

# Windows 7 Security

Jorge Orchilles  
Terremark Worldwide

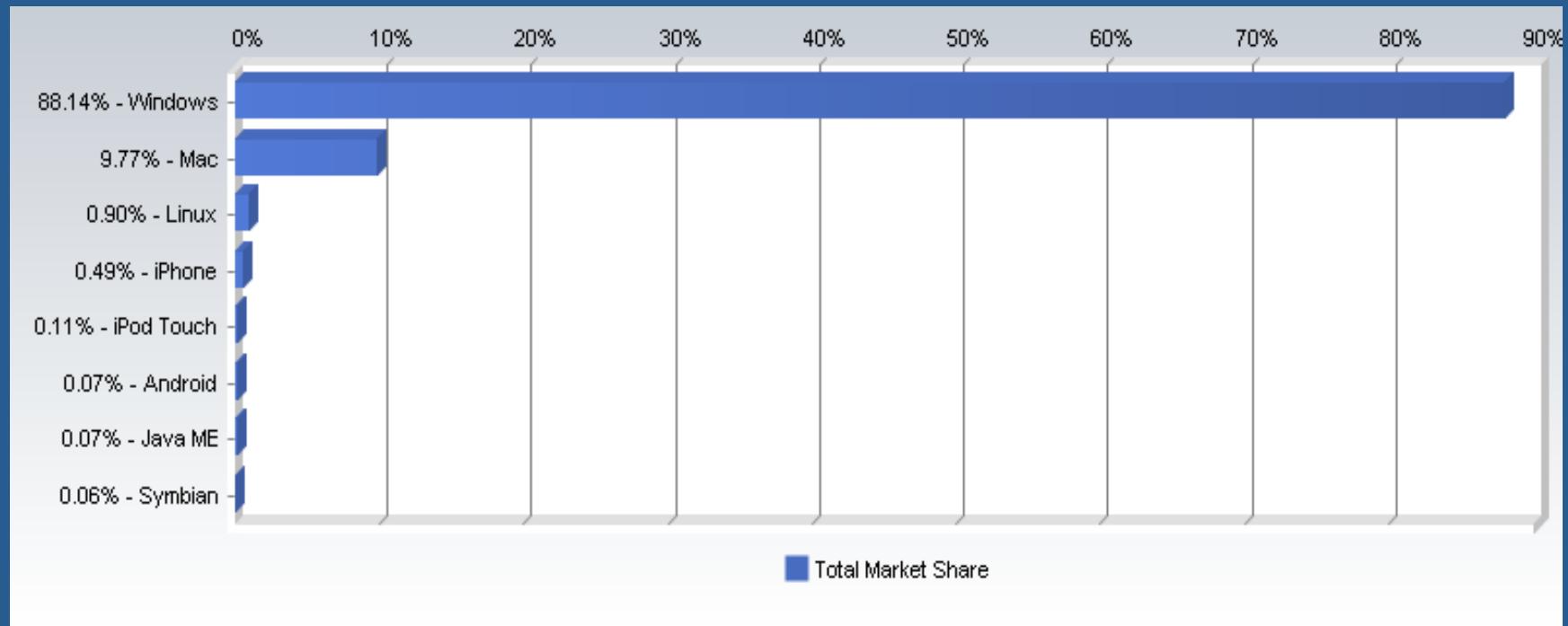
# About Me

- IT Consultant over 7 years ago
- Security Analyst at Terremark
- Master's of Science in Management Information Systems @ FIU
- Author of Microsoft Windows 7 Administrator's Reference, Syngress Publishing
- Few certs: CCDA, CSSDS, MCTS, MCP, Security+

# Audience Survey

- XP Users?
- Vista Users?
- Windows 7 Users?
- Mac OS X?
- Linux/Unix?

# Reality



March 2009 Survey - ComputerWorld

- 88% Windows
- 10% Mac
- 1% Linux

# Reality

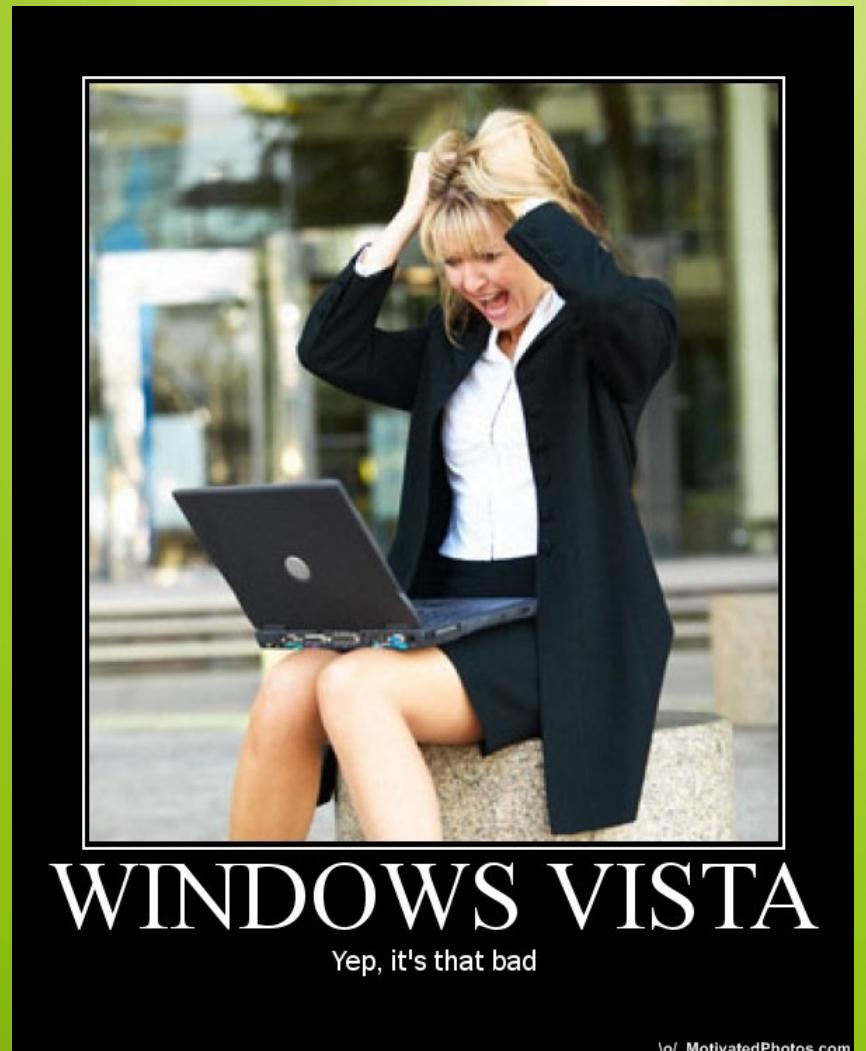
- Up to 94% of corporations skipped Windows Vista
- New PC users had a choice to “downgrade” to XP
- New OEM PCs will include Windows 7 and no choice for Windows Vista or XP for that matter.
- All enterprise systems will be required to upgrade to either Vista or Windows 7 soon! Microsoft is threatening cut off dates already.
- Windows XP is 8 years old!

# Windows Vista

FAIL?

Why?

- Bad Press
- Horrible release



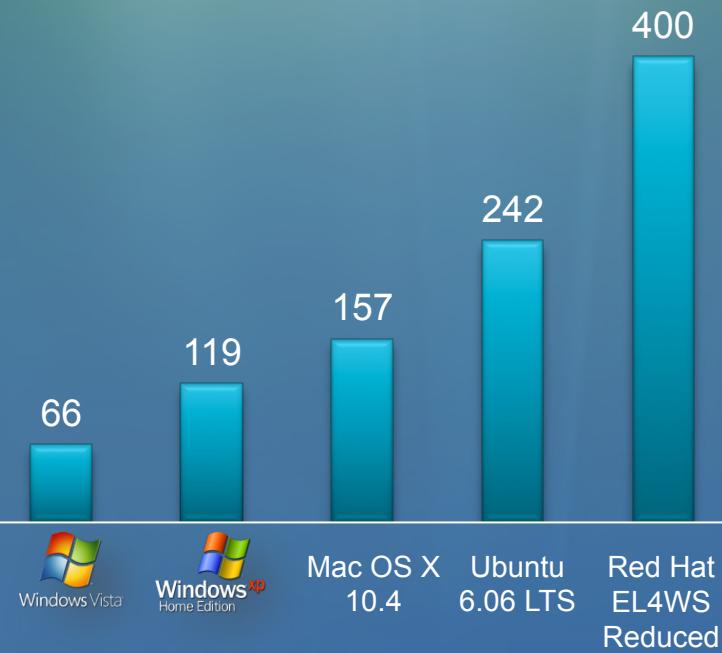
WINDOWS VISTA

Yep, it's that bad

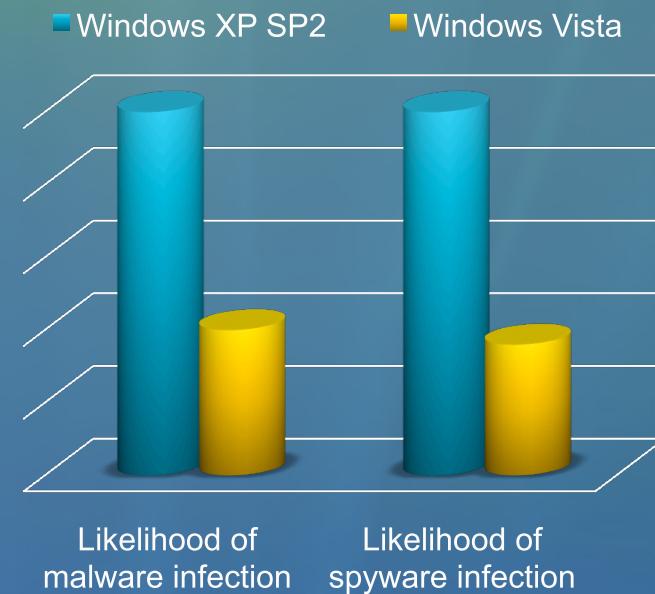
\o/ MotivatedPhotos.com

# Windows Vista - Security Fail? Not so much

## Fewer High Security Vulnerabilities in Year 1



## 60% Fewer Malware Infections Than Windows XP SP2



# Windows Vista - Security Features

- Security Development Lifecycle
- Windows Service Hardening
- Windows Defender
- Internet Explorer 7 w/Phishing Filter
- NG TCP/IP –IPv6, IPSec., WFP
- Vista Firewall – inbound and outbound
- Network Access Protection
- User Account Control – consent and credential prompting
- Code Integrity – all OS DLLS and exec digitally signed
- BitLocker, Encrypted File Systems, & Trusted Platform Module

# Introduction to Windows 7

Incremental update to Windows  
Vista

Uses the same technologies  
already in place with Vista

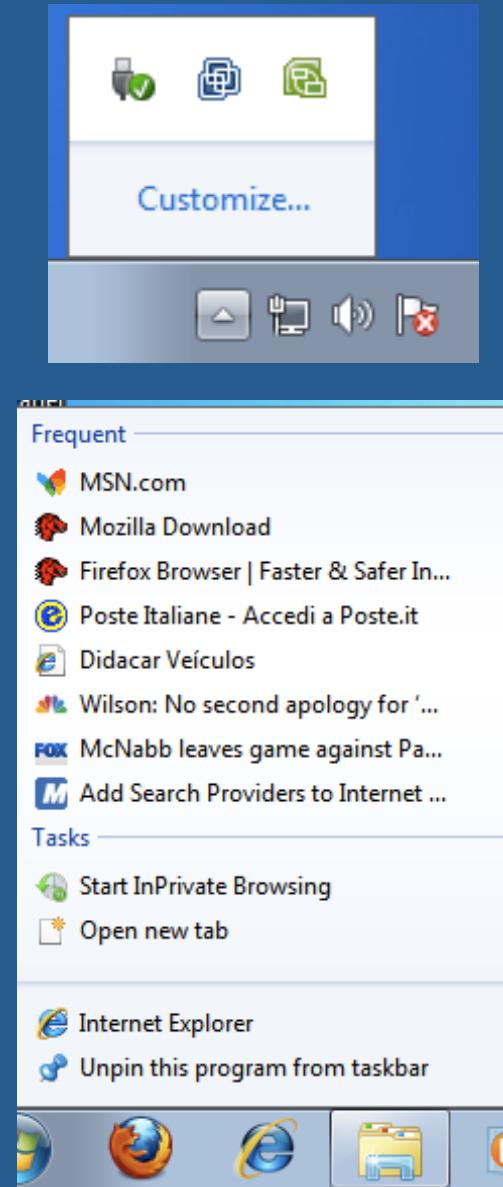
Simpler user interface and  
enhancements to performance

Extensive UAT via public Beta and  
RC



# New Desktop Features

- User Interface
  - Taskbar – Notifications
  - Aero Peak and Aero Snap
  - Jump Lists
- Desktop Search
- Driver and Device Support
- HomeGroup
- Windows Media Player/Center



# Security Features

- Action Center
- Better UAC
- Better BitLocker
- BitLocker ToGo
- Biometric security
- Internet Explorer 8
- AppLocker
- DirectAccess
- PowerShell v2

# Action Center - Security

## Replaces Security Center

- Firewall
- Windows Update
- Virus Protection
- Spyware / other malware
- Internet Security Settings
- User Account Control
- Network Access Protection

[Review recent messages and resolve problems](#)

No issues have been detected by Action Center.

### Security



Network firewall On

Windows Firewall is actively protecting your computer.

Windows Update On

Windows will automatically install updates as they become available.

Virus protection Currently not monitored

[Turn on messages about virus protection](#)

Spyware and unwanted software protection On

Windows Defender is actively protecting your computer.

Internet security settings OK

All Internet security settings are set to their recommended levels.

User Account Control On

UAC will notify when programs try to make changes to the computer.

[Change settings](#)

Network Access Protection Off

Network Access Protection Agent service is not running

[What is Network Access Protection?](#)

[How do I know what security settings are right for my computer?](#)

# Action Center - Maintenance

- Check for solutions to problems
- Backup
- Check for updates
- Troubleshooting
- Recovery

Maintenance

Check for solutions to problem reports      On  
[Check for solutions](#) | [Privacy policy](#) | [Settings](#) | [View reliability history](#)

Backup      Currently not monitored  
[Turn on messages about Windows Backup](#)

Check for updates      No action needed  
Windows Update does not require any action.

Troubleshooting: System Maintenance      No action needed  
Windows is actively checking your system for maintenance problems.  
[Change troubleshooting settings](#)

---

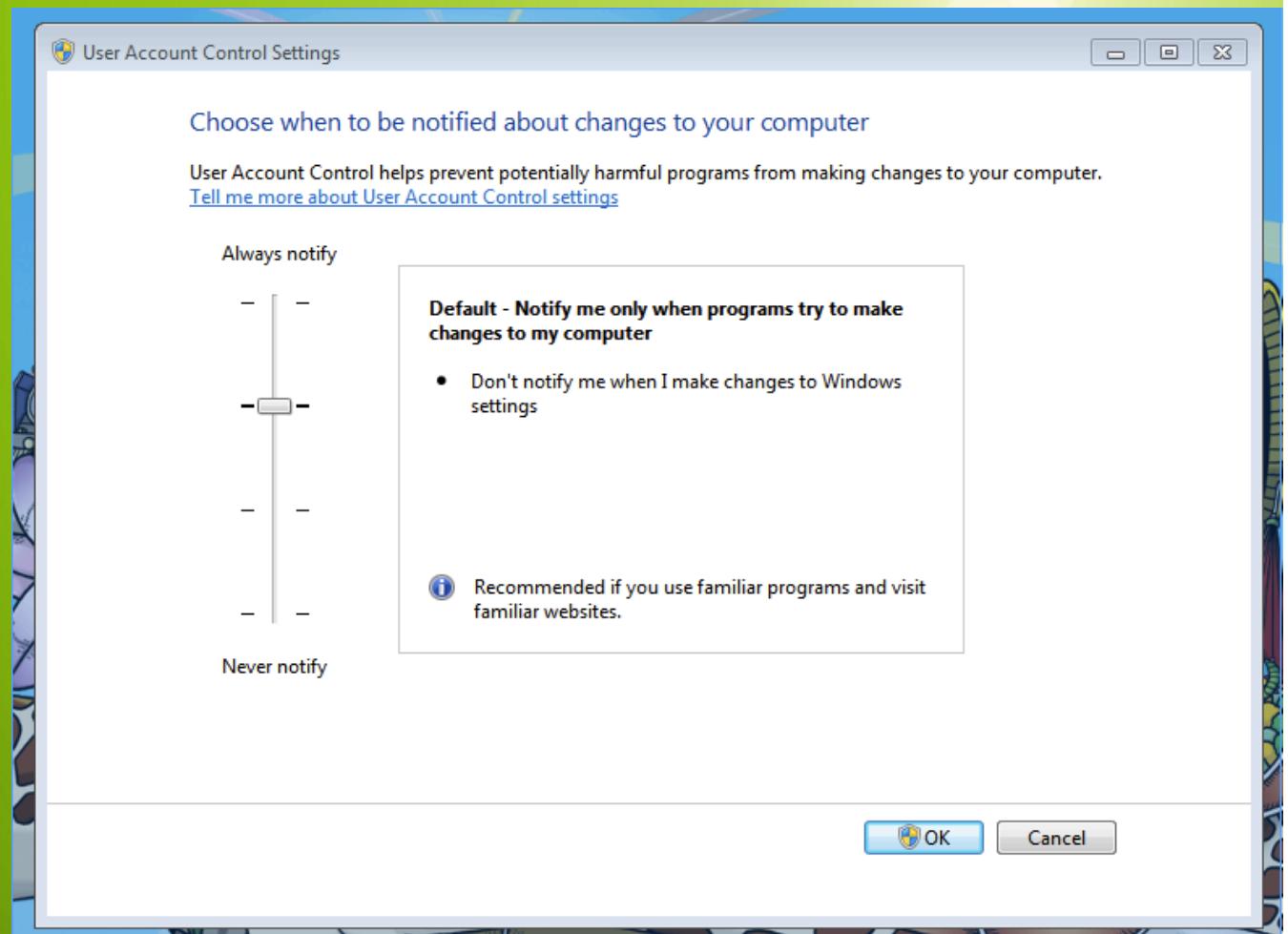
If you don't see your problem listed, try one of these:

 [Troubleshooting](#)  
Find and fix problems

 [Recovery](#)  
Restore your computer to an earlier time

# User Account Control

- Less nagging
- GUI for customizing
- Helpful?



# BitLocker

- Introduced in Windows Vista
- Encrypts the system volume, including the page file and hibernation files
- No need for partitioning!
- Whole drive/volume encryption
  - Trusted Platform Management (TPM) chip or pin/USB key

Help protect your files and folders by encrypting your drives

BitLocker Drive Encryption helps prevent unauthorized access to any files stored on the drives shown below. You are able to use the computer normally, but unauthorized users cannot read or use your files.

[What should I know about BitLocker Drive Encryption before I turn it on?](#)

BitLocker Drive Encryption - Hard Disk Drives



C:

Off

 [Turn On BitLocker](#)



LocalStorage (D):

Off

 [Turn On BitLocker](#)

BitLocker Drive Encryption - BitLocker To Go



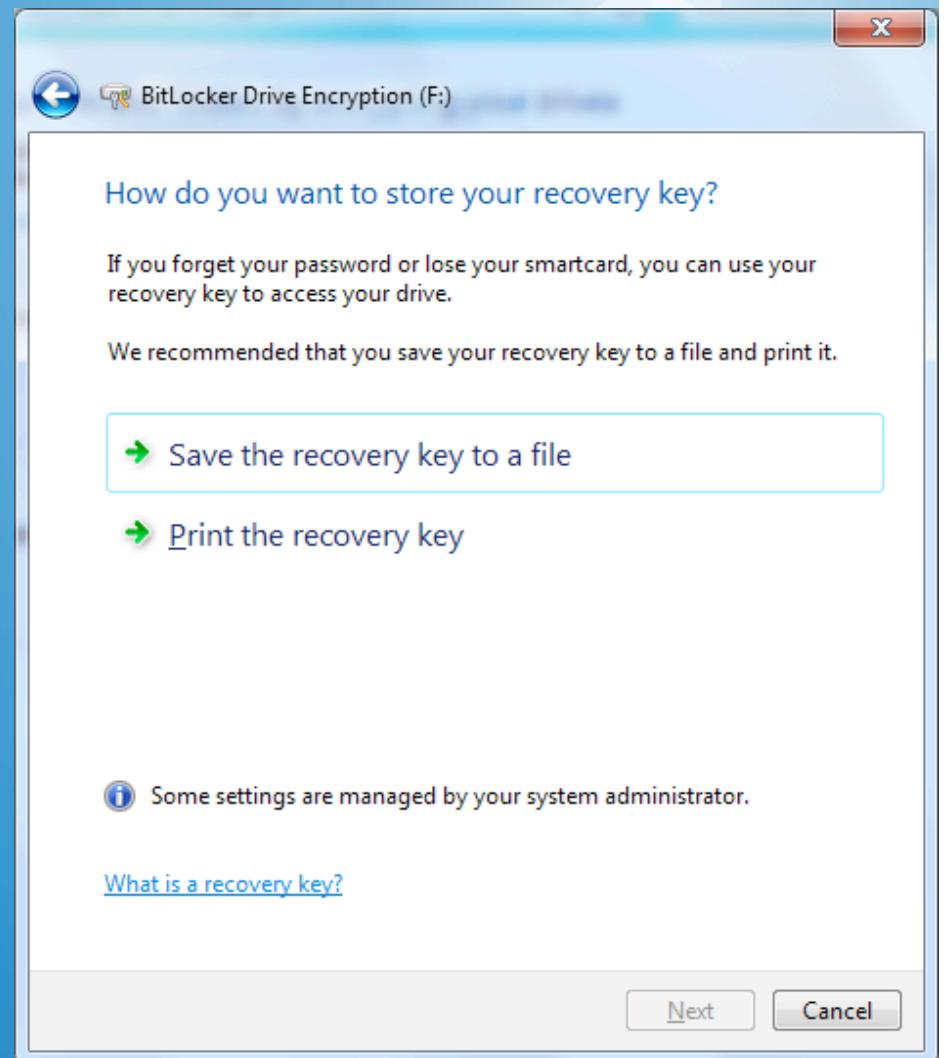
J:

Off

[Turn On BitLocker](#)

# BitLocker – Recovery Key

- All Bitlocker deployments require a copy of the recovery password to be stored somewhere
- Out of the box, your users must save their own recovery password
  - This probably isn't the best idea...

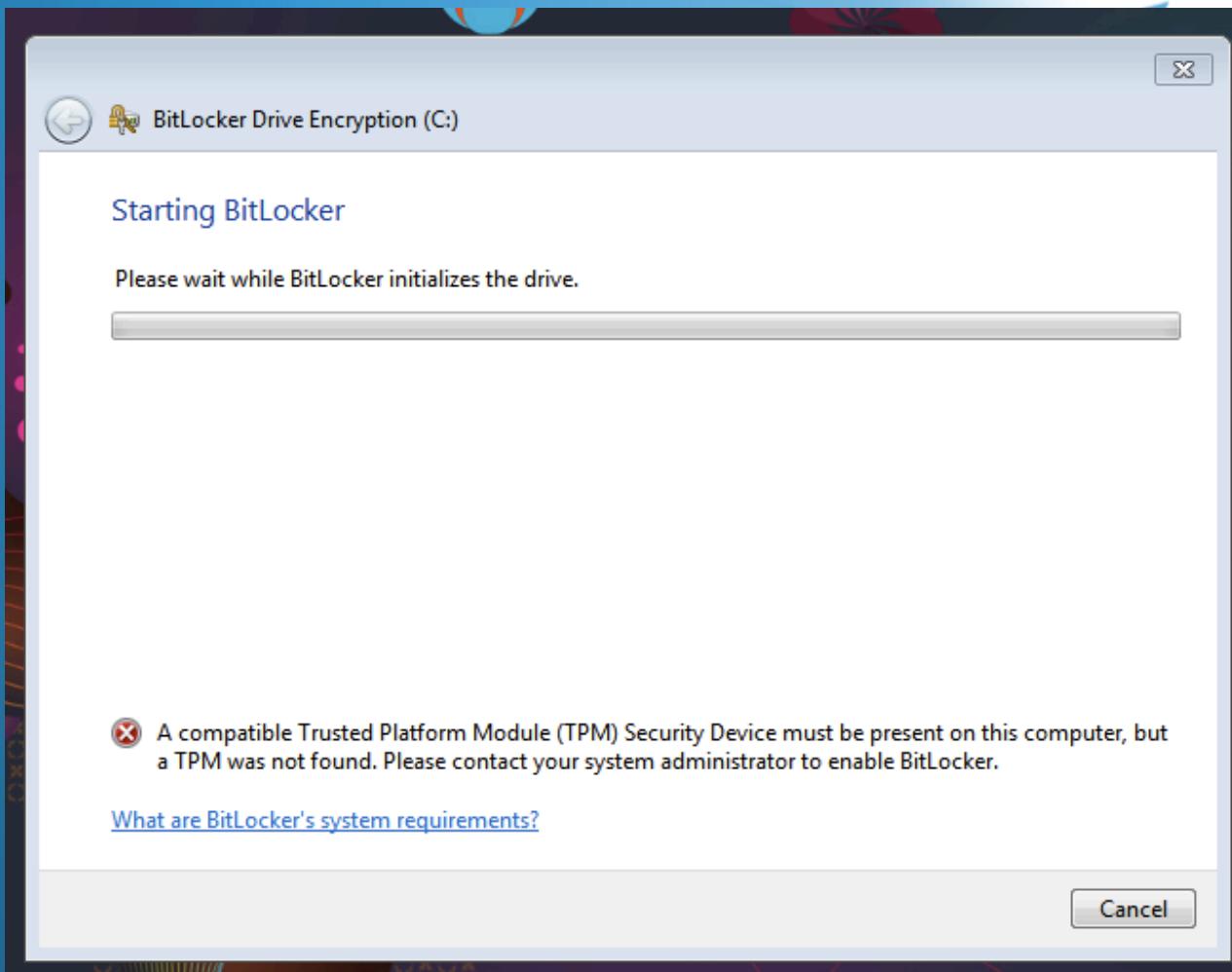


# BitLocker - Issues

- High security environments can require a pin # or USB key before the system will boot
  - Remote systems or servers in datacenter - BEWARE
- BitLocker is *not* a replacement for EFS
  - BitLocker protects the whole drive at boot
  - No protection from user A seeing user B's files post boot
  - EFS solves this problem

# BitLocker - Issues

- Trusted Platform Module required



# BitLocker – Corporate Environment

- Requires Windows Server 2003 SP1 or newer domain controllers
- Group Policy – Require Encryption!
- Universal Recovery Key: Data Recovery Agent
- What about deleted/disabled computer accounts?
  - Sales guy who's always on the road
  - High-powered exec who goes on a 3-month sabbatical

# BitLocker To Go

- Encrypt Removable Media
- Lost USB drive with corporate information?

## Survey: 40% Of Workers Have Lost A USB Stick

Nearly two-thirds also have left a drive unprotected in a PC, BlockMaster reports

**Updated** An Ealing council employee infected the UK local authority's IT systems with the Conficker-D worm after he plugged an infected USB into a work computer, causing tens of thousands of pounds in damages in the process.

<http://bit.ly/iJv4v>  
<http://bit.ly/1zFl3>



# BitLocker To Go - Issues

- Does not work with other OS
  - FAIL
- On Vista and XP you can view content but not edit
  - FAIL
- Password based
  - Recovery file?
  - Brute force?



# Biometric Security

- Options with most new laptops
- Had to use OEM software
- HP Biometric Security – FAIL
- Can login Local or Domain



# Internet Explorer 8

- Can be used on XP and Vista
- Better than IE 6 and 7
- SmartScreen
- XSS Filter
- Data Execution Prevention



# Internet Explorer 8 – Acid Test?

The Acid3 Test - Windows Internet Explorer

http://acid3.acidtests.org/

Favorites The Acid3 Test Page Safety Tools

This website wants to run the following add-on: 'MSXML 3.0 SP11' from 'Microsoft Corporation'. If you trust the website and the add-on and want to allow it to run, click here...

FAIL

**Acid3**

**20/100**

**LINKTEST FAILED**

To pass the test, a browser must use its default settings, the animation has to be smooth, the score has to end on 100/100, and the final page has to look exactly, pixel for pixel, like [this reference rendering](#).

Internet | Protected Mode: On

100% Done

9:59 AM 9/5/2009

The Acid3 Test - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://acid3.acidtests.org/ ows 7 biometric

The Acid3 Test

**Acid3**

**93/100**

To pass the test, a browser must use its default settings, the animation has to be smooth, the score has to end on 100/100, and the final page has to look exactly, pixel for pixel, like [this reference rendering](#).

Done

9:59 AM 9/5/2009

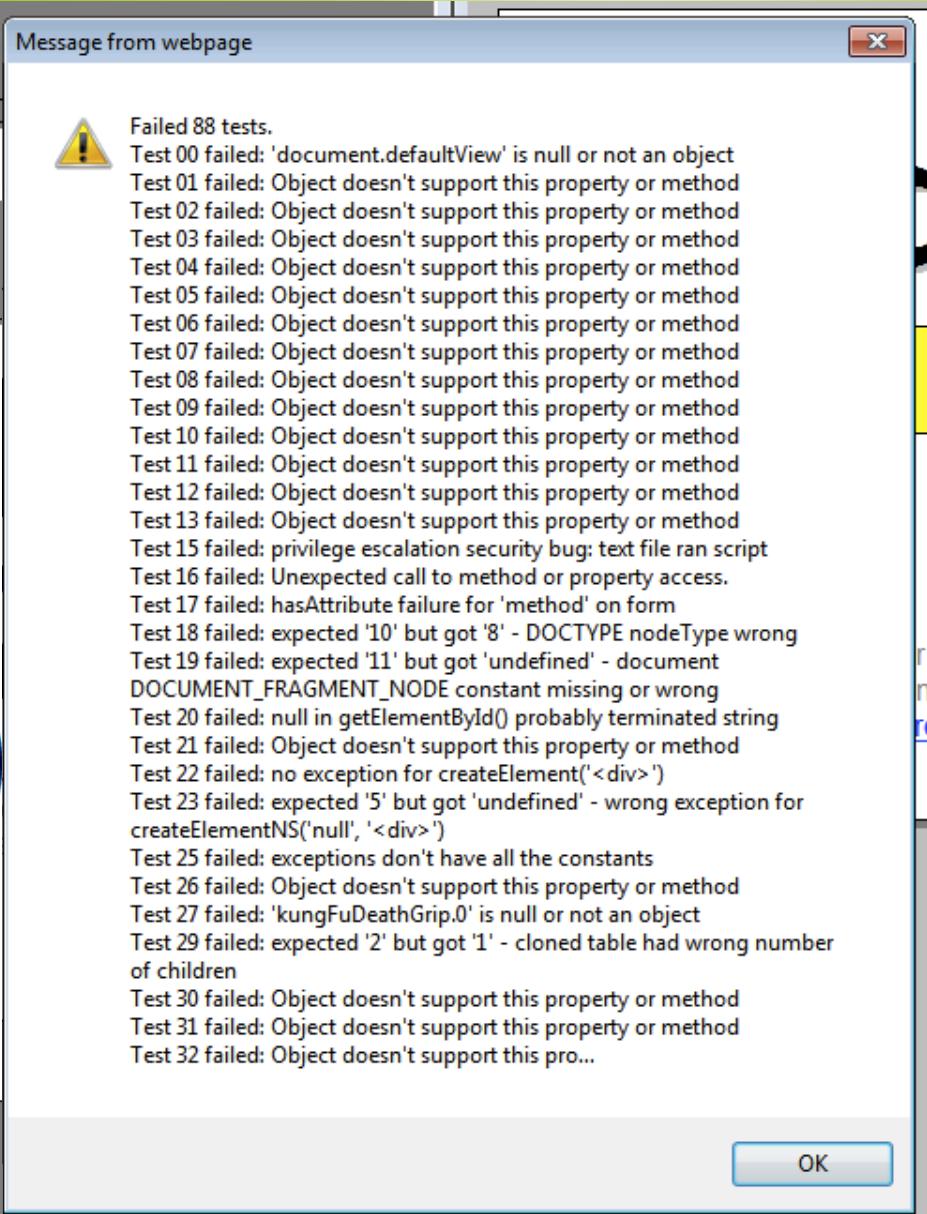
# Internet Explorer 8 – Acid Test?

FAIL

12/100

LINKTEST FAILED

To pass the test, a browser must use its default settings, the animation has to be smooth, the score has to end on 100/100, and the final page has to look exactly, pixel for pixel, like [this reference rendering](#).



# Internet Explorer 8 – SmartScreen?

Poste Italiane - Accedi a Poste.it - Windows Internet Explorer

http://72.46.238.205/PosteItaliane/Poste.it

Favorites Suggested Sites Web Slice Gallery

Poste Italiane - Accedi a Poste.it

Posteitaliane

Home Chi siamo Sala stampa English MyPoste Privati Es

DI COSA HAI BISOGNO? PRODOTTI BUSINESS

Servizi online

Scopri i servizi online Negozi online Registrazione Accedi ai servizi online Codice di attivazione Utenti pre-registrati Hai dimenticato la password? Privacy Sicurezza dei dati

Accedi a Poste.it

Per poter usufruire dei servizi online di Poste.it occorre prima identificarsi. Inserisci negli appositi spazi il tuo nome utente e la password.

Privati Business

Servizi on line Privati

Nome utente  Password  Accedi

Per utilizzare i servizi online e in caso di accesso o non funzionamento dei servizi necessario:

- ⇨ verificare il corretto inserimento del nome utente e della password. Il nome utente va inserito come nome.cognome più l'eventuale es (mario.rossi-1234) richiesta dura registrazione.
- La password va inserita rispettando una sequenza di caratteri maiuscolo come inseriti in fase di registrazione dell'ultimo cambio.
- ⇨ verificare che il browser consenta connessioni con protocollo SSL e cookie della sessione;
- ⇨ eseguire periodicamente la pulizia dei temporanei e dei cookie;
- ⇨ verificare le proprietà data/ora e fu del computer.

Qualora i problemi persistano è possibile contattare il Call Center al numero verde 803.160 (dal lunedì al sabato dalle ore 8.00 alle 20.00) effettuando la scelta "3" per Internet. In alternativa può inviare un email a info@poste.it indicando il suo nome e un recapito telefonico e la fascia oraria per essere contattato.

Al momento del contatto telefonico è consigliabile avere il computer collegato a Internet e avere disponizione il codice di attivazione (ritrasmesso via telegramma) o il codice di controllo (rilasciato al momento della registrazione).

Contattaci Privacy Mappa Trasparenza bancaria Forniture e gare Scadenzario fiscale © Poste Italiane 2009

Internet Protected Mode: On

100% Done

Windows Internet Explorer Mozilla Firefox

Reported Web Forgery! - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://72.46.238.205/PosteItaliane/Poste.it

Most Visited Getting Started Latest Headlines

Reported Web Forgery!

Reported Web Forgery!

This web site at 72.46.238.205 has been reported as a web forgery and has been blocked based on your security preferences.

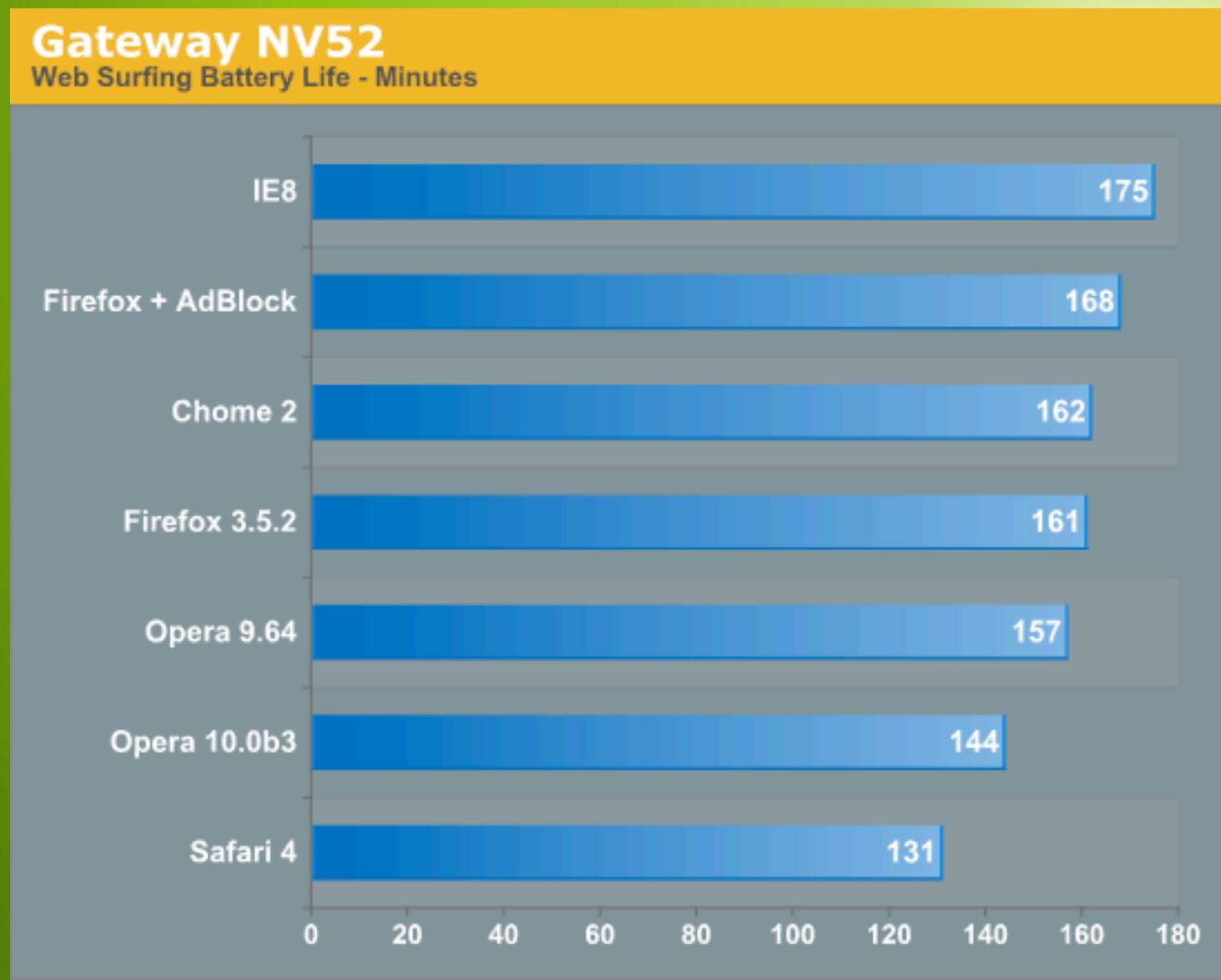
Web forgeries are designed to trick you into revealing personal or financial information by imitating sources you may trust.

Entering any information on this web page may result in identity theft or other fraud.

Get me out of here! Why was this site blocked? Ignore this warning

10:35 AM 9/14/2009

# Internet Explorer 8 – FTW?



<http://bit.ly/17KT8I>

# XP Mode

- XP remains App standard
- Makes it easy to be compatible
- Don't forget to secure this VM!



# With Server 2008 R2

*Windows 7 with Microsoft Windows  
Server 2008 R2 features:*

- AppLocker
  - Application White Listing
  - Enforce App Standardization
- Branchcache
  - Caches files from WAN
- DirectAccess
  - No need for VPN
  - Easier for administration
  - Uses SSL, IPv6, IPSec
- Federated Search
  - Search all assets including SharePoint

# Management

- PowerShell v2
  - IIS
  - Exchange
  - Cmdlets
  - Remote Management
- Enhanced Group Policy

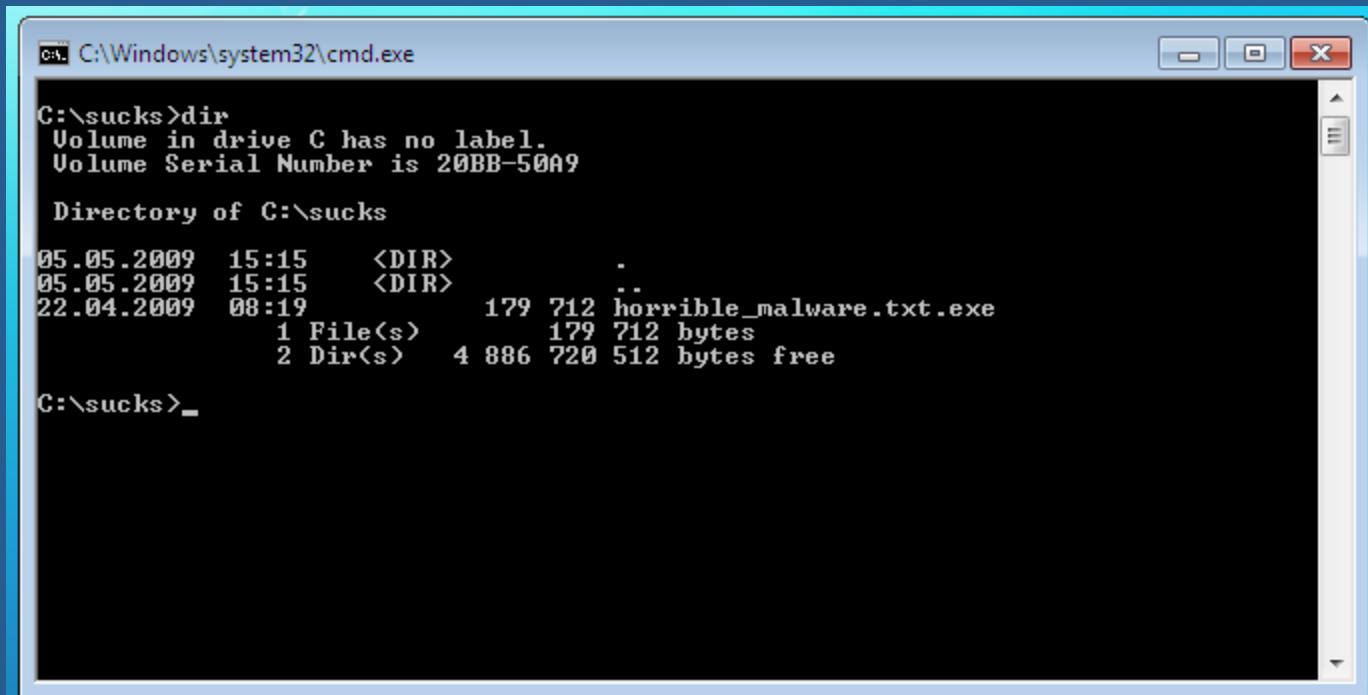
# Secure?

- So far yes!
- September Patch Tuesday
  - None for Windows 7
- SMB2 0day?
  - Does not affect Windows 7 final

**Windows 7 Unaffected By Zero-Day Flaw**

<http://bit.ly/10ffcx>

# Hide extensions for known file types

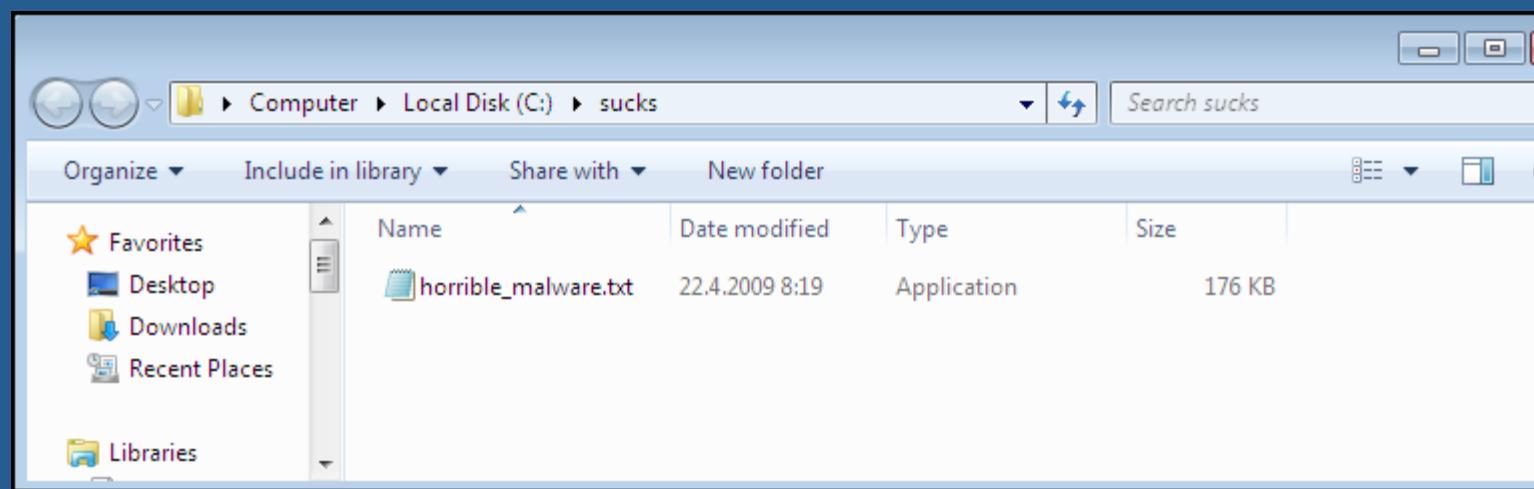


```
C:\Windows\system32\cmd.exe
C:\sucks>dir
 Volume in drive C has no label.
 Volume Serial Number is 20BB-50A9

 Directory of C:\sucks

05.05.2009  15:15    <DIR>      .
05.05.2009  15:15    <DIR>      ..
22.04.2009  08:19           179 712 horrible_malware.txt.exe
                  1 File(s)     179 712 bytes
                  2 Dir(s)   4 886 720 512 bytes free

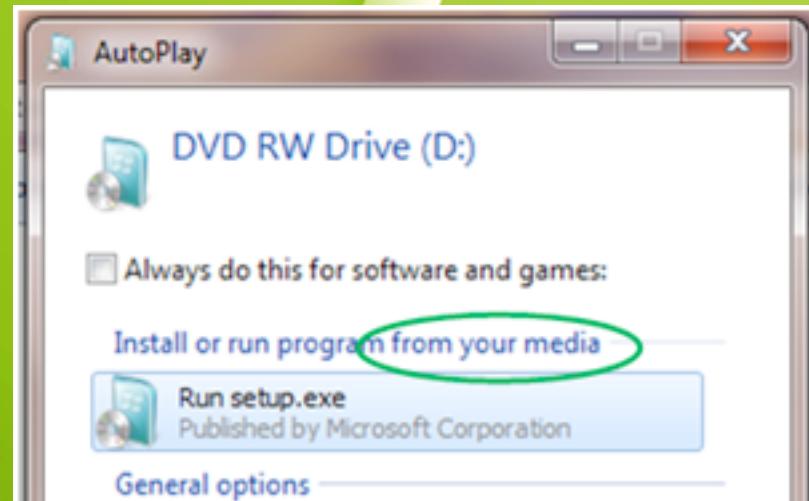
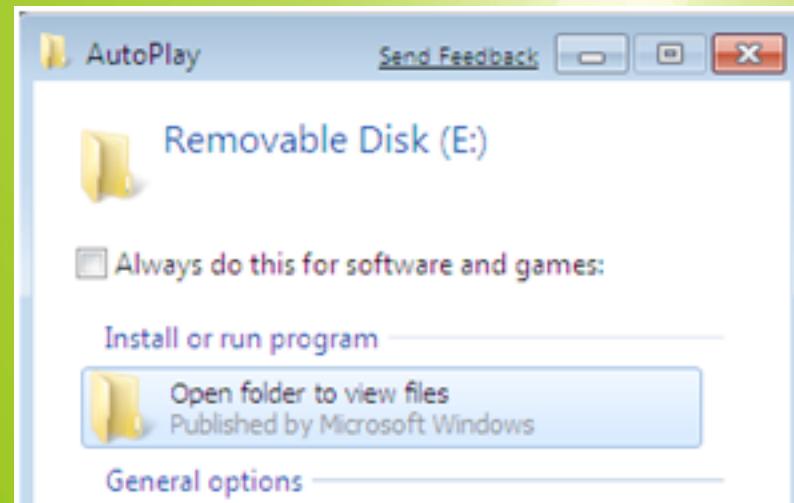
C:\sucks>_
```



# AutoRun

- No longer AutoRun/AutoPlay with non-optical media
- Easier to distribute CD's than Flash Drives!
- Patch available for past OS

<http://support.microsoft.com/kb/971029>



# Easy upgrade path?

Upgrade TO:



Upgrade FROM :

		32-bit	64-bit	32-bit	64-bit	32-bit	64-bit
Windows® XP*		Custom Install					
	32-bit	Custom Install					
Windows Vista® Starter	64-bit	Custom Install					
	32-bit	In-Place Upgrade	Custom Install	Custom Install	Custom Install	In-Place Upgrade	Custom Install
Windows Vista® Home Basic	64-bit	Custom Install	In-Place Upgrade	Custom Install	Custom Install	Custom Install	In-Place Upgrade
	32-bit	In-Place Upgrade	Custom Install	Custom Install	Custom Install	In-Place Upgrade	Custom Install
Windows Vista® Home Premium	64-bit	Custom Install	In-Place Upgrade	Custom Install	Custom Install	Custom Install	In-Place Upgrade
	32-bit	Custom Install	Custom Install	In-Place Upgrade	Custom Install	In-Place Upgrade	Custom Install
Windows Vista® Business	64-bit	Custom Install	Custom Install	Custom Install	In-Place Upgrade	Custom Install	In-Place Upgrade
	32-bit	Custom Install	Custom Install	In-Place Upgrade	Custom Install	In-Place Upgrade	Custom Install
Windows Vista® Ultimate	64-bit	Custom Install	In-Place Upgrade				

Note: To do an In-place upgrade on either a 32-bit or 64-bit system, please ensure that your PC has either Windows Vista Service Pack 1 (SP1) or Service Pack 2 (SP2) installed first.

# Upgrade can take a full day!

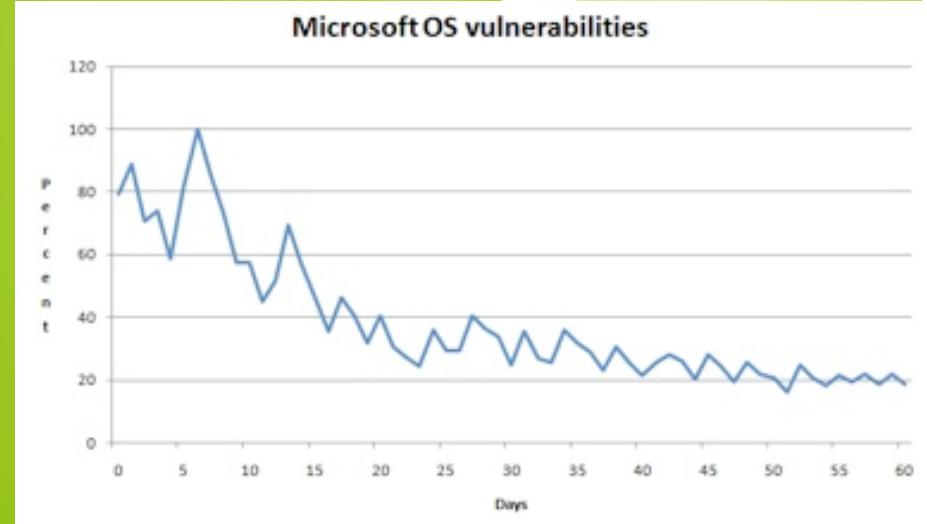
Data Profile	Low End Hardware	Mid End Hardware	High End Hardware
<b>Clean</b> No data and 0 applications	32-bit: 40 minutes 64-bit: 50 minutes	32-bit: 30 minutes 64-bit: 35 minutes	32-bit: 30 minutes 64-bit: 35 minutes
<b>Medium User</b> 70Gb of data and 20 applications	32-bit: 175 minutes 64-bit: 185 minutes	32-bit: 115 minutes 64-bit: 95 minutes	32-bit: 100 minutes 64-bit: 85 minutes
<b>Heavy User</b> 125Gb of data and 40 applications	32-bit: 345 minutes 64-bit: 355 minutes	32-bit: 185 minutes 64-bit: 165 minutes	32-bit: 160 minutes 64-bit: 150 minutes
<b>Super User</b> 650Gb of data and 40 applications	N/A	32-bit: 1220 minutes 64-bit: 675 minutes	32-bit: 610 minutes 64-bit: 480 minutes

<http://bit.ly/39iiVt>

# Evolve

**Cyber Crime Has Surpassed Illegal Drug Trafficking as a Criminal Moneymaker(1); 1 in 5 Will Become a Victim(2)**

- Cyber Crime is UP!
- Threats have evolved
  - Less platform-centric



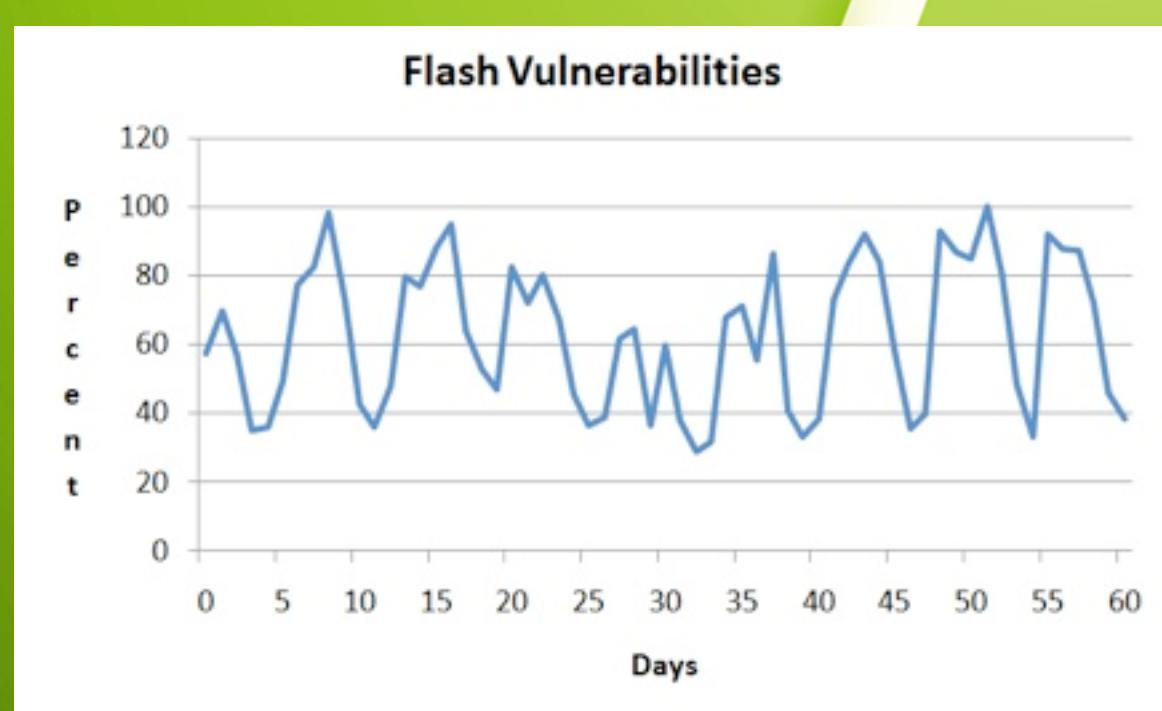
<http://bit.ly/akwRT>

<http://www.sans.org/top-cyber-security-risks/>



# Evolve

- Attack the applications
- Attack the browsers
- Attack the users



# Evolve – Stay Current

- Train Users!
  - Security Awareness
  - Browser Security
  - Windows Training?



# Recap

- If you run Windows now, you will be on 7 eventually
- Secure it!
  - Educate Users
  - Use BitLocker or FDE
  - Patch Everything
  - Use AntiMalware
  - Use Firefox
    - no script - <http://noscript.net/>
    - WOT - <http://www.mywot.com/>

# Recap

- Carefully plan migration from XP to 7
- Train users:
  - Security Awareness
  - Browser Use
  - Windows 7 training

# Questions?

## Thank You

Email: jorgeao@gmail.com

Blog: <http://www.orchilles.com>

[http://www.twitter.com/  
jorgeorchilles](http://www.twitter.com/jorgeorchilles)

