

Why is Cyber Security a Problem

- Everything in society relies on computers and internet.
- What are risks?
 - danger of virus/malware erasing your entire system
 - altering files
 - stealing your credit cards
- What can you do?
 - Protect yourself by recognizing the risks



1

Confidential

Everything in our society is run by computers - think about it.

Many risks and they are increasing everyday with new ones

By recognizing the risks - you can better protect yourself - SCADA very vulnerable but they protect themselves by recognizing their vulnerabilities.

Emails and the Workplace

- Don't take candy from strangers.
 - don't believe everything you read on internet
 - Spoof emails
- Sounds too good to be true
 - You have just one million dollars! Wiper Winer Winer!
 - employment or business partner opportunities



2

Confidential

Commercial about young lady that believe everything on internet and blind date shows up and she says he's a French Model

Emails can be spoofed ie Walt Disney Case

Greedy people - Notice misspelling which is typical

- Re: From Hong Kong 29/09/2012.

Hello, my name is Mr. Andrew LIU from Hong Kong. I want you to be my partner in a business project of 44.5M USD. Please reply back via my private e-mail address for more details andrewliu45@aol.com Or andrewliu19@yahoo.com.hk Thank you. Mr. Andrew LIU



I received this email Sept 29th - again greed and offering money

Hoax or Urban Legend

- Hit man Scam
 - see handout
- DEA scam for online prescription
 - see handout
- Web site to check hoaxes
 - <http://urbanlegends.about.com/>
 - <http://www.snopes.com>
 - <http://www.truthorfiction.com/>
 - <http://www.symantec.com/avcenter/hoax.html>
 - <http://home.mcafee.com/VirusInfo/VirusHoaxes.aspx>
 - <http://www.google.com/>



4

Hit man - Every year this scam comes out notice the misspelling

DEA Scam = Got a call from legal secretary where a DDA went to bank to pay the fine.

Web sites you can check re scams and hoaxes = I like GOOGLE

Emails at the Workplace

- Hoax or Urban Legend Summary:
 - Don't believe everything you read on internet
 - Tragic consequences for not performing action
 - Promise of money or employment
 - Instruction on protecting you from a virus from anti virus company and will hold your computer hostage
 - Multiple spelling or grammatical errors



5

Confidential

You probably seen man^ variations of the scam emails

Anti virus companies that hold your computer hostage

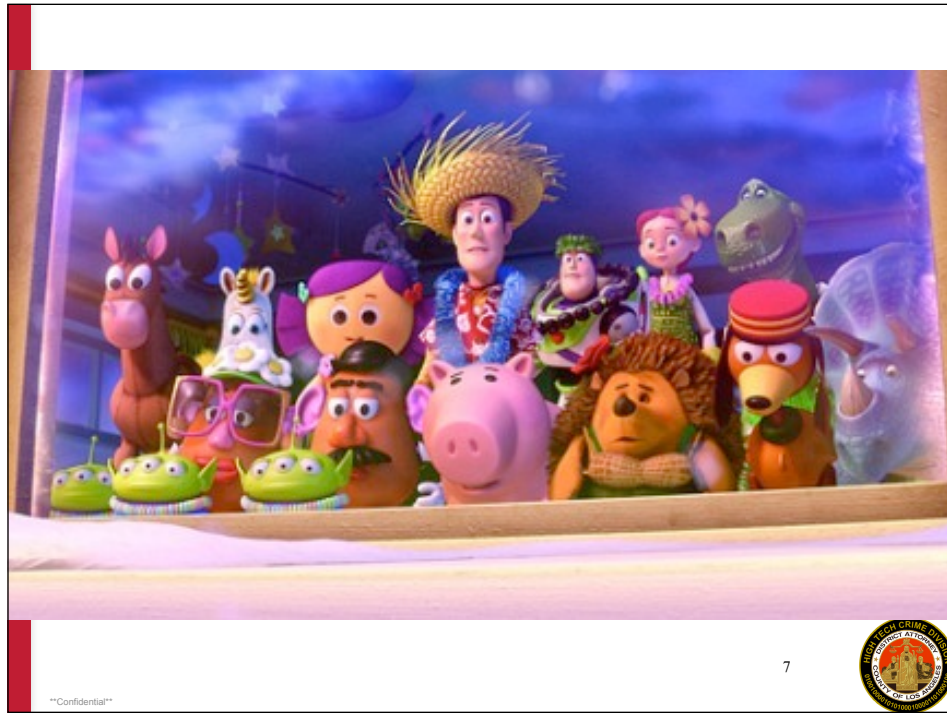
Emails at the Workplace

- Out of the Office or On Vacation
 - Do not advertise you are away
 - Suggestion: “I will not have access to email from (date) to (date)”



Auto reply that you are on vacation is similar to telling everyone in neighborhood you are away from house on vacation and there are several days of newspapers in driveway and your mail is busting out of the mailbox.

Setting yourself up for trouble



Confidential



Woody and friends at a leu au Aloha!

ON VACATION

- Do not use public WiFi at airports and coffee shops or hotels.
 - personal business
 - online banking
 - online shopping
 - online trading
- Cautious charging your phone
 - strange computers
 - USB charging stations at airports or hotels



8

Confidential

WiFi may not really be a WiFi and maybe not secure and someone is capturing all the packets

USB charging stations at airport - just saw one and better to use electrical charge

If use USB turn your phone off - Hackers

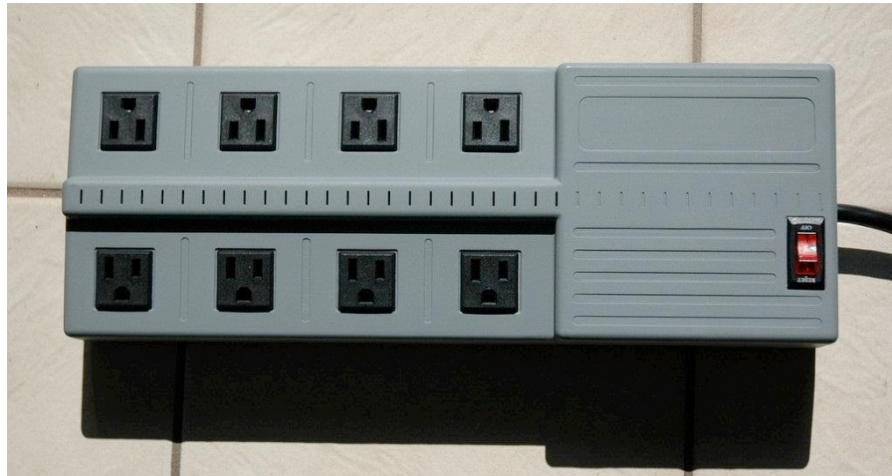
Hacking Devices



This was a usb charging station at DEFCON this year and people were warned that this could be a hacker - computer can be inside/ behind the metal facing.

Hackers can make hotel clock into a hacking device.

Hacking Device



10



this is a device that looks like a power strip - Power PWN

It is a Debian OS with metasploit (hacker tools) than is capable of performing penetration testing if placed inside a network.

Costs over \$1200. Wireless device

Hacking Device



11



Confidential

You can see some ports

Cell Phone Security

The screenshot shows the MobiStealth website with the following details:

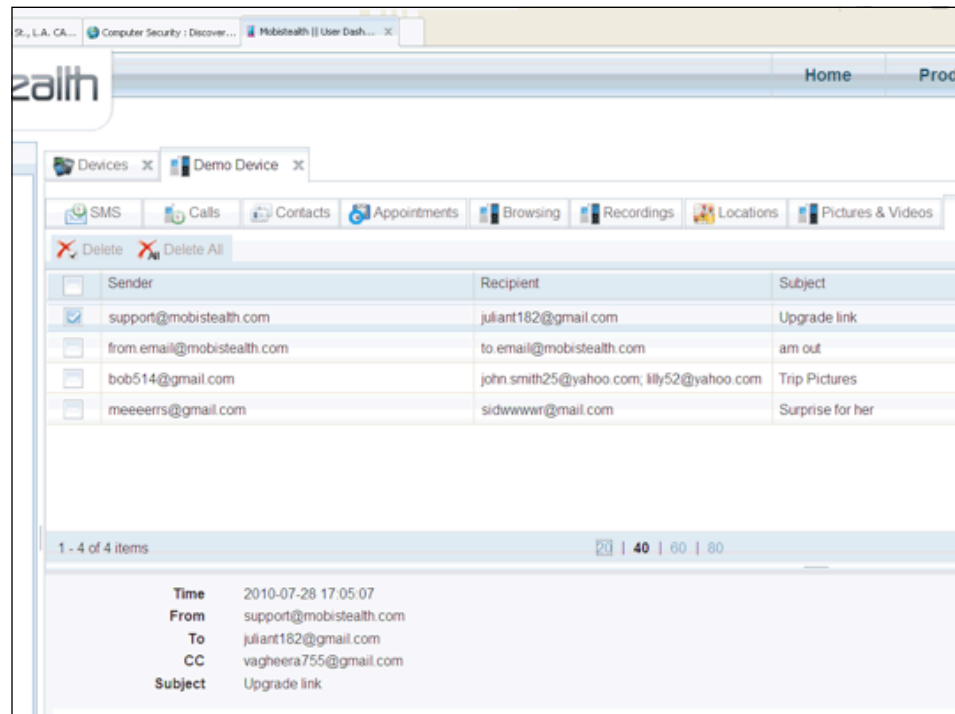
- Navigation:** Home, Mobile Phone Spy, Computer Monitoring, Reverse Phone Lookup, Affiliates, Demo, BUY NOW
- Media Coverage:** AS SEEN ON YAHOO! NEWS, Newsweek, PCWorld, WIRED, SFGate, msn
- Selected Product:** iPhone (change)
- Pricing:**

Plan	Price
Pro-X	As Low as \$12.00 per month
Pro	As Low as \$7.00 per month
Lite	As Low as \$7.00 per month
- Advanced Features:**
 - Blackberry Messenger Chat Logging
 - Email Logging ✓
 - Live Listening to Surroundings/Spy call ✓
 - Picture Logging ✓
 - Recording of Calls
- TESTIMONIALS:** "We have six dedicate outside sales reps after noticing sale"

MobiStealth software

All the Spy, are for phones typically need to have physical access & download and place spyware on the phone - do not leave your phone unlocked and unattended.

\$12 per month for the works

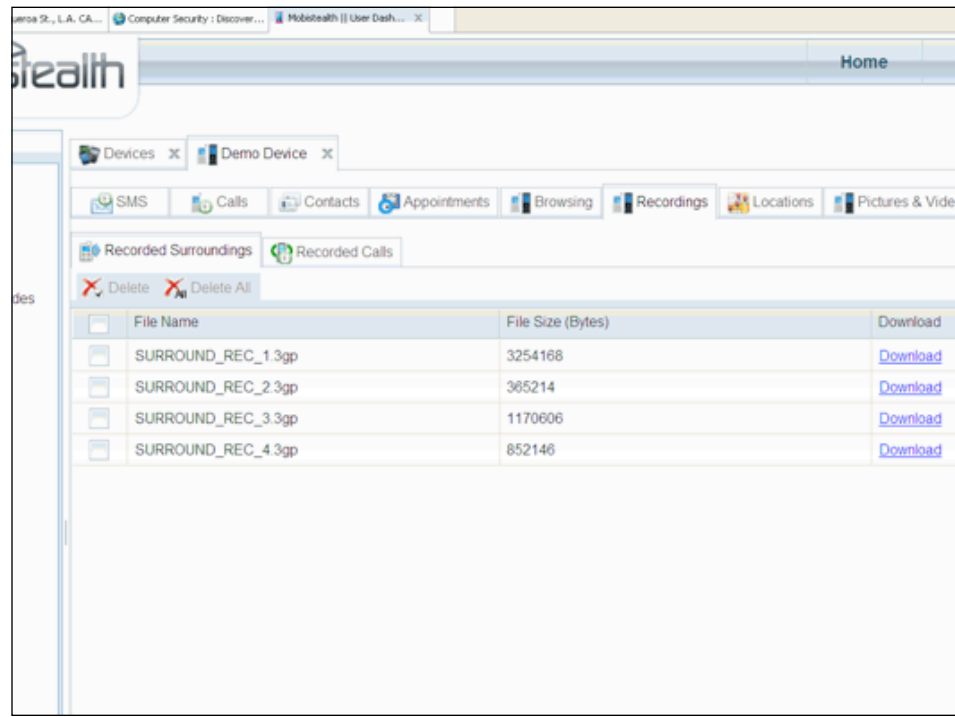


Person monitoring goes up on MobiStealth Web site and logs in
All EMAILS captured here

The screenshot shows a web-based interface for managing a mobile device. At the top, there are navigation tabs for 'Home', 'Products', and 'Ph'. A user greeting 'Hello! der' is visible. Below the navigation, there are tabs for 'SMS', 'Calls', 'Contacts', 'Appointments', 'Browsing', 'Recordings', 'Locations', 'Pictures & Videos', and 'Emails'. The 'Calls' tab is selected, and a 'Delete' button with a red 'X' icon is visible. The main content is a table of call logs with the following data:

Type	Contact Name	Contact Phone	Started
	Kameron	5151218631	2010-04-06 13:08:20
		1085450531	2010-03-15 13:04:30
	Marshall	0845565151	2010-02-23 13:20:38
	Gustavo	16165605648	2009-06-27 13:11:16
		2126734067	2009-02-23 12:09:36
	Elie	4048981804	2009-02-23 12:08:37
	Kely	4082264922	2009-02-23 11:53:05
	John	6172420949	2009-02-23 11:51:34

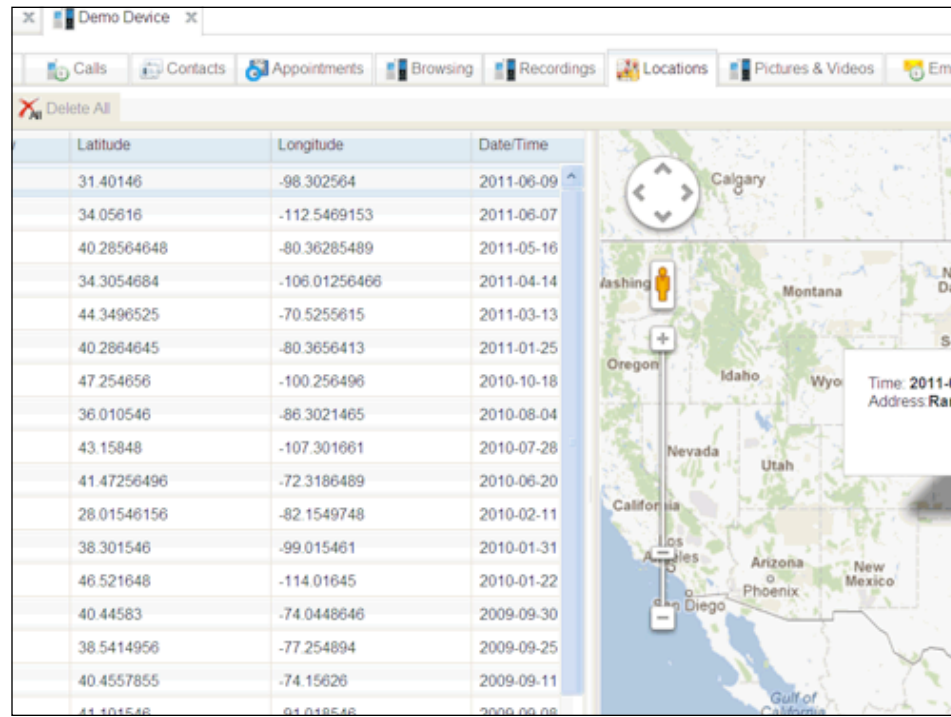
Call logs
incoming and outgoing



You can turn on recording on subject's cell phone and record

Type	Sender	Recipient	Text
	13345113030	26050620636	are you going to be working late again? i need to make dinner
	Julia	13345113030	first i need to drop some stuff off at home, ill prolly see u by nite
	16841205520	13345113030	yew r stoopid
	13345113030	81261046202	my boss is a jerk she needs to get a life and get wasted shes a life a living hell
		13345113030	me! i need to tk to u! something major happened!
	29233451151	13345113030	are we still on for tomorrow?
	13345113030	80453206566	PARTY TOMORROW! My parents are going to be out so i'm in lifetime bash! be there!
	0534105175	13345113030	that is HOT!!!!!!!
	65215465326	13345113030	I think I am failing my chem test :(
	98382005	13345113030	snd me a pic... i miss ur face
	13345113030	09058656053	my boss is a jerk she needs to get a life and get wasted shes a life a living hell

text messages



GPS location - Longitude and Latitude

track where you go

Secure your Cell Phone

- When not using your cell keep your cell phone locked with password
- Do not loan phone out
- Only takes a minute to download spyware
- Do not open attachments of people who you do not know
- Use Mobile Anti Virus



Confidential

Secure your phone

lock it when you are not using

Use Mobile Anti Virus

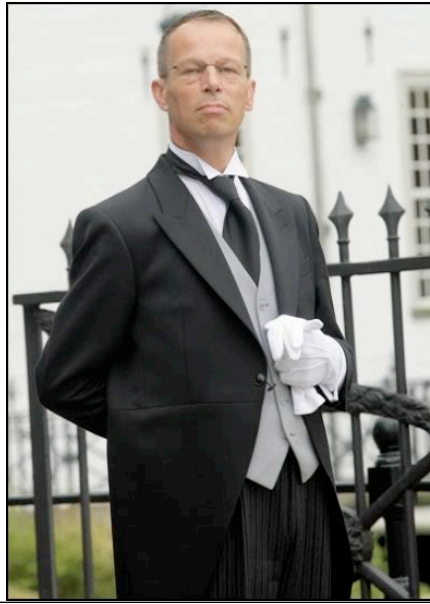


Blueguard Mobile Security - Lockout Premium -
Kapernsky Mobile Security

All very reasonable - Should catch any spyware on phone

File Server - Security Issues

- Butler did it!
 - “VatiLeaks” case in the Vatican Judicial System.
 - Paolo Gabriele
- People v. Heller



Confidential

Insiders:

Pope Benedict's long-time butler (Paolo Gabriele) was stealing vatican and papal documents - he was aided by an IT person within Vatican. On trial for "Aggravated Theft" in the Vatican Judicial System.

Heller Case Justin can give a quick briefing of investigation

File Server Security

- Permission
 - Groups
 - Read Write Execute Privileges
 - r (read) - file readable by owner, group or others
 - w (write) - file is writable (you can add or delete files)
 - x (execute) - run programs
- Vulnerability
 - If someone has access with full privileges to file server and also has access to internet.

21



Confidential

Need to have Share Points created with permission.

Common Myths

- Anti virus software and firewalls 100% effective.
- Once software installed on your computer, do not have to worry about it anymore.
- Nothing important on your computer so do not have to worry about security.
- Attackers only target people with money.
- When my computer slows down, it means that it is old

22



Confidential

Anti virus 100% effective - NO but together with anti virus and firewall - REDUCE RISK

Once Software Installed - UPDATE often security patches for software

Nothing Important on Computer - Financials (QuickBooks, Turbo Tax) PII, Bank Account Info, and Pictures

Attackers Only Target those with Money - ANYONE can be victim of ID Theft - want your PII - Breaches involve databases with PII.

My Computer SLOW - New Software or Operating System on OLD Machine - upgrade with more Memory - Processes running in Background (TASK MANAGER) files running in background.

Thank You!

Confidential

