




The New “Insider” Threat



Extending Device and Data Protection
to the Mobile Workforce

Jim Szafranski
www.Fiberlink.com

FIBERLINK

Simple. Secure. Mobility.

> Agenda

- Mobility Trends and Their Impact on IT
- Addressing Challenges of Greater Mobility
- Solutions Being Pursued to Help Close Gaps
- WiFi Security – a “Tutorial”

> Fiberlink Overview



- **Company** – Founded in 1994. Headquarters in Blue Bell, Pennsylvania. Presence in NA, EMEA & Asia. Over 250 employees.
- **Leader in Mobility as a Service (MaaS)** – Help enterprises leverage new developments in mobile technology to increase productivity, lower costs and improve overall management
- **Leadership** – Recognized by industry analysts as an innovator and leader in the mobile market.
- **Financials** - Privately held, profitable and growing. Investors include Goldman Sachs, GE and TCV.

> Fiberlink Overview



- **Company** – Founded in 1994. Headquarters in Blue Bell Pennsylvania. Presence in NA, EMEA & Asia. Over 250 employees.
- **Mission** – Make Laptop mobile computing simpler and more secure, so enterprises can realize the full potential of mobile work.
- **Customers** – Over 1,000,000 deployed users across over 700 enterprise customers,
- **Leadership** – Recognized by industry analysts as an innovator and leader in the mobile market.
- **Financial** - Privately held, profitable and growing. Investors include Goldman Sachs, GE and TCV

> Today Everyone is Mobile and Access is Everywhere

Road Warriors



Planes

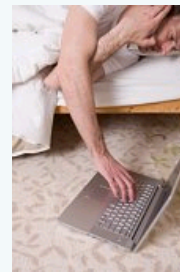
Trains



Automobiles

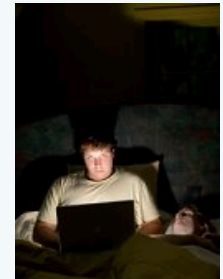
Highly Mobile Employees: 25%

Day Extenders



Morning

Noon



Night

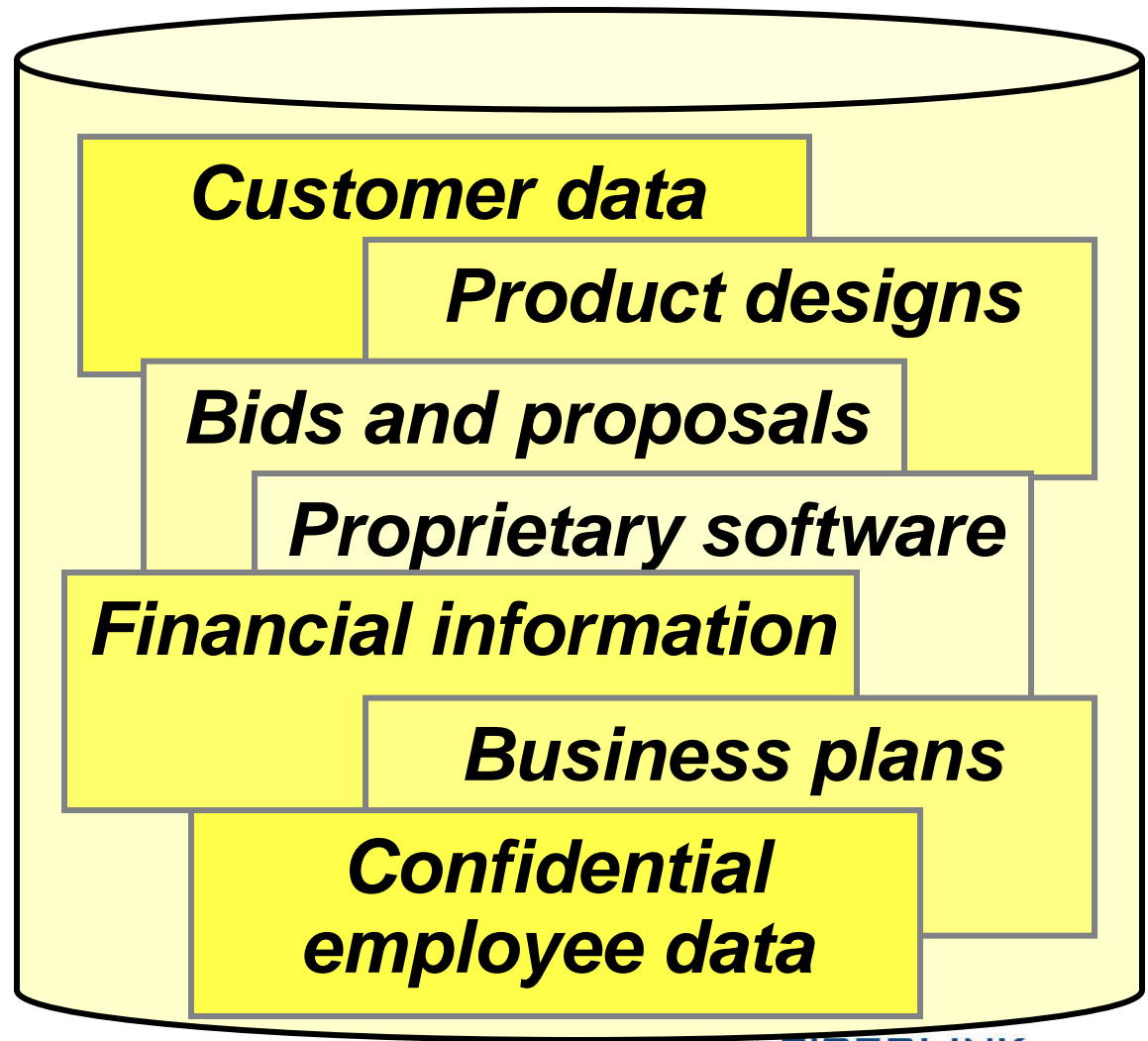
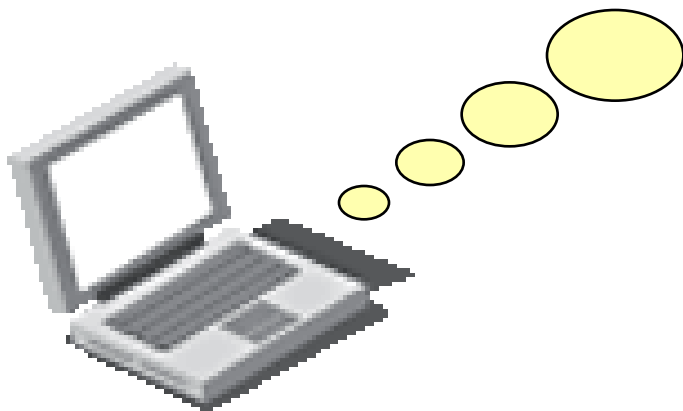
Employees with Laptops: > 50%

[Mobility] is not limited to the traditional 'hot' employee categories, who are typically 'road warriors' seeking to access corporate applications while on the move or in public places; increasingly it also includes part-time and full-time home workers and so-called 'day extenders.'

- Jeremy Green & Pauline Trotter, Ovum, 12/05

> More Data is Exposed on Laptops

IDC estimates that 60% of corporate data resides on laptops and PCs





> Gone Phishing? They are Motivated!

Recent Information Week Article:

- **\$10 - \$150**
 - Price range on the black market for full set of identity information
- **\$.50 - \$5**
 - Price range per stolen credit card number
- **196,860**
 - Unique phishing messages detected by Symantec for the first half of 2007, up 18% over previous 6 months
- **52,771**
 - Number of active bot-infected computers per day during first half of 2007

Source: 2008 Symantec Internet Security Threat Report Trends, 01/07-06/07

> Targeting the Mobile Device

Data In Motion:



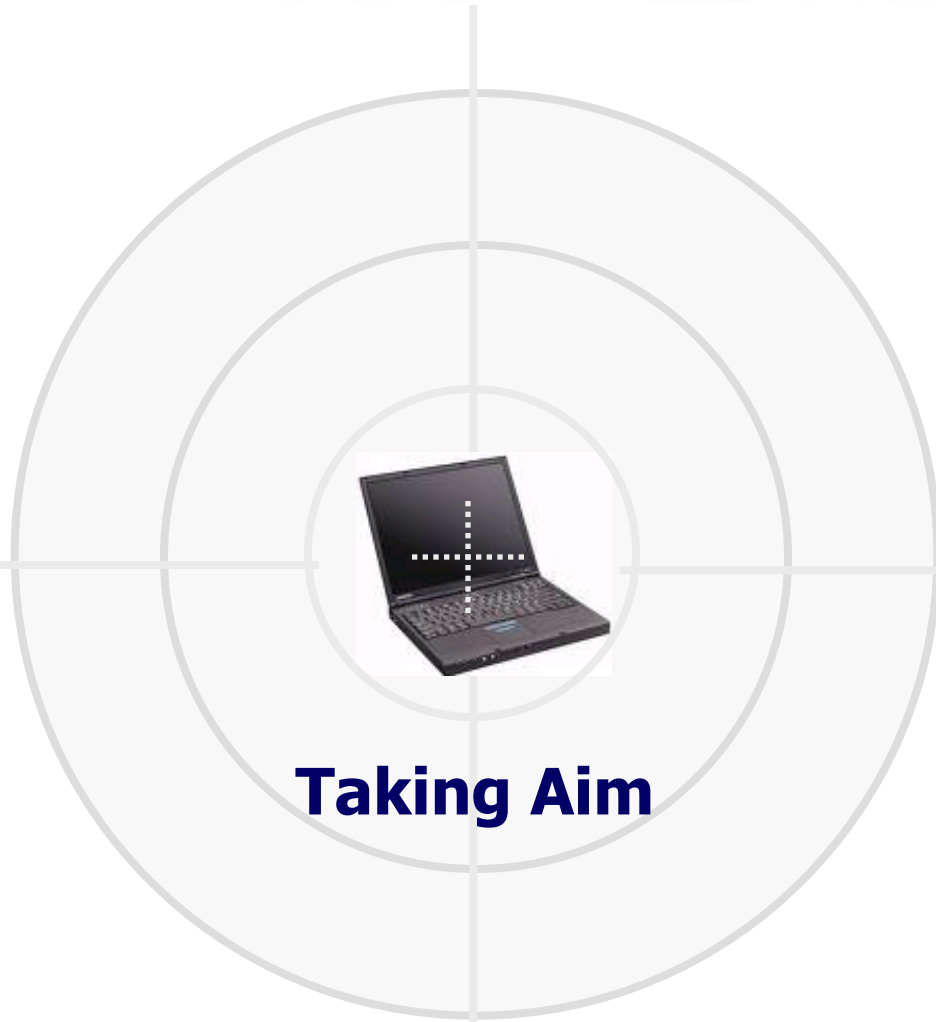
Wireless Hacking:



Lost Device:



Stolen Laptop:

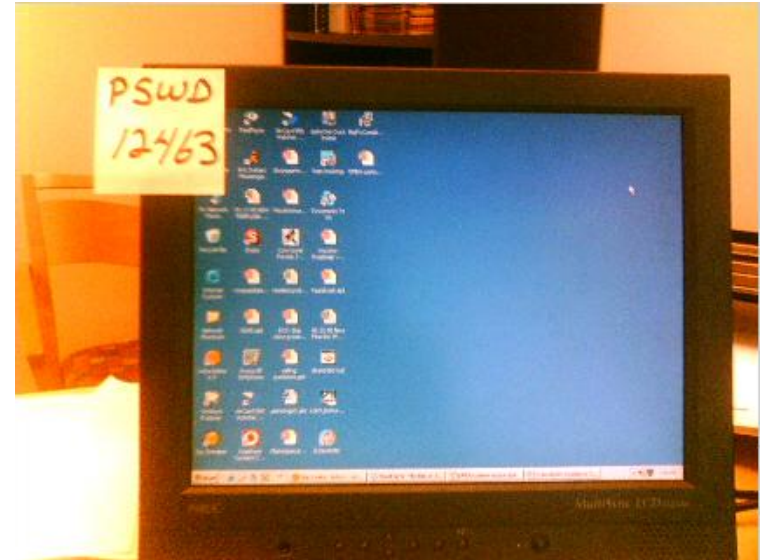
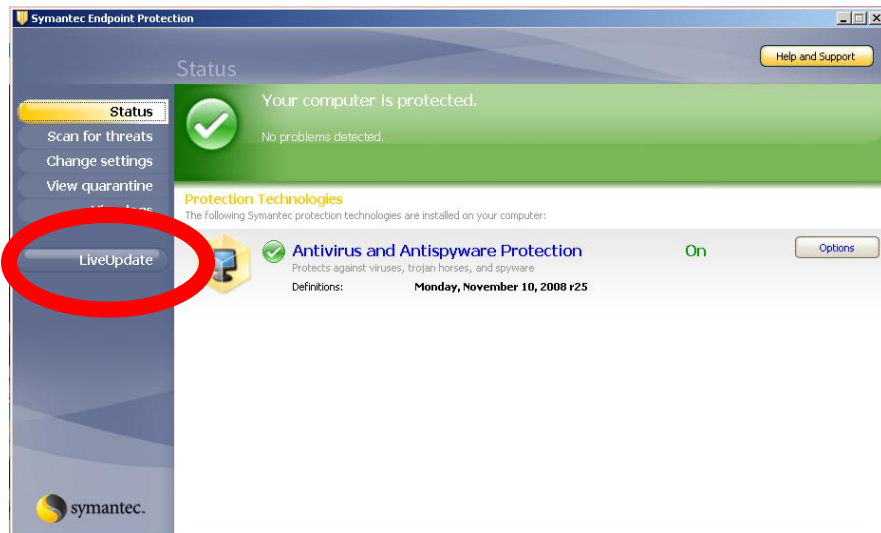


Taking Aim

> You've Got Security Covered, Right?

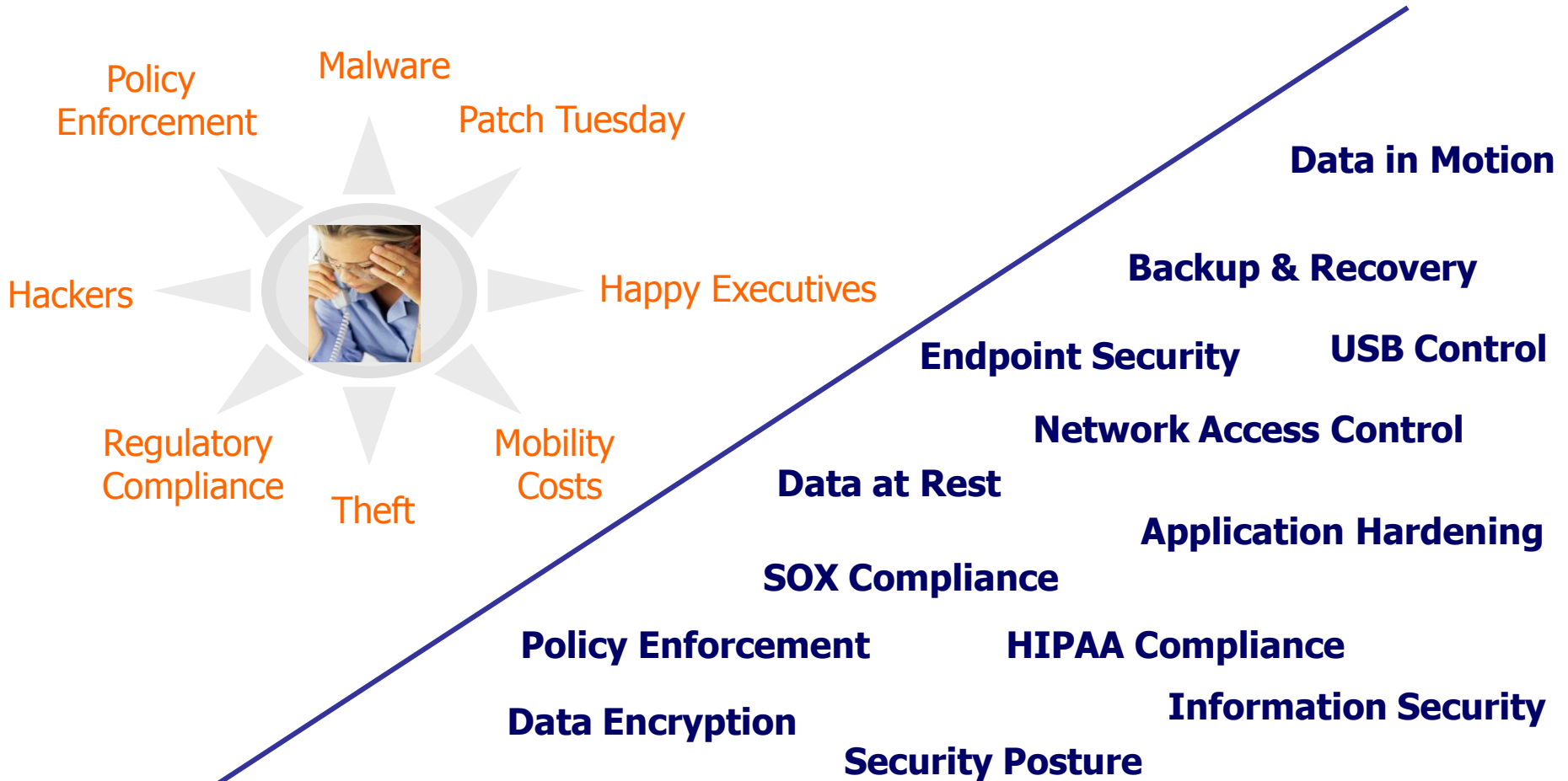
Human Engineering Issues

When it comes to security, you can not depend on the end user alone



Organizations must automate the process and make it seamless to the end user

> Decisions, Decisions...



How do you extend this protection to the remote device?





SSL VPNs:

> Expanding The "Mobile Blind Spot"?

"By 2008, SSL VPNs will be the primary remote-access method for more than two-thirds of business teleworking employees, more than three-quarters of contractors and more than 90% of casual employee access (0.8 probability)." *Gartner*

- An SSL VPNs is referred to as an "application layer" technology.
 - Great for email access, the "killer app"
 - IPSec VPNs are Network Layer connections
- *The Question: Even if the user connects, will IT have the ability to update this device?*

> A Look at Access Control (NAC)

- Initiatives by Cisco, Microsoft, and others
- Fundamental goal: Protect the network, not specifically the data or device
- Users must connect to the LAN (physically or through a VPN)
 - What if they gain Internet access only
- Addressing “baseline” problems
 - AntiVirus, AntiSpyware, Personal FW
 - Not all remediate, many just block the user
- The products do not address “the mobile blind spot” and their unique threats



> Mobile Device Visibility Is Very Important

- It's something most organizations can't do effectively
- The risks to those devices are greater while they are off the LAN
 - Users are off the LAN more than ever
- Business initiatives around data protection and regulatory compliance are focused on preventing disclosure
 - Existing processes must embrace the mobile environment
- Apathy is no excuse.
 - You can't wait for an event to occur first.

> Benefits of a More Mobile NAC Solution

- **Protects the corporate network**
 - Blocks non-compliant systems from connecting
- **Addresses the “mobile blind spot”**
 - Monitors, protects and updates mobile computers even when they don’t connect with the corporate LAN
 - Provides protection from start-up to shut-down, anywhere
- **Protects “data at rest” and “data in motion”**
 - Beyond firewalls: data encryption and backup & recovery if devices are lost or stolen
 - Device control and information protection to reduce the risk of internal threats
- **Real-time compliance reporting**
 - Audit trail provides visibility to The Blindspot

> Recommendation: A Phased Approach to Securing the New Insider Threat

Defend against network-based threats and phishing

- Zero-Day Protection
- Intrusion Prevention
- Anti-Spyware
- Anti-Virus
- Firewall

2

Defend against loss and theft (Data at rest)

- Data encryption
- Backup and recovery

3

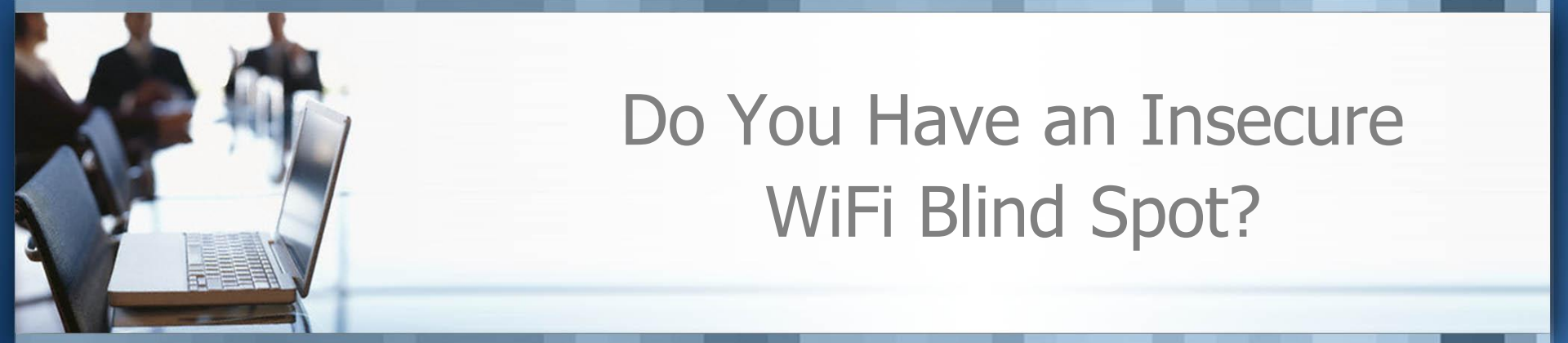

Defend against user policy violations (Incl. data in motion)

- Device control
- Information protection

4

1 Endpoint monitoring and remediation, patch management, vulnerability management, inventory management

Improve administration; Support other defenses



Do You Have an Insecure WiFi Blind Spot?

FIBERLINK

Simple. Secure. Mobility.

Securing WiFi

> Is it a False Sense of Security?

- Not all WiFi access points are the same
- Public access points don't want security
 - Too painful for the user to manage it
 - Desire simple connection only
- Even secure points are at risk
 - Home and office environments with WEP are exposed
 - 46% of companies still use WEP for securing WiFi
- How easy is it to break WiFi security?



A Short “Training” Video

FIBERLINK

Simple. Secure. Mobility.

> The Internet as a Hacking Source

The screenshot shows a Microsoft Internet Explorer browser window with the address bar containing the URL: `http://www.youtube.com/results?search_query=hacking+wep&search_type=`. The page displays the YouTube search results for "hacking wep".

YouTube - Broadcast Yourself. - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites RSS Print Mail News Groups

Address `http://www.youtube.com/results?search_query=hacking+wep&search_type=` Go Links >>

Google `Go` Bookmarks 156 blocked Check AutoLink AutoFill Send to Settings




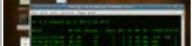
You Tube Broadcast Yourself™ [Sign Up](#) [QuickList \(0\)](#) [Help](#) [Log In](#) [Site:](#)

[Home](#) [Videos](#) [Channels](#) [Community](#)

hacking wep Videos Search [settings](#) [advanced search](#) [Upload](#)

"hacking wep" video results 1 - 20 of about 154

[Videos](#) [Channels](#) Sort by: [Relevance](#) Uploaded: [Anytime](#) Display:

	Hacking WEP Encryption WEP being hacked. MORE: hacks1010.webs.com...hacks hacks1010 hacking wep wpa tsk cell phone upload	Added: 3 months ago From: sloggyman83 Views: 4,234 ★★★★★ 01:47 More in Education
	IEFD ep. 2 - Wireless Hacking - Cracking WEP To download a High quality version visit our website, www.infinityexists.com...Cracking 128 bit WEP aircrack airodump aireplay hack hacking Infinity Exists (more)	Added: 10 months ago From: Gregorpm Views: 131,005 ★★★★★ 04:42 More in Howto & Style
	Hacking WEP by ĐăĐK Hacking WEP in anyone wireless network....kismet wireless wep aircrack hacking	Added: 1 year ago From: darkkill666 Views: 66,728 ★★★★★ 03:36 More in Sports
	Wireless WEP Key Hacking com For a Hacking Guide. This video	Added: 6 months ago From: jortex187

Copyright 2

Done Internet

at&t
better than flowers
Give mom a FREE* Nokia 6085 camera phone
Get a free phone
*Signif. restrict. apply

> All You Need to Break a WEP Key

Programs Used: (These are all free and easily downloaded online)

- Backtrack 2 Final- CD Bootable Linux Operating System with built in auditing/cracking tools
- Airodump- Captures wireless packets from access point
- Aireplay- Injects packets at the access point to create traffic and increase cracking speed
- Aircrack- Statistical algorithm to crack WEP 64/128 bit codes. Current version can crack 64bit in 2 minutes and 128bit in < 6.
- Aircrack-ng- Used to create an Evil Twin attack
- Ettercap- Man In the Middle Attacks, can also sniff data and

> 46% of Corporations Still Use WEP as a Standard

The reason is:

- > It takes time, money and resources to setup a better WLAN infrastructure
- > It takes time, money and resources to setup and manage the wireless client software
- > End-user machines utilize different WLAN hardware and software

Now There is a Blind Spot!

> Recommendations for WiFi Usage

- Use an enterprise-grade WLAN solution, such as PEAP (802.1x), that requires authentication
 - Verifies identity
- Do not broadcast the SSID of the WLAN
- Change default ADMIN usernames/pwds on all wireless hardware (access points)
- Ensure all systems have an active personal firewall
- Ensure all devices are current with patches and have AV and ASW running

> Summary: What's It All Mean To You?

- Increased mobility is creating new device and data threats
 - Insiders are becoming outsiders
- Mobile devices are the most vulnerable
- Implement security solutions that reach the “unconnected users” – the Mobile Blind Spot
- Data in motion exposures can occur maliciously or by accident
- Devices are exposed, with or without the Internet
- You will need a blended/layered approach with security
- An integrated NAC and Mobile NAC solution will provide the overall most compliant and secure solution



Thank You

Questions? STAYLOR@Fiberlink.com

FIBERLINK

Simple. Secure. Mobility.

> Use Cases For A Mobility Platform

- **Managing Compliance Initiatives**
 - Provides a comprehensive picture of:
 - Devices in and out of compliance
 - Reasons for falling out of compliance
 - Enforcement and remediation actions taken
- **Controlling the Costs of Mobility**
 - Visibility and analysis of 3G, WiFi and other user behavior
 - Cost and usage control
- **Protecting Company Data**
 - The data protection overview consolidates information from multiple applications into a unified status view
 - Encryption, Backup & Recovery, Data Leak Prevention
 - A view into the blind spot