Patrick Gray
Principal Security Strategist

HACKERS, CRACKERS, BOTS, MALWARE AND WEB 2.0

DATA SECURITY CHALLENGES IN THE ALL TOO PUBLIC AND NOT SO PRIVATE SECTORS

I want you to take home four points

- Understand
- Educate
- Collaborate
- Prepare

It’s a great to be in Blue Ash today, but uh, do you know where your data is right now?

- The confidentiality
- The integrity
- The availability
- It’s hard to protect that which we have no idea as to its whereabouts

So, where is your data today?

- On any device
- Any place
- Any time
- When “aren’t” we working anymore?
- When do we call it a day?
- We don’t, do we?

Today, it's about mobility…

- In the past few years we shifted our lives to the PC and the Internet
- Now, it's all about being mobile
- A PC in your pocket
- Our mobile work force is growing and expanding

Where?

- Where does work happen?
- No longer does business take place solely behind network walls
- The critical work is happening increasingly on social networks, on handheld devices, in the field, and at local cafes

Diminishing Border

- The traditional corporate perimeter, with clearly identifiable boundaries, has diminished
- In its place, a network with limitless potential is rising
- One where agencies, companies, their customers, and their partners demand access to information whenever and wherever they need it

New Considerations

- It is information technology's role to ensure that the appropriate people, using the correct devices, are accessing the proper resources while having a highly secure yet positive user experience within your networks

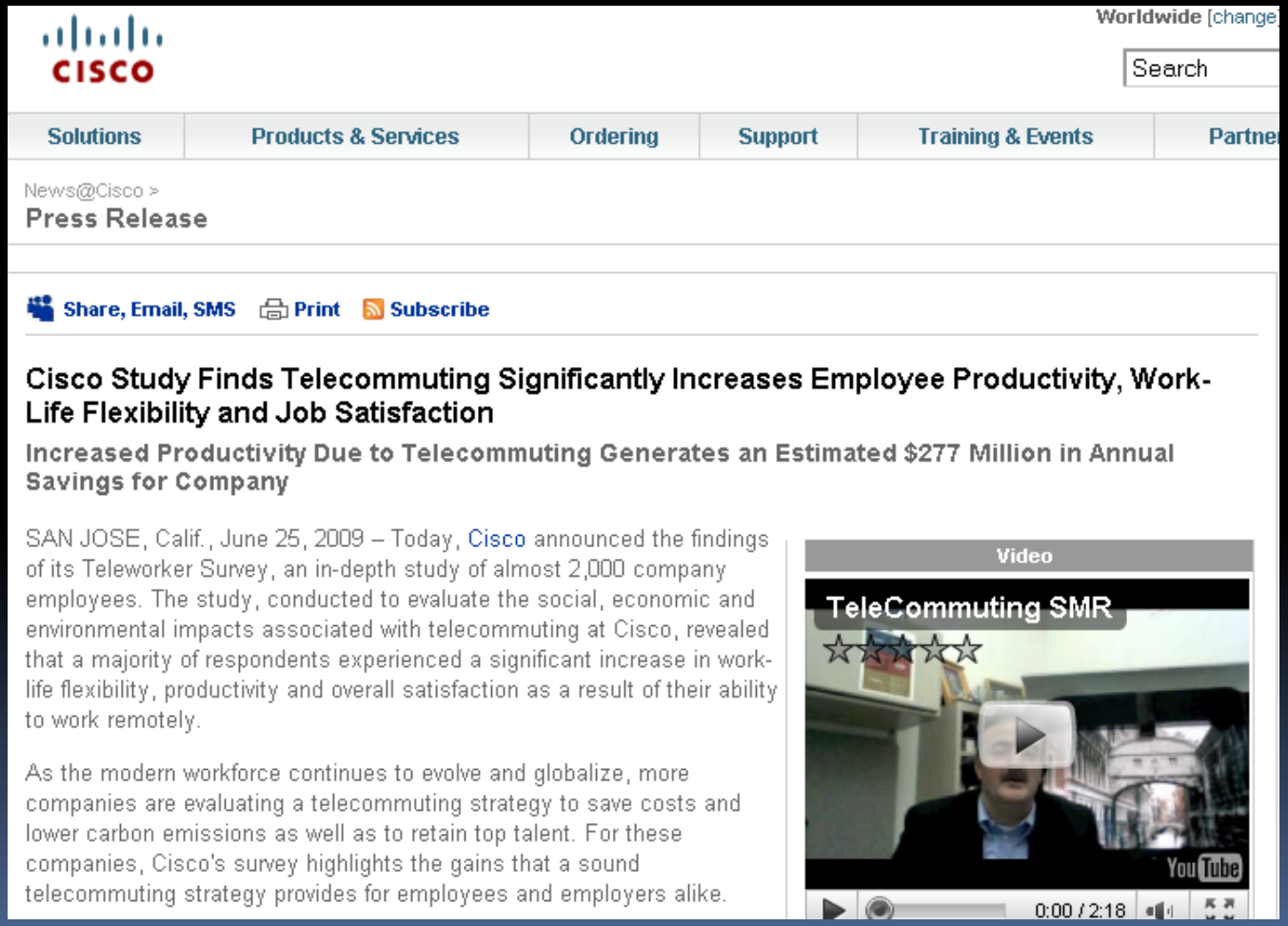
New Considerations

- Operations, behaviors, and ideas are transcending the artificial boundary outside of the network perimeter—the firewall—and, in turn, are being shared in ways that current security models may not have considered

A blurring of activities

- In addition, it is common for workers to blend business and personal communications on these social networks, further blurring the network perimeter

We are a mobile workforce - $277M



Worldwide [change]

Search

Solutions | Products & Services | Ordering | Support | Training & Events | Partne

News@Cisco >

Press Release

Share, Email, SMS Print Subscribe

Cisco Study Finds Telecommuting Significantly Increases Employee Productivity, Work-Life Flexibility and Job Satisfaction

Increased Productivity Due to Telecommuting Generates an Estimated $277 Million in Annual Savings for Company

SAN JOSE, Calif., June 25, 2009 – Today, Cisco announced the findings of its Teleworker Survey, an in-depth study of almost 2,000 company employees. The study, conducted to evaluate the social, economic and environmental impacts associated with telecommuting at Cisco, revealed that a majority of respondents experienced a significant increase in work-life flexibility, productivity and overall satisfaction as a result of their ability to work remotely.

As the modern workforce continues to evolve and globalize, more companies are evaluating a telecommuting strategy to save costs and lower carbon emissions as well as to retain top talent. For these companies, Cisco's survey highlights the gains that a sound telecommuting strategy provides for employees and employers alike.

Video

Our own technologies

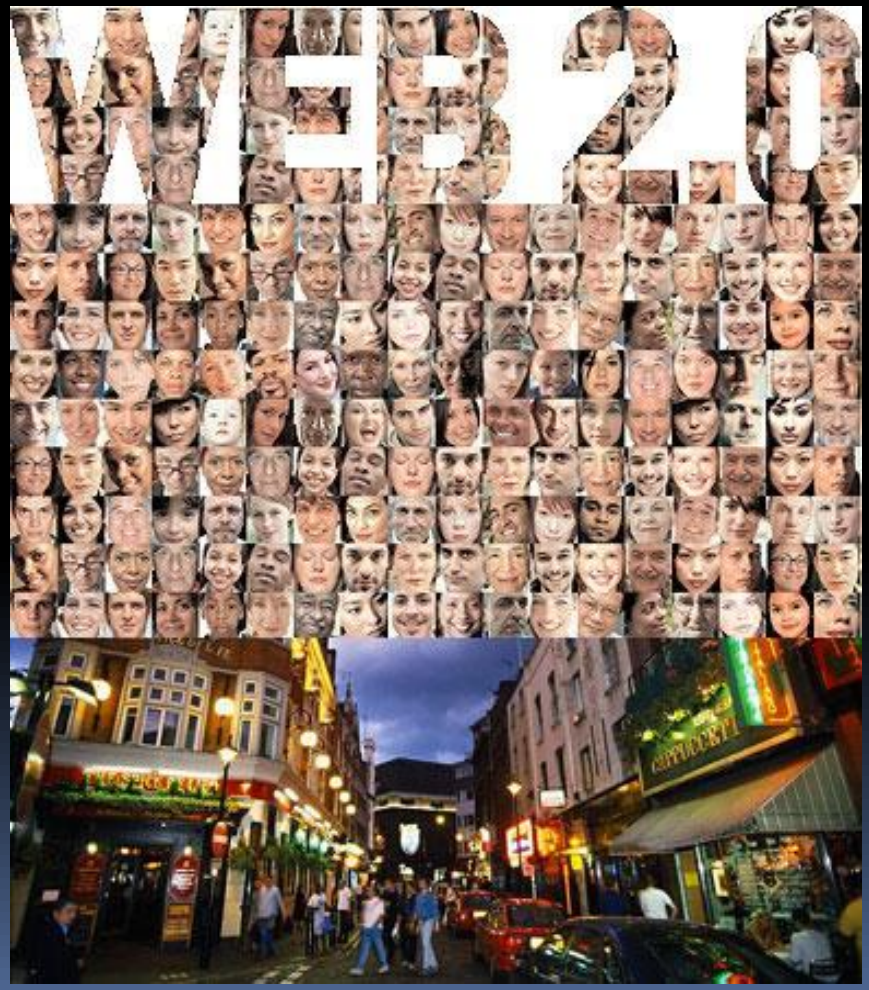
Remember when…

- Security meant having someone who could set a rule on a firewall
- The security officer was the guy at the desk in the lobby
- Browsing was something you did at a Mall
- Podcasting was throwing peas into the wind

Remember when…

- Intrusion prevention was locking your front door
- Identity theft was handing in someone else's homework
- Data loss was forgetting where you put your car keys
- Those days are gone…

Where are we going and what are we doing?



Facebook

- Over half a billion users

Facebook

- If Facebook were its own country, it would be the third most populous nation in the world behind China and India--both countries have populations north of one billion people

Some bone-jarring statistics

- 50% of facebook active users log on to facebook on any given day
- More than 60 million users update their status - daily
- People spend over 500 billion minutes per month on Facebook

Billions

- More than 3 billion photos uploaded to the site each month
- More than 5 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) shared each week

The involvement is viral

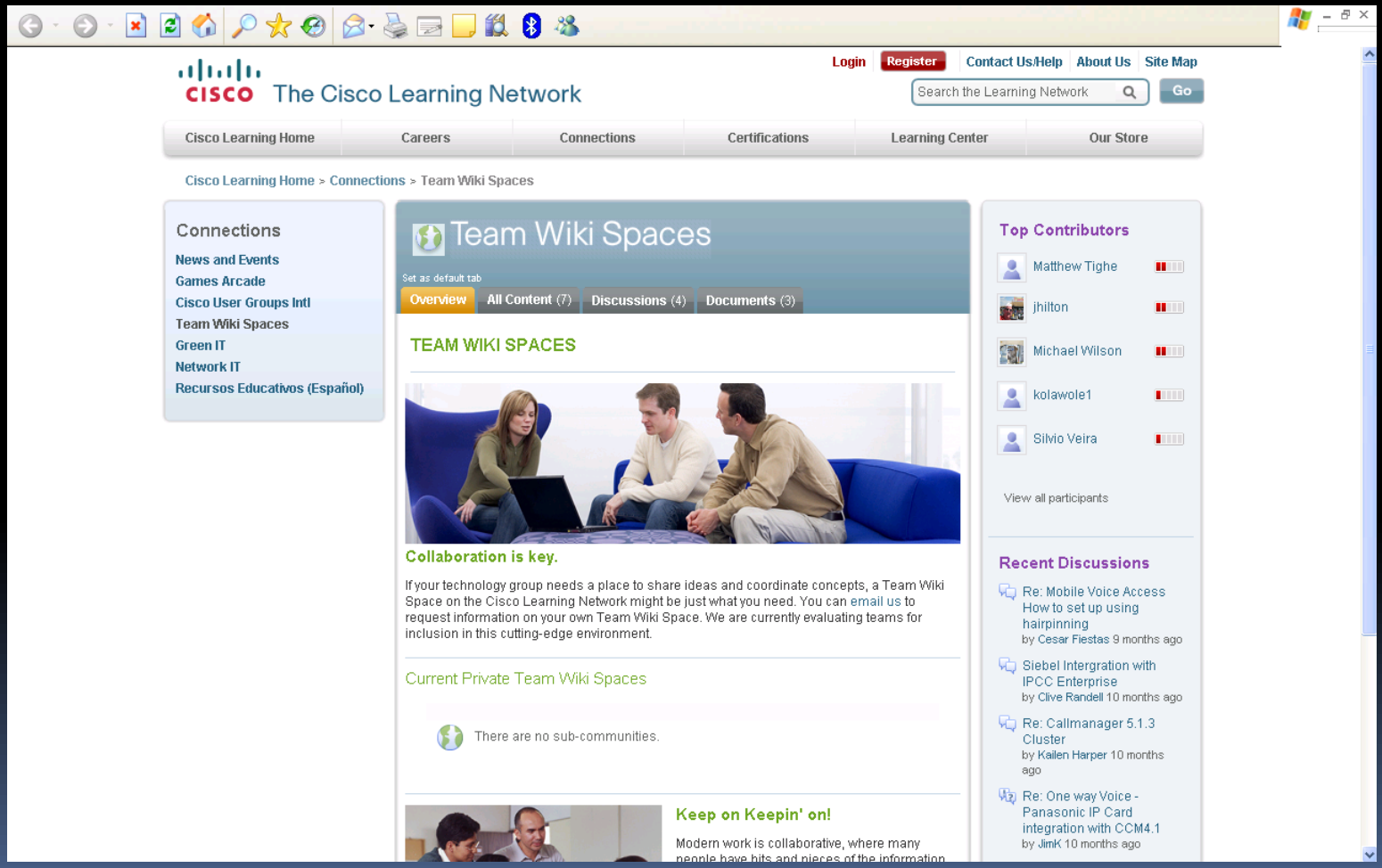
- Millions of local businesses have active Pages on Facebook
- More than 20 million people become fans of Pages each day
- Pages have created more than 5.3 billion fans

Mobility

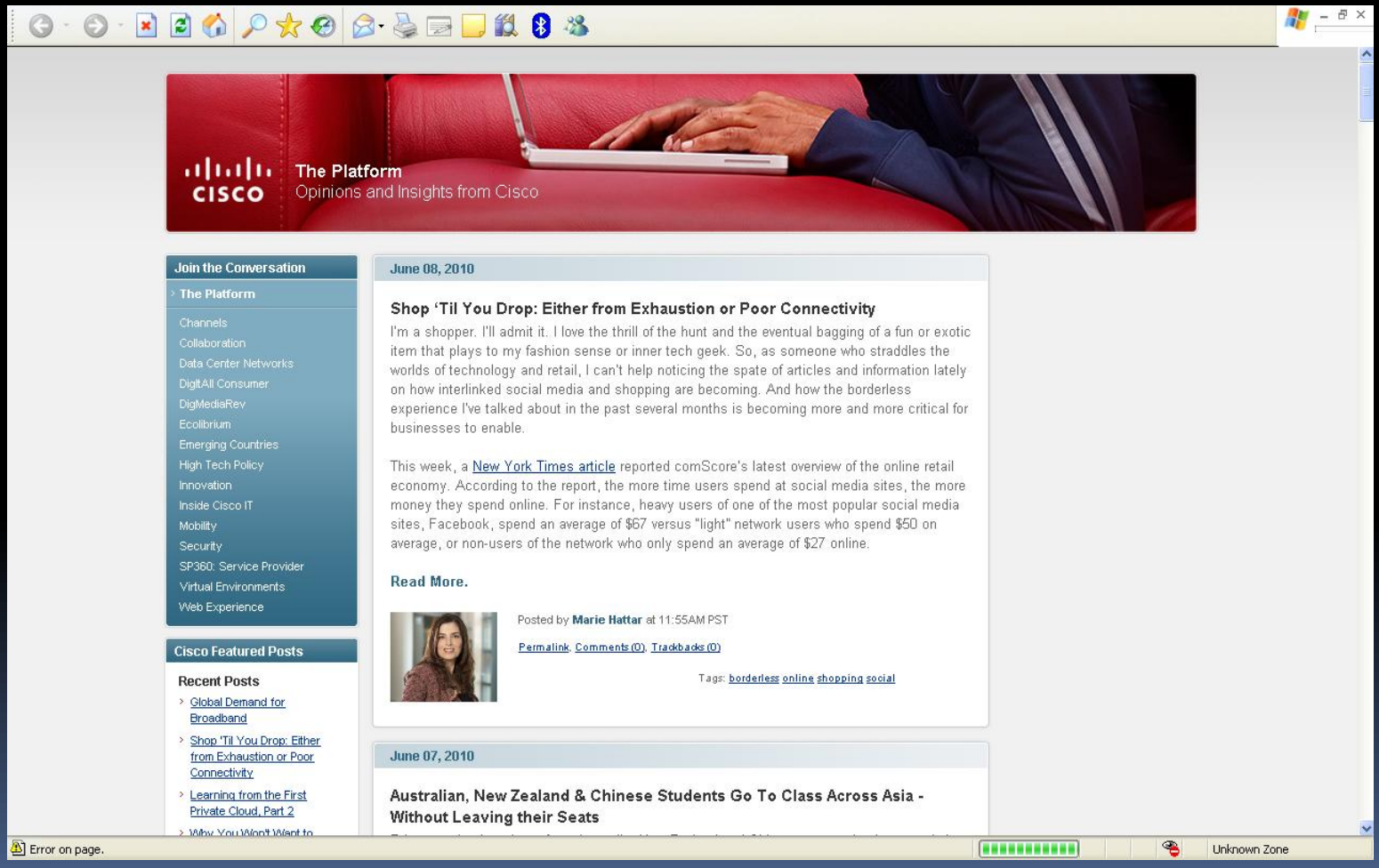
- There are more than 100 million active users currently accessing facebook through their mobile devices

Cisco on Facebook

Cisco Wikis

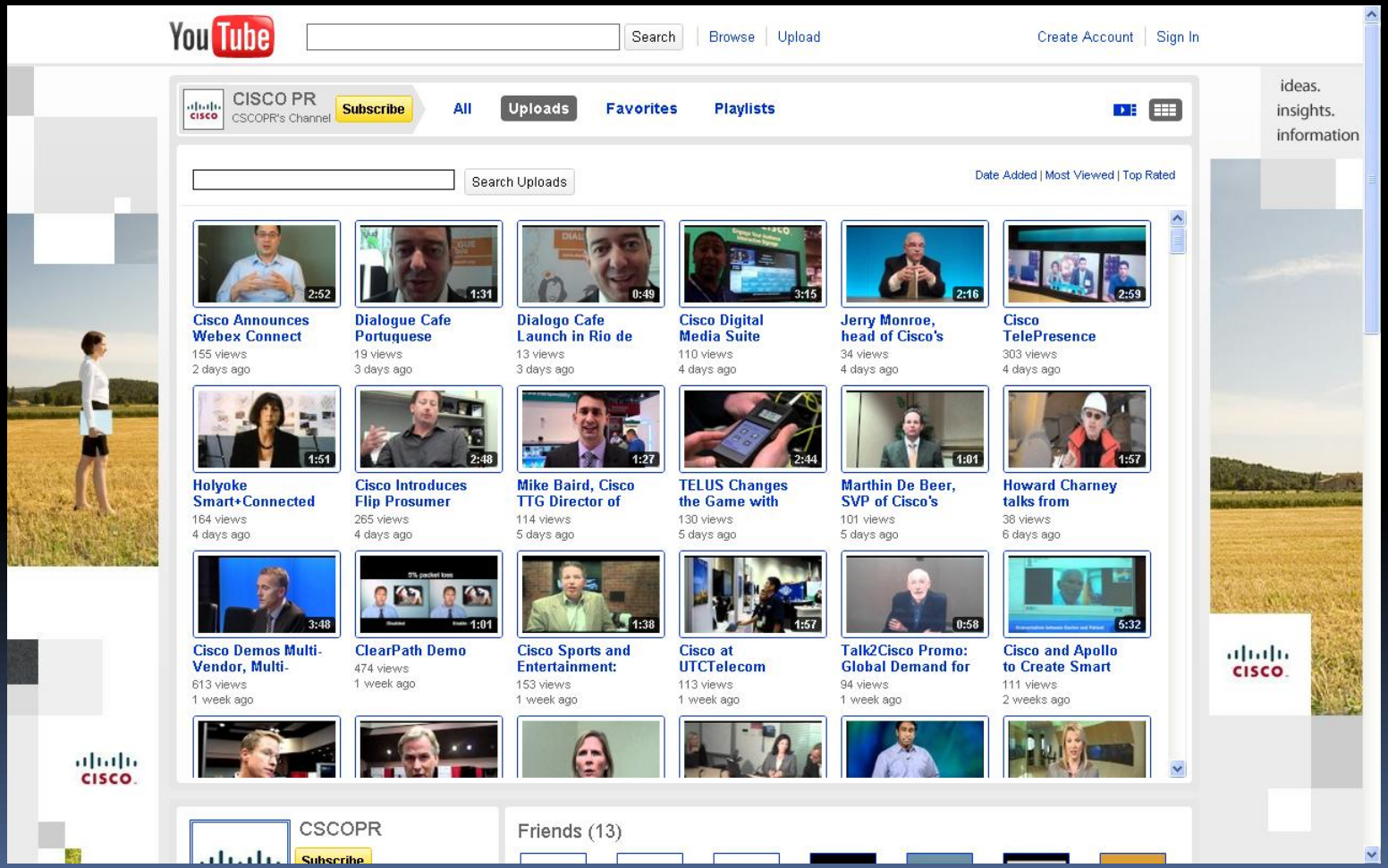

Login
Register
Contact Us/Help
About Us
Site Map
cisco
The Cisco Learning Network
Search the Learning Network
Go
Cisco Learning Home
Careers
Connections
Certifications
Learning Center
Our Store
Cisco Learning Home > Connections > Team Wiki Spaces
Connections
News and Events
Games Arcade
Cisco User Groups Intl
Team Wiki Spaces
Green IT
Network IT
Recursos Educativos (Español)
Team Wiki Spaces
Set as default tab
Overview
All Content (7)
Discussions (4)
Documents (3)
TEAM WIKI SPACES
Collaboration is key.
If your technology group needs a place to share ideas and coordinate concepts, a Team Wiki Space on the Cisco Learning Network might be just what you need. You can email us to request information on your own Team Wiki Space. We are currently evaluating teams for inclusion in this cutting-edge environment.
Current Private Team Wiki Spaces
There are no sub-communities.
Keep on Keepin' on!
Modern work is collaborative, where many
Top Contributors
Matthew Tighe
jhilton
Michael Wilson
kolawole1
Silvio Veira
View all participants
Recent Discussions
Re: Mobile Voice Access How to set up using hairpinning
by Cesar Fiestas 9 months ago
Siebel Intergration with IPCC Enterprise
by Clive Randell 10 months ago
Re: Callmanager 5.1.3 Cluster
by Kailen Harper 10 months ago
Re: One way Voice - Panasonic IP Card integration with CCM4.1
by JimK 10 months ago

Cisco Blogs


The Platform
Opinions and Insights from Cisco
Join the Conversation
The Platform
Channels
Collaboration
Data Center Networks
DigItAll Consumer
DigMediaRev
Ecolibrium
Emerging Countries
High Tech Policy
Innovation
Inside Cisco IT
Mobility
Security
SP360: Service Provider
Virtual Environments
Web Experience
Cisco Featured Posts
Recent Posts
Global Demand for Broadband
Shop 'Til You Drop: Either from Exhaustion or Poor Connectivity
Learning from the First Private Cloud, Part 2
June 08, 2010
Shop 'Til You Drop: Either from Exhaustion or Poor Connectivity
I'm a shopper. I'll admit it. I love the thrill of the hunt and the eventual bagging of a fun or exotic item that plays to my fashion sense or inner tech geek. So, as someone who straddles the worlds of technology and retail, I can't help noticing the spate of articles and information lately on how interlinked social media and shopping are becoming. And how the borderless experience I've talked about in the past several months is becoming more and more critical for businesses to enable.
This week, a New York Times article reported comScore's latest overview of the online retail economy. According to the report, the more time users spend at social media sites, the more money they spend online. For instance, heavy users of one of the most popular social media sites, Facebook, spend an average of $67 versus "light" network users who spend $50 on average, or non-users of the network who only spend an average of $27 online.
Read More.
Posted by Marie Hattar at 11:55AM PST
Permalink, Comments (0), Trackbacks (0)
Tags: borderless online shopping social
June 07, 2010
Australian, New Zealand & Chinese Students Go To Class Across Asia - Without Leaving their Seats
Error on page.
Unknown Zone

Cisco on Twitter

Cisco on YouTube



What else are they doing?

- In August, people spent a total of 41.1 million minutes on Facebook

Facebook outage spotlights social media addiction

- After Facebook went down on Thursday, one thing was certain: People don't like to go without their favorite social networking site
- Industry watchers say Facebook users suffering through the two-and-a-half-hour outage were like drug addicts going through withdrawal

In despair…

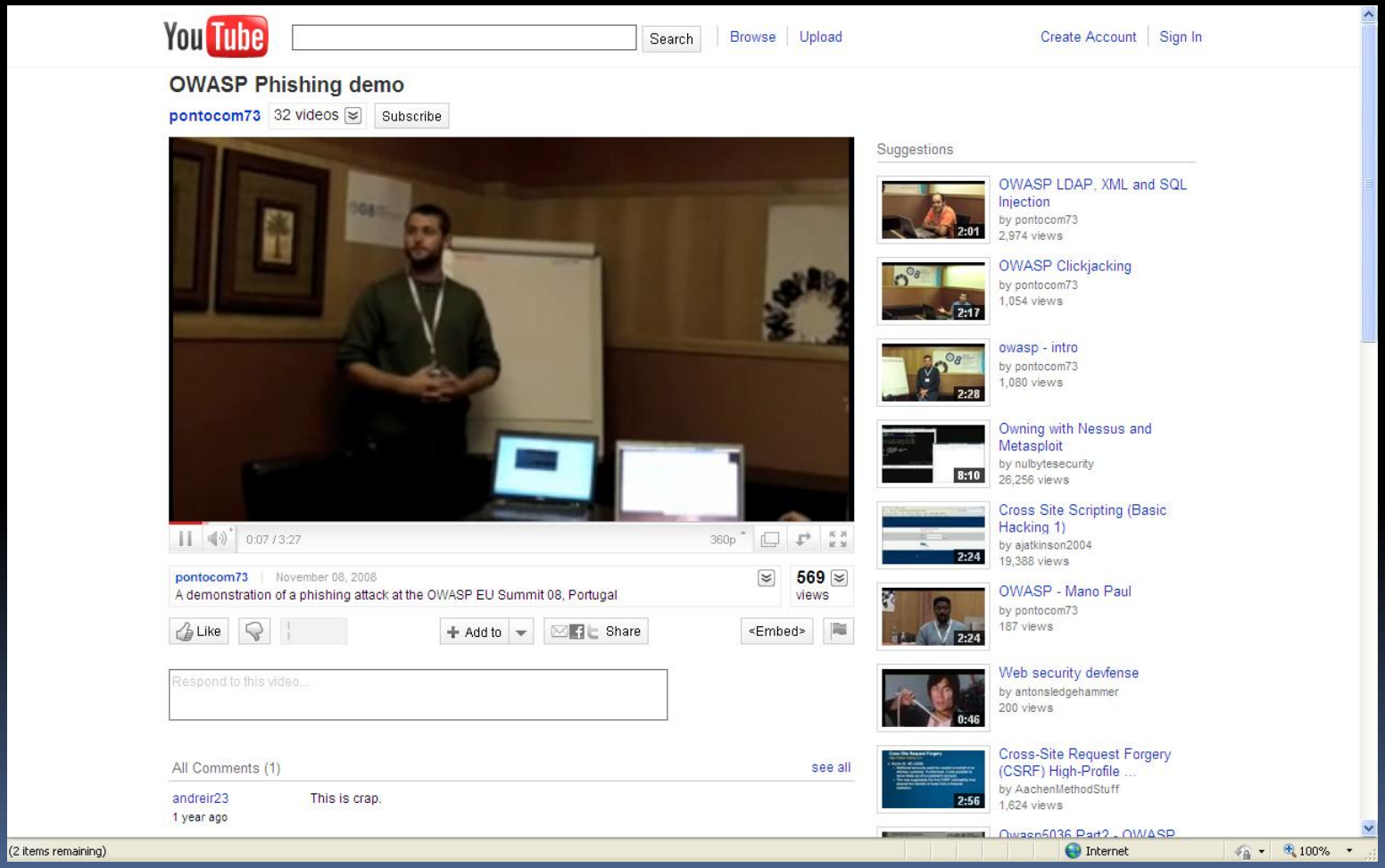
- Facebook's more than 500 million users have grown accustomed to sharing updates about their cats and colleagues, and posting funny pictures of drunken friends and kids acting silly

OWASP on Twitter

On Facebook

facebook
Email
pgray525@gmail.com
Password
Login
Keep me logged in
Forgot your password?
Sign Up
Open Web Application Security Project (OWASP) is on Facebook
Sign up for Facebook to connect with Open Web Application Security Project (OWASP).
Open Web Application Security Project (OWASP)
Wall
Info
Photos
Discussions
Events
Tom Brennan OWASP Company Profile
OWASP - Company Profile on LinkedIn
www.linkedin.com
The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software. Our…
June 24 at 12:19am · Comment · Like
DJe Jérôme Radar's SQL injection... ;-)
Open Web Application Security Project (OWASP) Photos
May 12 at 7:15am
Jeff Snyder Web Application Secuity Consultant Job Openings, Full-Time and Contract, Telecommute 70-80% of the time. Strong Java Enterprise development background desired prior to getting into application security. Find these opportunties at SecurityRecruiter.com
misjobs.com
misjobs.com
April 2 at 2:58pm · Comment · Like
Sylvain Maret
The Open Web Application Security Project (OWASP) is a 501c3 not-for-profit worldwide charitable organization focused on improving the security of application software.
Information
Category:
Internet & Technology - Websites
Description:
The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications that can be trusted. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security. We advocate approaching application security as a people, process, and technology problem because the most effective approaches to application security include improvements in all of these areas. (read more)
Privacy Type:
Done
Internet
100%

YouTube


YouTube
Search
Browse
Upload
Create Account
Sign In
OWASP Phishing demo
pontocom73
32 videos
Subscribe
0:07 / 3:27
360p
pontocom73 November 08, 2008
A demonstration of a phishing attack at the OWASP EU Summit 08, Portugal
569 views
Like
Add to
Share
<Embed>
Respond to this video...
All Comments (1)
see all
andreir23
1 year ago
This is crap.
Suggestions
OWASP LDAP, XML and SQL Injection
by pontocom73
2,974 views
2:01
OWASP Clickjacking
by pontocom73
1,054 views
2:17
owasp - intro
by pontocom73
1,080 views
2:28
Owning with Nessus and Metasploit
by nulbytesecurity
26,256 views
8:10
Cross Site Scripting (Basic Hacking 1)
by ajatkinson2004
19,388 views
2:24
OWASP - Mano Paul
by pontocom73
187 views
2:24
Web security devfense
by antonsledgehammer
200 views
0:46
Cross-Site Request Forgery (CSRF) High-Profile ...
by AachenMethodStuff
1,624 views
2:56
(2 items remaining)
Internet
100%

This is viral

- Overall, 43 percent of Americans said they keep in touch via social networking websites such as Facebook, MySpace and LinkedIn
- Forty percent of men, and 45 percent of women, said they had a profile on a networking site

There is a human element to all of this, an element that is more often than not, overlooked…

It’s no longer just close relationships

- Our employees are going places they’ve never gone before and are touching technology daily
- That which they are touching is touching our networks as well

Web 2.0?

- Businesses today find that social media use is no longer the exception, but rather the rule
- It marks the global trend of seeking friendships or relationships online

Who is using it?

- Business units such as research and development, marketing, human resources, sales, and customer service
- They are realizing the potential for utilizing social media tools to stimulate innovation, create brand recognition, hire and retain employees, generate revenue, and improve customer satisfaction

With Web 2.0

- A new breed of malware is evolving
- Google Mashups, RSS feeds, search, all of these can be misused by hackers to distribute malware, attack Web surfers and communicate with botnets

Risk – it's everywhere

- And no one knows that better than IT security professionals
- Disgruntled employees, students, fired employees, clueless employees who succumb to social engineering, passwords left on Post-it notes, wide-open instant messaging and increasingly powerful hacker tools in the hands of teenagers, Web Mobs and Organized Crime targeting Social Media sites

Objective?

- The key objective, of course, is to recognize risk, safeguard your reputation and not reveal sensitive or confidential information that may prove harmful to your business

Social Media Benefits

- It is very difficult to argue with many of the benefits being provided by the numerous social media networks for both personal and business purposes

Information sharing

- These networks, Facebook, Twitter, LinkedIn, and YouTube to name some of the heavy hitters, enable millions of people to exchange up-to-the-minute information with each other across the globe

Concerns

- As with most new voice, video, and data applications that traverse the network, this pervasiveness brings with it additional security concerns.

How do we secure it?

- It becomes difficult and, in fact, almost contradictory for organizations to crack down on the use of social networks while they are simultaneously promoting the use of such networks to do business

Ease the burden

- This balancing act can be made a bit easier through:
- The development and enforcement of corporate security policies
- Ongoing education of employees in the proper use of social networks when corporate assets are involved
- The identification and mitigation of related malware using network and host-based anomaly detection technologies

Malware

- Historically, malware has plagued e-mail, hidden in malicious attachments
- While that's still happening, more malware writers are putting their efforts into malicious Web sites

Constant Mutation

- The goal in developing malware is not to simply infect as many systems as possible but to specifically steal usage information and other data from compromised systems
- Use of polymorphic code that constantly mutates

Bad Statistic

- 1 in 1,000 web pages is infected with malicious drive-by download software

Two biggest vectors for Malware

- Email
- Web-based

So, what do we have to do?

- Create a Human Firewall

The Human Firewall – an invaluable tool

- A good *human firewall employee* is one who filters good security practices and rejects any others—much like a network firewall only allows authorized traffic and rejects any other
- The only way to build a good human firewall is to raise people's awareness; to teach them good habits, to make them recognize bad practices and change them into good practices
- Your cyber security is only as good as the people who manage it and those who use it

So Patrick, why do we really need that Human Firewall?

- Because, ‘Friend’ has become a verb
- Social media users believe there is protection in being part of a community of people they know
- Criminals are happy to prove this notion wrong
- The threats and security issues that come with social media aren’t usually caused by vulnerabilities in software
- More commonly, these threats originate from individuals who place an unwarranted amount of “transitive trust” in the safety of these communities

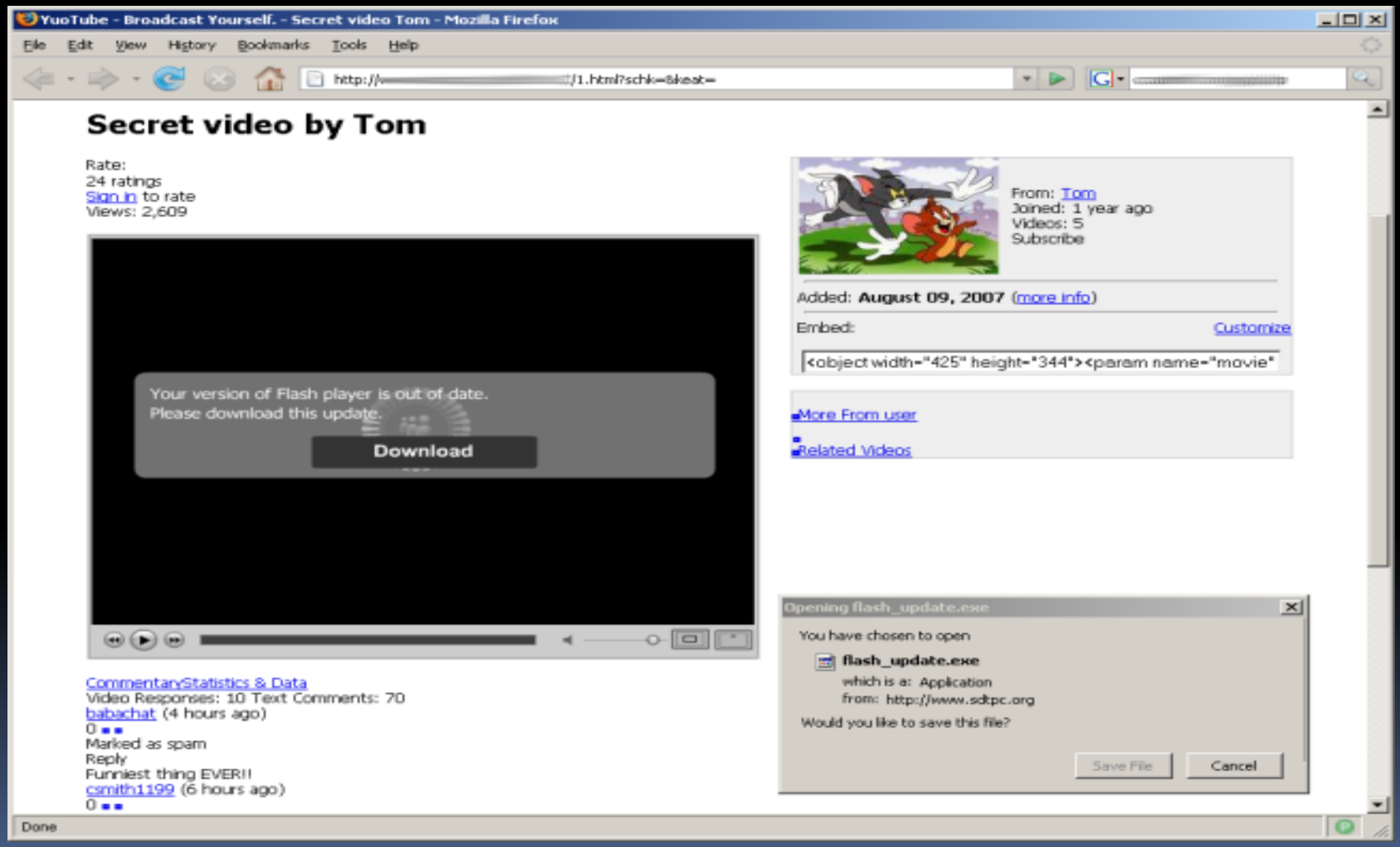
Remember…

- On social sites –
- Your privacy is history
- They don't have your best interests in mind
- Social engineering attacks are getting more targeted

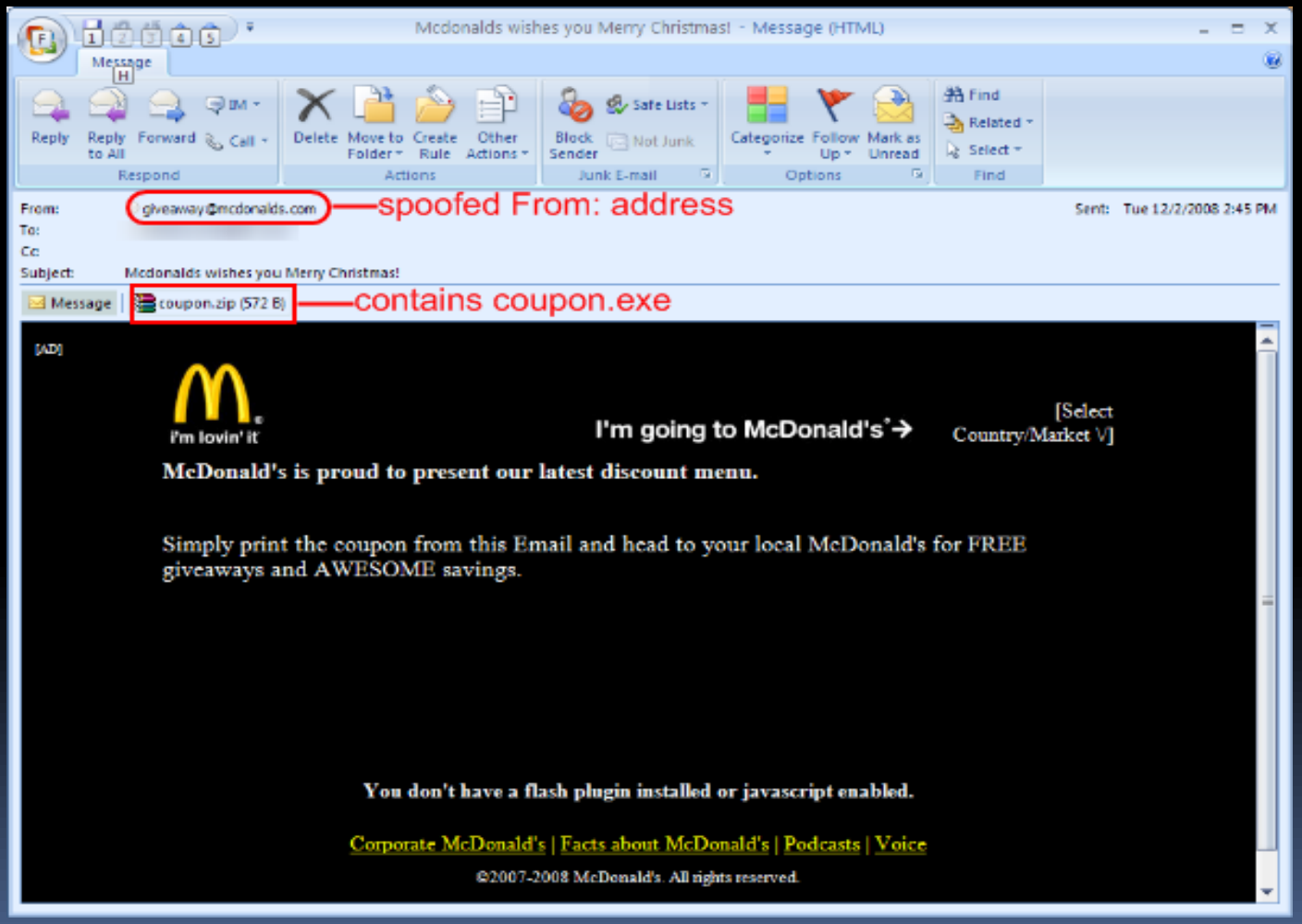
Trust?

- Users will trust something or someone because a user they know has also expressed trust in that person or subject
- We trust because we are curious and curiosity…

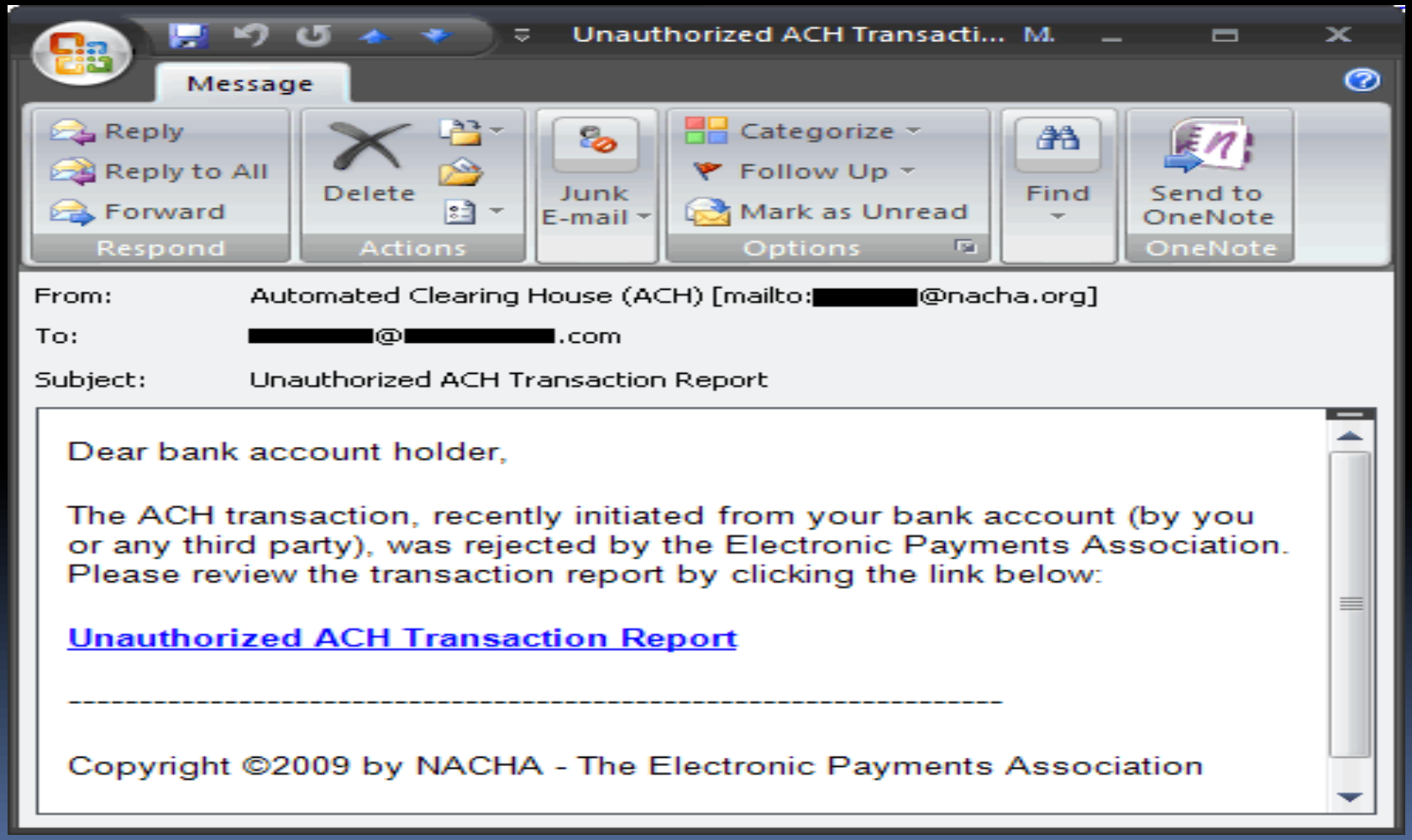
Curious? This is why! Out of date???



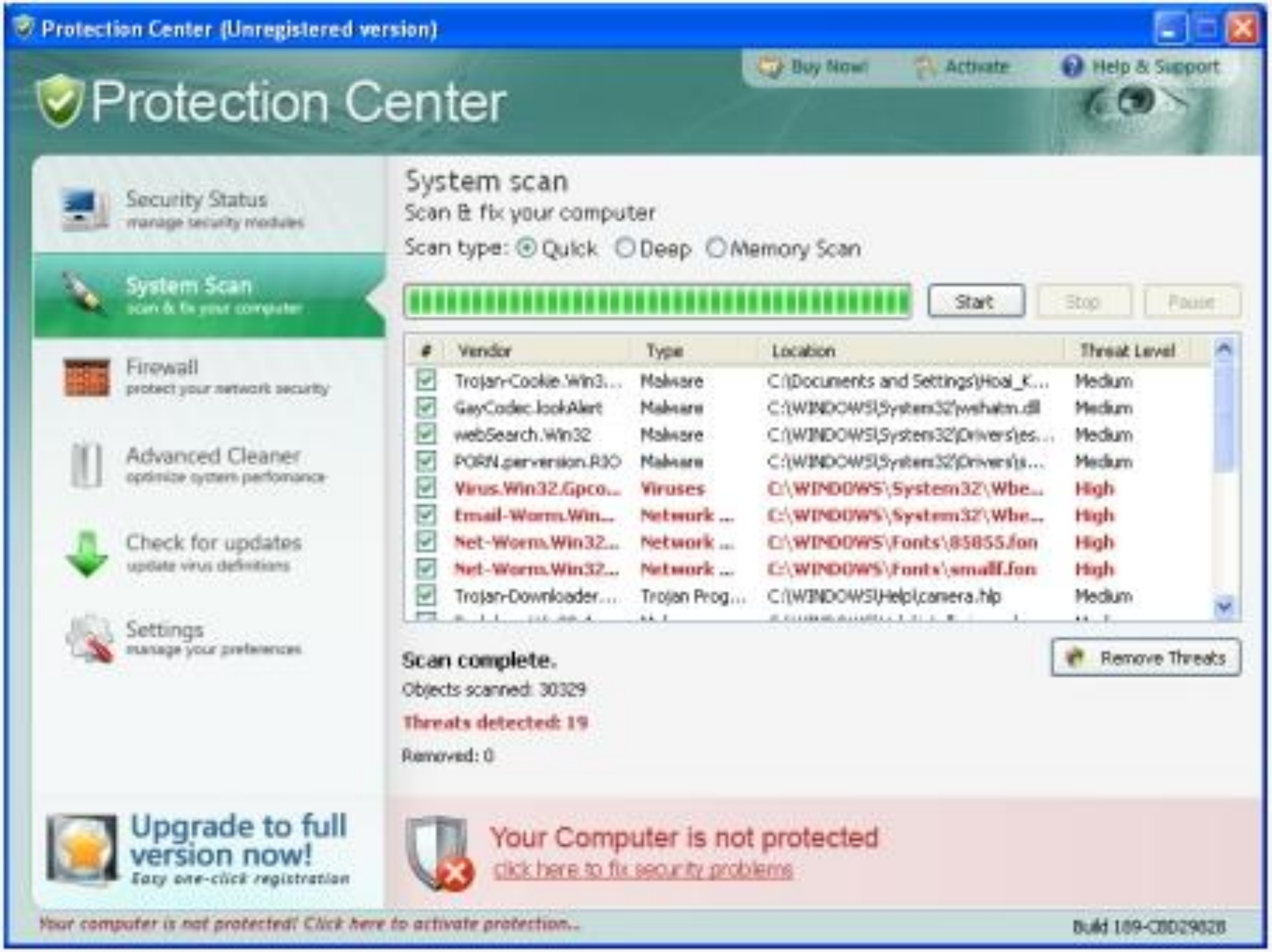
Or a Big Mac!


Mcdonalds wishes you Merry Christmas! - Message (HTML)
Message
Reply
Reply to All
Forward
IM
Call
Respond
Delete
Move to Folder
Create Rule
Other Actions
Actions
Block Sender
Safe Lists
Not Junk
Junk E-mail
Categorize
Follow Up
Mark as Unread
Options
Find
Related
Select
Find
From:
giveaway@mcdonalds.com
spoofed From: address
Sent: Tue 12/2/2008 2:45 PM
To:
Cc:
Subject: Mcdonalds wishes you Merry Christmas!
Message
coupon.zip (572 B)
contains coupon.exe
[AD]
i'm lovin' it
I'm going to McDonald's
[Select Country/Market V]
McDonald's is proud to present our latest discount menu.
Simply print the coupon from this Email and head to your local McDonald's for FREE giveaways and AWESOME savings.
You don't have a flash plugin installed or javascript enabled.
Corporate McDonald's | Facts about McDonald's | Podcasts | Voice
©2007-2008 McDonald's. All rights reserved.

They want to send us somewhere else…



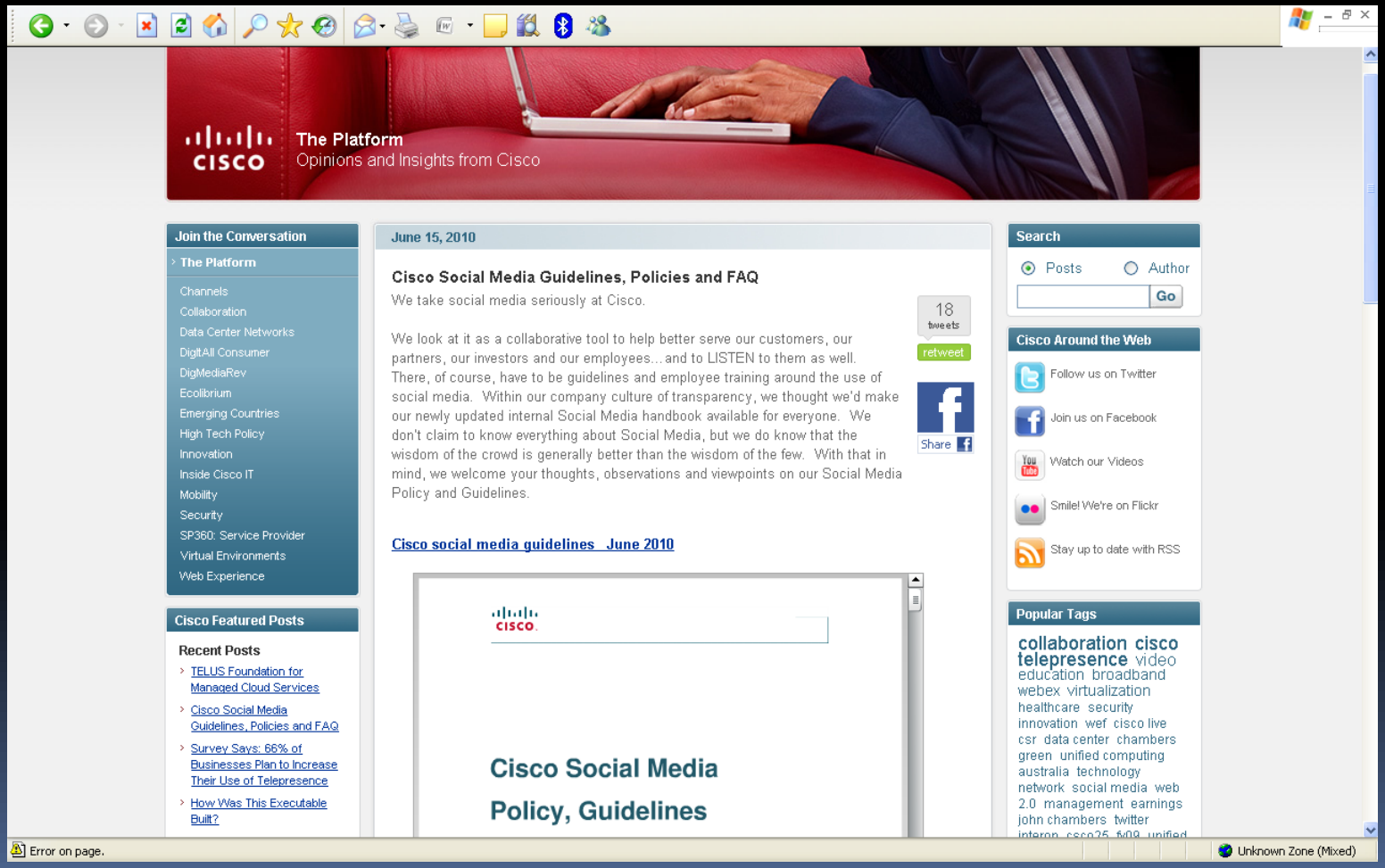
The unknown… DO NOT TOUCH THIS!!!


Protection Center (Unregistered version)
Buy Now!
Activate
Help & Support
Protection Center
Security Status
manage security modules
System Scan
scan & fix your computer
Firewall
protect your network security
Advanced Cleaner
optimize system performance
Check for updates
update virus definitions
Settings
manage your preferences
Upgrade to full version now!
Easy one-click registration
System scan
Scan & fix your computer
Scan type: Quick Deep Memory Scan
Start
Stop
Pause
Vendor Type Location Threat Level
Trojan-Cookie.Win3... Malware C:\Documents and Settings\Hoai_K... Medium
GayCodec.lookAlert Malware C:\WINDOWS\System32\wshatm.dll Medium
webSearch.Win32 Malware C:\WINDOWS\System32\Drivers\es... Medium
PORN.perversion.R30 Malware C:\WINDOWS\System32\Drivers\s... Medium
Virus.Win32.Gpco... Viruses C:\WINDOWS\System32\Wbe... High
Email-Worm.Win... Network ... C:\WINDOWS\System32\Wbe... High
Net-Worm.Win32... Network ... C:\WINDOWS\Fonts\85855.fon High
Net-Worm.Win32... Network ... C:\WINDOWS\Fonts\smallf.fon High
Trojan-Downloader... Trojan Prog... C:\WINDOWS\Help\camera.hlp Medium
Scan complete.
Objects scanned: 30329
Threats detected: 19
Removed: 0
Remove Threats
Your Computer is not protected
click here to fix security problems
Your computer is not protected! Click here to activate protection...
Build 109-080129028

Windows Security Alert
To help protect your computer, Windows Firewall has detected activity of harmful software.
Do you want to block this software from sending data over the Internet?
Name: Trojan-Spy.Win32.GreenScreen
Risk Level: CRITICAL
Description: This is spy trojan that installs itself to the system, hides itself and then captures screen images and saves them to disk files in encrypted form. Thus it allows to a hacker to watch screen images.
Keep Blocking
Unblock
Enable Protection
Windows Firewall has detected unauthorized activity, but unfortunately it cannot help you to remove viruses, keyloggers and other spyware threats that steal your personal information from your computer, including your Credit Card data and access passwords to the online resources you use. Click here to pick recommended software to resolve this issue.

SystemDefender
HOME
DOWNLOAD
YOUR SYSTEM MAY BE
INFECTED!
Scanning:
Internet trheats and viruses found:
FREE SCAN NOW!

Social Media Policy, Guidelines



But what does all this mean?

- I am just an employee and am not an engineer or a technician or a programmer or a geek!
- I’m just sitting at my desk, talking to friends, patients and all sorts of people
- How in the world am I threatening our network???

2 Reasons…

- You probably do not understand policies, procedures, best practices and standards
- If you do understand them, they are violated because there are no consequences – the policies are not enforced
- Who, me?

Education is Critical

- Few executives grasp the case for investing in safeguards against hackers, malware, and the like
- Education starts at the top and works its way down the food chain throughout the entire business
- Before any employee puts their fingers on the keyboard they must understand that it is not ***their*** computer

The Seven Deadly Sins of Network Security

1. Not measuring risk
2. Thinking compliance equals security
3. Overlooking the people
4. Too much access for too many
5. Lax patching procedures
6. Lax logging, monitoring
7. Spurning the K.I.S.S.

You Must Understand…

- That you are a target
- These hackers are smart, and most have much more time to spend attacking them than a typical systems administrator can spend defending against them

The Opposing Team

- The Hackers
- Disgruntled Insiders
- Clueless employees
- Competitors
- Foreign Governments
- Terror organizations

Top 8 Perceived Threats

- System penetration
- Sabotage of data
- Theft of proprietary information
- Denial of service
- Viruses and Worms
- Unauthorized insider access
- Laptop theft
- Insider abuse of the Internet

System Penetration

- It is an unfortunate reality that you will suffer a breach of security at some point
- To bypass security, an attacker only has to find one vulnerable system within the entire network
- But to guarantee security, you have to make sure that 100 percent of your systems are invulnerable -- 100 percent of the time

Data Leakage: How many breaches in 2009?

- 498 Breaches
- 222,477,043 records exposed
- How were you impacted?

Who?

- Businesses - 36 percent
- Healthcare - 29.2 percent
- Government, military - 16.9 percent
- Financial Services – 11.1 percent

2010

- 327 Data Breaches

Not good…

- But Patrick! It won't happen to us!

Whether you get hacked depends…

- Do you assume the posture of, “It can’t happen here.”
- Do you hear, “We haven’t heard of any worm outbreaks and all seems quiet. Why upgrade those devices?”
- “We have no budget.”
- “We’re just hanging out in Cincinnati!”
- “They’re only going after the Government and those really big banks.”
- Then my question is, “Can you really afford to give up data today?

You can't! So,

- Be compliant but don't rest on your laurels
- Be vigilant
- Educate
- Know that you are a target
- Be ready to respond

So, what are they really after?

- Your Intellectual Property
- Your assets
- Your employee's data
- Your personal data
- Your paycheck
- Your friends
- Your family

G-Man's tips to secure your data

- **Consider threats** from insiders and business partners in your enterprise-wide risk assessments
- **Clearly document** and consistently enforce policies and controls
- **Institute periodic** security awareness training for all employees

G-Man's tips to secure your data

- **Monitor and respond** to suspicious or disruptive behavior, beginning with the hiring process
- **Anticipate and manage** negative workplace issues

G-Man's tips to secure your data

- **Implement strict** password and account management policies and practices
- **Enforce separation** of duties and least privilege
- **Implement system change** controls
- **Log, monitor and audit** employee online actions
- **Use layered defense** against remote attacks

G-Man's tips to secure your data

- **Deactivate computer access** following termination
- **Implement secure backup** and recovery processes
- **Develop an insider** incident response plan

You are the last line of Defense! Don’t drop the ball!!!

- Understand
- Educate
- Collaborate
- Prepare

Thank You!

pagray@cisco.com