding the secrecy of their private key
- Useful approach both for transmitting secure documents and for providing digital signatures

Some Uses of PKC Technology

Secure (encrypted) transactions on the world wide web

- The “s” in https://

Verifiable identities of computers on a network

- Digital certificates

Secure telephone calls

- Motorola’s Sectera system

Secure network transactions

- Virtual Private Network software and Novell’s NetWare

PKC and You

Make sure you are using a secure (and trusted) Web server (https://) whenever you provide sensitive information

Download and use VPN software whenever you can

- Especially you are accessing sensitive data via a public network (wireless or DSL).
- See the ITS/Enterprise Network Services web site for additional instructions and free software: http://its.ucsf.edu/information/network/vpn/

What About Passwords?

Traditional authentication relies on passwords…

And passwords are notoriously easy to steal or “guess”

- Passwords need to be easy for a human to remember
  - But if it’s easy to remember, then it’s probably also easy to guess.
  - If it’s a word in a dictionary, then it’s susceptible to a “dictionary attack”
- Typical passwords are not longer than 6 or 7 characters
  - Even a slow computer can try every possible combination of alphanumeric passwords in ~50 hours, and every possible keystroke password in ~500 hours.
- If a password is not easy to remember, then the user probably will write it down
  - …like on a Post-it note that they stick on their monitor!

More on Passwords

People tend to re-use the same password for different applications.

Here's an approach that has been shown to be quite effective at collecting user names and passwords:

- Put up a Web site with something interesting on it: porn, baseball scores, stock tips; whatever will attract the demographic you're after
- Don't charge for it, but require that people register with a username and password
- Collect these – chances are good that someone will use the same username and password that they already use on another system
- Use this data to break into the target system

Traditionally people tend to share their passwords with others they trust, especially when they need help getting work done.

Tips For Safeguarding Your Digital Life

Create Strong Passwords:

- Don't use easy-to-guess passwords such as "password," "1234," your user name or any word that appears in a dictionary.
- Don't use your pet's name, street address, date of birth, mother's maiden name, or nickname.
- Combine numerals and letters. Use uppercase and lowercase along with special characters such as the exclamation point.
- Create longer passwords for the most sensitive sites. For example, consider 16 characters for banks.
- Create strings that appear random to others. For instance, think of a phrase like "Mary had a little lamb." Then start your password by using only the last letter of each, as in "ydaeb." Then insert numerals or special characters. Mix it up by making every other letter uppercase.

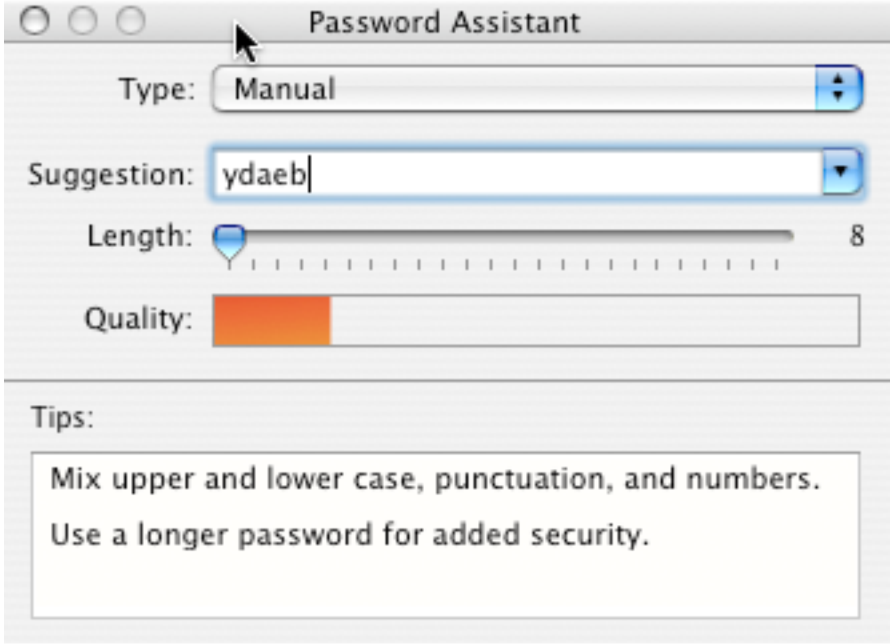
Tips For Safeguarding Your Digital Life

Secure Your Passwords:

- Don't write your passwords on sticky notes attached to your monitor. If you do write them on paper, keep them in a secure place such as wallet or safe.
- Encrypt any computer files you use to store passwords.
- Avoid reusing passwords at different sites. If you must in order to remember them, share passwords only for low-risk uses such as newspaper registrations.
- Change passwords when you have a reminder sent via e-mail. Delete the e-mail immediately.
- Change passwords on a set schedule, such as the first day of spring, summer, etc.
- Guard your e-mail password, as that can be used by others obtain "reminders" for other passwords. Change it after visiting insecure locations like cybercafes.
- Create a system for remembering passwords without having to write them down. For instance, begin with your random-looking string and add a constant you memorize, such as "4!5." End with something related to the Web site you are creating the password for, such as the first four consonants of the domain name.

Mac OS X users take note

Apple added a nifty new feature in Tiger...



Type: Manual

Suggestion: ydaeb

Length: 8

Quality:

Tips:

Mix upper and lower case, punctuation, and numbers.

Use a longer password for added security.

But passwords are used everywhere!

Computer accounts
Bank accounts
Brokerage accounts
Web sites
Credit card companies
On-line shopping
Employee benefit accounts
Secured computer files (e.g. Excel)
ATM machines
IRS accounts
Voice mail
Alarm codes
Digital locks
And many others...

How can you possibly remember separate passwords for each of these?

Do you just write them down and keep the list in your wallet?

Consider keeping an encrypted file of all your passwords on a computer (preferably more than one computer in case the file is lost).

Encrypted Computer Files for Storing Passwords

Encryption technology available today is very good -- often based on the NIST Advanced Encryption Standard (AES) -- it is essentially unbreakable

So therefore it makes good sense to use this technology to protect your passwords

On Windows, try "AxCrypt" file encryption software -- free from Source Forge (http://axcrypt.sourceforge.net/)

On Mac OS X, try the "Secure Notes" feature of the Keychain Access application (Applications->Utilities->Keychain Access)

On a Palm PDA, try STRIP -- Secure Tool for Recording Important Passwords -- free from ZETETIC (http://www.zetetic.net/)

Be sure to use a strong password to encrypt the file!

“Trojan Horse” Software Example

Password authentication program

- Normally prompts a user to provide their username and password, then verifies that the password is correct and, if so, gives user access to the system

- Malware version: Do the same, except also send a copy of the username and password to the bad guys

As a user of this system, you have no idea that anything is amiss!

Therefore, your only protection is to do your best to ensure malware never gets installed on your computer.

Defining Malware

The term **malware** (short for *malicious software*) refers to software explicitly designed to cause damage to a computer workstation, server or network.

Malware is typically classified based upon it's intent and the symptoms/effects it causes, as well as how it's executed and propagates:

- Classifications can often overlap, though, and the distinction between one type of malware and another is not always obvious
- Common classifications include: viruses, trojans, worms, adware, spyware, browser helper objects, keyloggers, browser hijackers,…

The Malware Explosion

Malware originally was most often propagated via floppy disks. In 1999 that changed, and e-mail became the propagation mechanism of choice. The ubiquity of networked computers and e-mail means that malware can infect 10 million or more computers in just a few hours (e.g. ILOVEYOU worm).

Anti-virus software (AVS) is only a partial answer, since new malware can always propagate faster than the anti-virus signature updates and not all types of malware are detected by AVS.† But it's sure a lot better than doing nothing!

† AVS does a pretty good job handling viruses, trojans, and worms.

Protection from Malware

Organizations AND INDIVIDUALS must exercise and enforce strict discipline in their installation and use of software:

- Regularly check for and install any security-related operating system updates
- Install virus-checking programs and keep them updated on all computers (Sophos Anti-Virus available at no cost for use on all UCSF computers. Symantec Antivirus v9 is another good choice.)
- Install network firewalls that limit exposure from outside attackers

Protection from malware is currently the most technically challenging area of computer security.

New Malware Challenges

So, you've installed all the latest OS updates and AV software. Your computer should be pretty safe now, right?

Wrong!

- Adware
- Hijackers
- Toolbars
- KeyLoggers

- Spyware
- Dialers
- Network redirectors
- Browser helper objects

(At least for the time being this new type of malware is primarily targeted PCs and not Macs.)

How does it get on my system?

Bundlers

- Freeware (Weatherbug, WebSearch toolbar, etc)
- Peer-to-Peer applications (Kazaa, eDonkey, Grokster)
- Misleading EULA (end user license agreement)

Drive-By Downloads

- Browsing to a website that “tricks” the user into installing

  “If a user gets tricked into pressing "Yes" once, the user often receives extra web browser toolbars and extra popups, along with programs that transmit information about what web sites the user visits.”

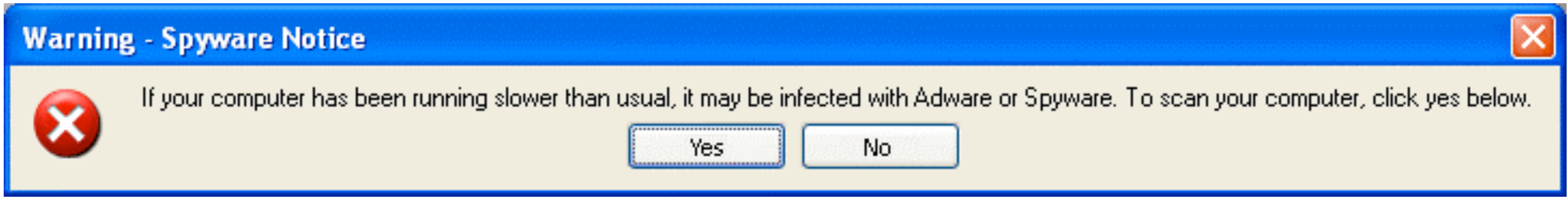
  (source: www.benedelman.org)
- Using security vulnerabilities (e.g., HTML exploit)

Distribution by other malware

E-mail attachment

Drive-By Downloads – a common vector

A common technique of malware installation is a browser pop-up that's disguised as a *Windows* error dialog, advising the user that there's an "infection" already on the computer, and trick him/her into visiting a website that … you guessed it, installs a malicious application…



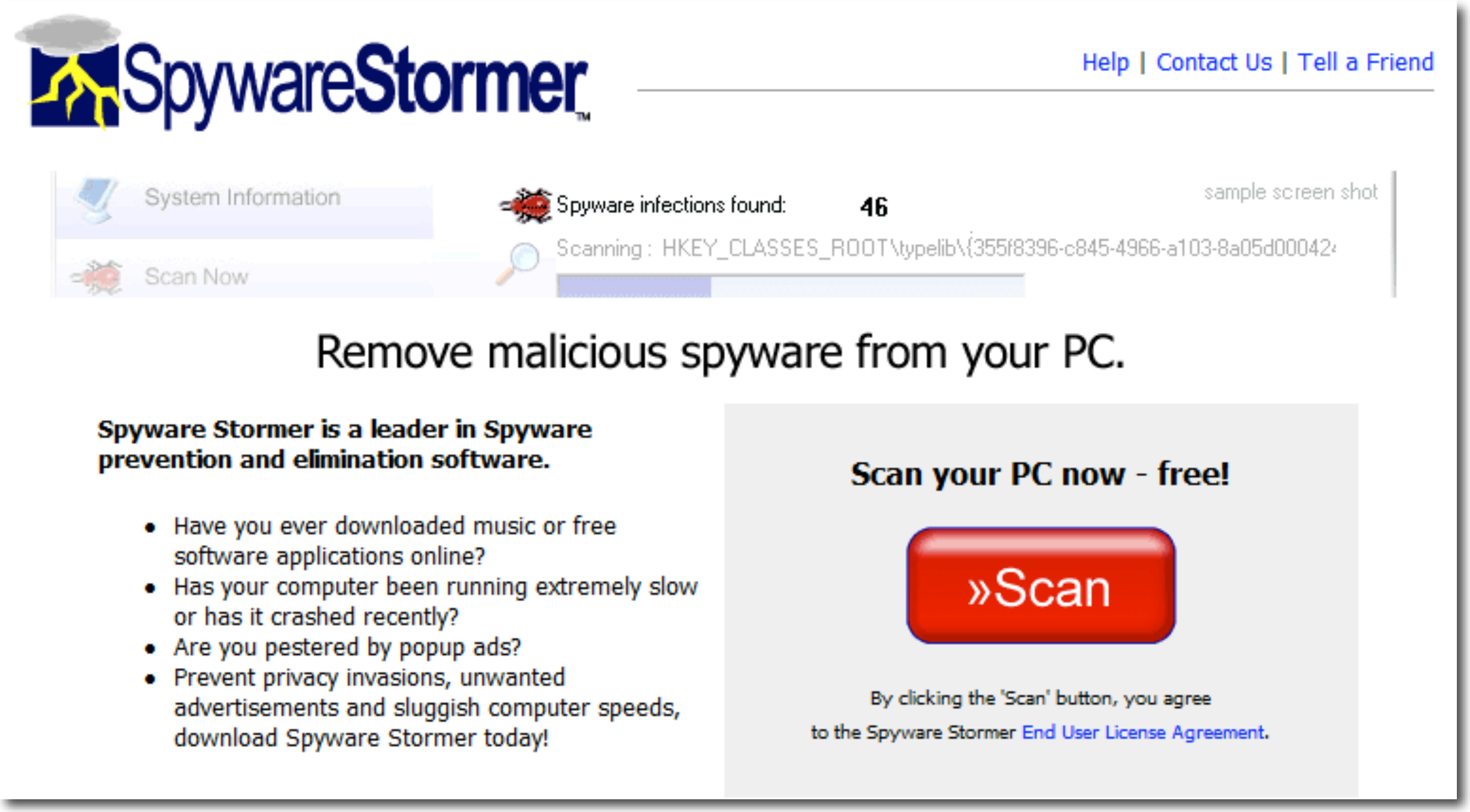
Warning - Spyware Notice

If your computer has been running slower than usual, it may be infected with Adware or Spyware. To scan your computer, click yes below.

This is the <u>only</u> button that is safe to press!

In this case, since the "warning" is a web pop-up, clicking anywhere on the windows except for the red X in the upper right-hand corner – including the NO button! – will cause the user to visit the intended website.

Drive-By Downloads – a common vector



Spyware infections found: 46

Scanning : HKEY_CLASSES_ROOT\typelib\{355f8396-c845-4966-a103-8a05d00042

Remove malicious spyware from your PC.

Spyware Stormer is a leader in Spyware prevention and elimination software.

- Have you ever downloaded music or free software applications online?
- Has your computer been running extremely slow or has it crashed recently?
- Are you pestered by popup ads?
- Prevent privacy invasions, unwanted advertisements and sluggish computer speeds, download Spyware Stormer today!

Scan your PC now - free!

By clicking the 'Scan' button, you agree to the Spyware Stormer End User License Agreement.

This is <u>not</u> the helpful Web site it pretends to be and will actually install spyware on your computer if you let it.

Malware is a Business!

What do Malware creators have to gain?

Adware & spyware creators find it to be a profitable business

- Financial backing from advertisers and VCs
- Personal information extracted can lead to:
  - compromise of financial information
  - compromise of contact information
  - Identity theft

"Investors Supporting Spyware" report

- http://www.benedelman.org/spyware/investors/

McAfee projects that in 2005 these new forms of malware will surpass viruses in both rate of growth and number of examples; malware growth will continue unabated, while viruses level off.

"Potentially Unwanted Programs" by McAfee, Feb 2005

Malware vendors are actively working to create legislation favorable to their "business" methods

What Can You Do?

Malware programs are becoming progressively more complex and intelligent, and as a result are proving to be increasingly difficult to detect and remove!

So <u>prevention</u> is the single best method to avoid malware.

It's pretty much taken for granted these days that a <u>single</u> anti-malware program is not sufficient to remove an infestation.

- Spybot Search & Destroy may find a handful of apps/reg settings/cookies, AdAware will find more,… So standard protocol in malware removal these days is to run <u>multiple</u> (sometimes as many as 3-4!) anti-malware programs.

If you can't/won't do this, at least try out Webroot's highly rated *Spy Sweeper* (http://www.webroot.com/consumer)

Additional Information:

A copy of these slides is available from:
http://www.cgl.ucsf.edu/home/tef/talks/SecurityAwareness.pdf

"Malware: what it is and how to prevent it" by Adam Baratz & Charles McLaughlin. (Available free from http://arstechnica.com/articles/paedia/malware.ars)

"Secrets and Lies – Digital Security in a Networked World" by Bruce Schneier. Wiley Publishing, 2004. (Good bedtime reading)

"Web Security, Privacy & Commerce, Second Edition" by Simson Garfinkel. O'Reilly & Associates, 2001. (Available from http://www.ora.com/catalog/websec2)

Good Web sites:

http://en.wikipedia.org/wiki/Malware

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