



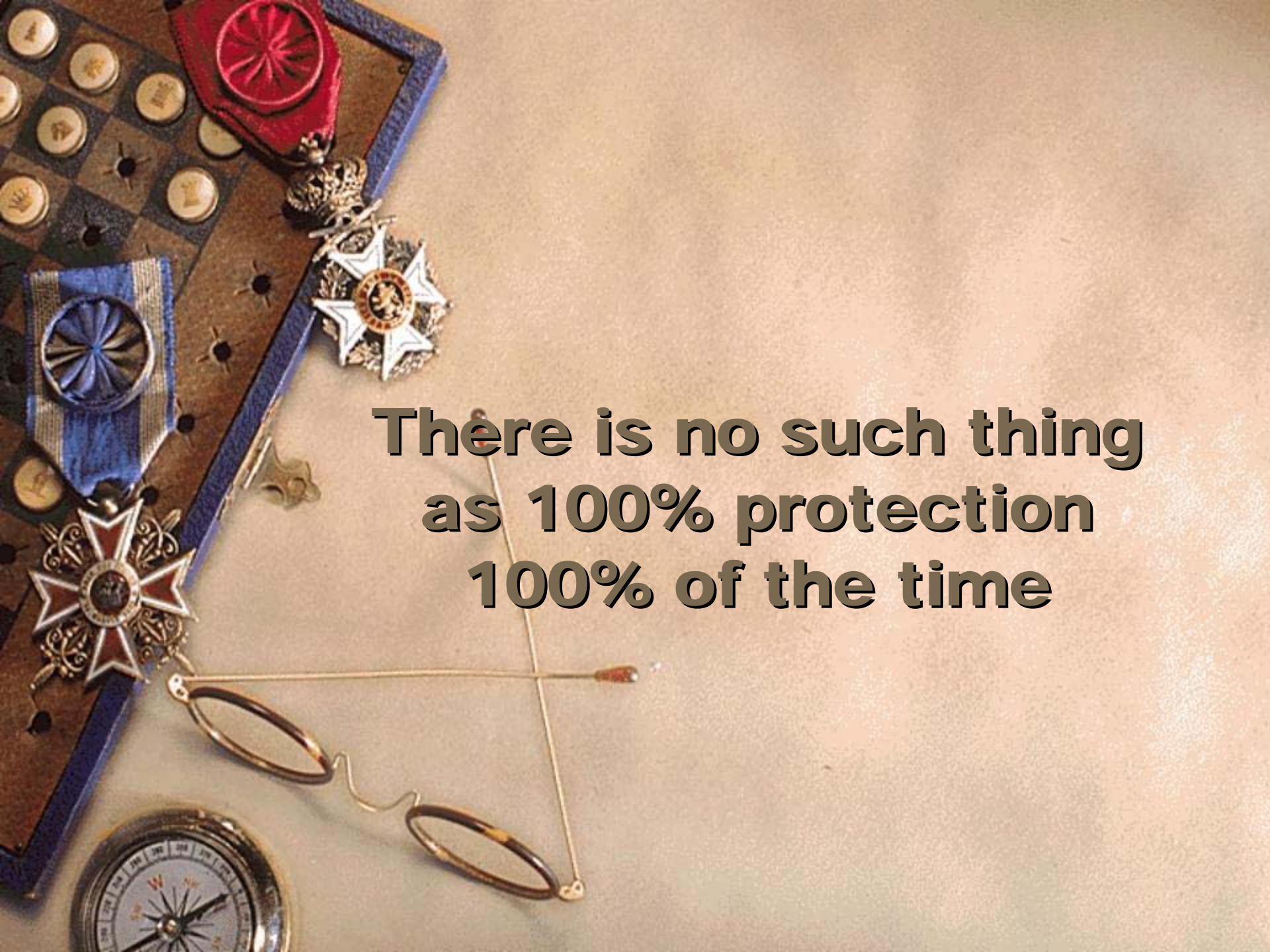
Hackers: Changing the Face of ID Theft

**Elaine Bryskar
Temecula Valley
Computer User Group**



The Headlines Shout...

- ◆ **Freeloaders tap into peril**
 - Press Enterprise: 5/12/06
- ◆ **Thieves peer into digital homes**
 - Press Enterprise: 11/27/06
- ◆ **Look for danger signs when shopping online**
 - Press Enterprise: 11/27/06
- ◆ **Personal data gets onto mailing labels**
 - LA Times: 12/31/06

A collection of military medals and a compass are arranged on a wooden surface. On the left, a blue ribbon with a circular emblem is pinned to a wooden board with a checkered pattern. Below it is a large, ornate silver star-shaped medal with a central emblem. To the right, another similar star-shaped medal is pinned to the board. A pair of gold-rimmed glasses lies horizontally across the lower part of the scene. In the bottom left corner, a circular compass is visible, showing cardinal directions and degree markings. The background is a plain, light-colored surface.

There is no such thing
as 100% protection
100% of the time

Let's Talk About...

◆ The past

- Unsecured wireless networks
- Botnets
- Vishing
- RFID



Let's Talk About...

- ◆ **The present**
 - Security Bloopers
 - Medical ID Theft
 - Child ID Theft
 - Cyberstalking





Let's Talk About...

- ◆ **The future**

- Cyborgs

- ◆ **What can we do?**

But first, some statistics

Conducted by the Consumer Reports National Research Center, reported in September, 2006 issue. (National Incidences)

◆ **SPAM**

- 1 in 2 experienced high levels of spam

◆ **Viruses**

- 1 in 4 had major problems
 - Cost per incident: \$109
 - Total damage: \$5.2 billion





Some statistics (cont)

◆ **Spyware**

- 1 in 8 had major problems
 - Cost per incident: \$100
 - Total damage: \$2.6 billion

◆ **Phishing**

- 1 in 115 lost money from an account
 - Cost per incident: \$850
 - Total Damage: \$630 million

Internet ID Theft





Example of Internet ID Theft

- ◆ Imagine a phony website targeting pet owners
- ◆ Site users register with a name, address, password
- ◆ Thief visits 10 bank websites using name, password (gets a hit)
 - **Most people use same password for all their accounts ☺ BINGO!!!**

The Past



Wireless Networks





Unsecured wireless networks

Freeloaders tap into peril

- ◆ **Press Enterprise: 5/12/06**
- ◆ **Last year, Jupiter Research found about 14.3 million households nationwide had wireless networks**
- ◆ **That number is expected to more than triple over the next four years**
- ◆ **Based on an earlier study, which found that 1/3 of home wireless networks are left unsecured, a large percentage of those networks are likely to be unsecured**

Unsecured Wireless Networks

◆ So what??

- ◆ **What if someone is piggybacking on your connection**
 - Slows your system down by overusing your connection
 - Accesses your files
 - Accesses someone else's files
- Or just
 - Does something illegal?
 - Starts hacking, spreads a virus?
- ◆ **This is tracked back to your computer**
- ◆ **And what's worse, they may catch your viruses, Oh my...**





Wireless Network Solution

- ◆ **www.wi-fi.org for more tips**
- ◆ **www-dcn.fnal.gov/DCG-Docs/mac for basic illustrated instructions**
- ◆ **Encrypt and password protect your network**
- ◆ **Use MAC filtering**
- ◆ **Change admin password**
- ◆ **Get latest security (WPA2)**
- ◆ **Change SSID settings**

Botnets





Botnets

- ◆ Microsoft sees botnets as top cyberthreat
 - ◆ PC World: 12/26/06
- ◆ **Remote-controlled PCs that have been taken over without their user's knowledge or permission**
- ◆ **Symantec counted more than 4.5 million of them during the first 6 months of the year**
- ◆ **It has been stated that botnets are the backbone of today's cybercrime**
- ◆ **Number one source of spam over past year**



Botnets

- ◆ **Botnet hacker admits computer crime**
 - ◆ Press Enterprise: 1/14/06
- ◆ **20-year old seized control of hundreds of thousands of Internet-connected computers**
- ◆ **Used a zombie network to serve pop-up ads**
- ◆ **Rented the network to those who mounted attacks on websites and sent out spam**



Botnets

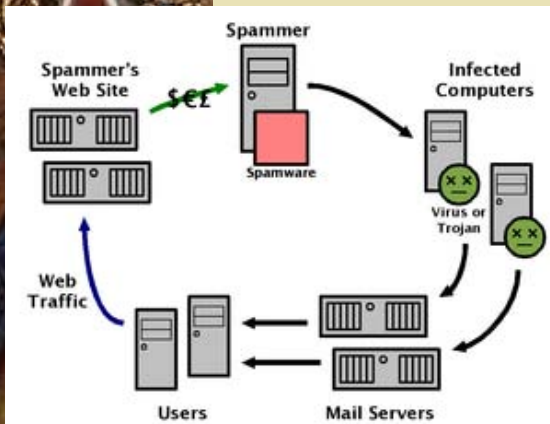
- ◆ **Botnet hacker admits computer crime (cont)**
 - ◆ Press Enterprise: 1/14/06
- ◆ **Advertised network of “bots” in chat rooms**
- ◆ **Web site maintained schedule of fees for renting botnet**
- ◆ **Site contained guidelines on how many bots required to bring down a website**

Botnets

Zombies try to blend in with the crowd

- ◆ C|net News.com: 10/19/06
- ◆ Criminals make money by networking their zombies into a “botnet”
- ◆ Used to

- Extort money from businesses
- Host fake websites in phishing scams
- Relay spam
- Load adware and spyware on compromised systems





Botnets and Wireless

- ◆ **Thieves peer into digital homes**
 - ◆ Press Enterprise: 11/27/06
- ◆ Last month BBC conducted an investigation into home computer security
- ◆ Using WinXP and no additional virus software
 - **Within seconds was computer attacked**
 - **Attacks continued every 15 minutes**
 - **Attacked by a program to attack other computers**
 - **Ports were scanned**



Botnets and Wireless

- ◆ **Thieves peer into digital homes (cont)**

- ◆ Press Enterprise: 11/27/06

- ◆ **Example Attack**

- ◆ Tax software prompts you to save return as a .pdf file
- ◆ Child installs music-sharing software incorrectly, sharing drive
- ◆ Hacker has music-sharing software and searches drive for “tax return” or “.pdf”



Botnets and Wireless

- ◆ **Thieves peer into digital homes (cont)**
 - ◆ Press Enterprise: 11/27/06
- ◆ **Symantec, in its September report, stated that 86% of all targeted attacks against computers are now directed at home users**
- ◆ **Yet about 80% of those using electronic devices on a home network don't activate the safety features**



Botnets / Wireless Solution

- ◆ **Be sure your anti-virus signatures, OS updates, and adware software are up-to-date.**
- ◆ **Turn on all safety features.**

Vishing



Vishing

- ◆ Short for “voice phishing”
- ◆ Uses VoIP
- ◆ Technology disguises true location
- ◆ Caller ID device may list legitimate looking U.S. phone number
- ◆ May use “automated dialing programs” to “cold-call” victims



Vishing (cont)


- ◆ Prerecorded message (or live “employee”) claiming account is compromised
- ◆ Request for account number, password, or other private info
- ◆ Request for three digit security code on back of card





Vishing (cont)

- ◆ **According to a March, 2006 article in New Money Magazine**
- ◆ FTC recently brought charges against a Costa Rica-based company that sold bogus franchises for investments between \$18,000 to \$85,000 using VoIP to appear as if operating from New Mexico.



Vishing Solution

- ◆ Hang up
- ◆ Call your bank using the phone number on the back of your card
- ◆ Banks will not request identifying information. They already have it
- ◆ Don't trust a number based on the area code. Con artists can hack into Caller ID systems

The Present and Near Future



RFID





RFID Microchip Devices

- ◆ Radio frequency identification
- ◆ Miniscule microchips (half the size of a grain of sand) which listen for a radio query and respond by transmitting their unique code. No batteries. Use power of initial radio signal for transmission.



RFID Chip Implants

◆ Current uses

- Animal identification
- Used by Walmart for inventory control
- Restrict entry to high-security areas
- Toll booth access (automatic deduction)
- **To be used shortly in passports**



RFID Chip Implants (cont)

- ◆ Patrons of VIP Baja Beach Clubs in Barcelona and Rotterdam can have a microchip injected into their arms to get access to VIP lounges and get drinks without waiting in line.



RFID Chip Implants

◆ **Future Uses**

- Implanted in ill patients (i.e., Alzheimer/Parkinson's patients) for quick access to complex medical records
- Tracking sex offenders
- Track easily disoriented Alzheimer's patients

A collection of military medals and a pair of glasses are arranged on a light-colored, textured surface. On the left, a blue and white checkered ribbon bar is visible, with several circular medals pinned to it. Below the ribbon bar, a large, ornate silver star-shaped medal with a central emblem is displayed. To its right, another similar star-shaped medal is pinned to the surface. A pair of gold-rimmed glasses with thin temples lies horizontally across the lower part of the scene. In the bottom left corner, a circular compass rose is partially visible. The text "Security Bloopers" is overlaid in the center-right area of the image.


Security Bloopers



Security Bloopers

Spyware infection prompts McDonalds MP3 recall
theregister.co.uk, 10/16/06

- ◆ **McDonalds Japan launched recall after discovering that MP3 players, preloaded with ten tunes, offered as a prize, were also loaded with a variant of the QQpas spyware program**
- ◆ **It transmits web passwords and other sensitive info to hackers**
- ◆ **Up to 10,000 people may have been affected**




Security Bloopers

Sony BMG settles anti-piracy program case

Press Enterprise, 12/20/06

- ◆ **Sony BMG will pay \$1.5M plus thousands more in customer refunds to settle lawsuits in CA and TX over music CDs that installed a hidden anti-piracy program (rootkit) for copy-protection on consumer computers.**
- ◆ **The program contained a security hole for hackers, and removal damaged computer systems.**




Security Bloopers

Report finds Medicare flaws

Press Enterprise, 10/8/06

- ◆ **The Government Accounting Office say they have found serious computer flaws that could lead to improper disclosure of sensitive medical information on people enrolled in Medicare and Medicaid.**




Security Bloopers

Report finds Medicare flaws (cont)

Press Enterprise, 10/8/06

- ◆ **GAO stated that Medicare would not necessarily know if a security breach had occurred because they had no “audit trail” to document use of computer network or detect intrusions.**



Security Bloopers

Market a common link in debit card breaches

LA Times, 10/28/06

- ◆ **“About 40 debit-card users in Huntington Beach area had money stolen from their bank accounts...”.**
- ◆ **“...the cards had been used at a Ralphs supermarket...”. Thieves accessed bank accounts and several banks were affected through ATMs.**

Security Bloopers

Market a common link in debit card breaches (cont)

LA Times, 10/28/06

- ◆ **“We are noticing more and more card and PIN numbers offered for sale in chat rooms,” said a spokesman for Cardcops.com, which investigates card fraud for businesses.**



Medical ID Theft





Medical ID Theft

ID Theft infects medical records

LA Times: 9/25/06

- ◆ **A 2003 federal report estimated that at least 200,000 ID theft cases involved medical identity fraud.**
- ◆ **Victims may find clearing their medical records of bad information more difficult than fixing credit reports**




Medical ID Theft

ID Theft infects medical records (cont)

LA Times: 9/25/06

- ◆ **Hospital bill collectors demanded patient pay for amputation of her right foot after shoulder surgery last year**
- ◆ **She sent notarized photos of her foot, with toes attached**
- ◆ **An ID thief had obtained medical care under her name and sent bill to her insurer**
- ◆ **A year later, she is still catching medical errors and clearing fraudulent hospital bills**




Medical ID Theft Redux

Your medical records stolen

Reader's Digest: November 2006

- ◆ **In March, 2004 a man got a collection notice from a billing agency for a hospital in Denver**
- ◆ **He had never set foot in that hospital**
- ◆ **Someone with his name and SSN had been admitted for surgery**
- ◆ **Two years later, he is still trying to clear his credit rating and doesn't know if his medical records have been cleared of errors**



Medical ID Theft Redux

Your medical records stolen (cont)

Reader's Digest: November 2006

- ◆ **Medical theft involves using your name to receive**
 - Drugs
 - Expensive medical treatment
 - Fraudulent insurance payouts
- ◆ **Erroneous medical history becomes part of your record, and hard to fix**
 - Information spread among multiple providers
 - Can lead to denial of insurance coverage
 - Keep you from getting a job
 - Lead to injury or death
 - HIPAA may block you from seeing your own records since they contain another's history



Medical ID Theft

Thieves peer into digital homes

Press Enterprise: 11/27/06

- ◆ Major electronics companies like Intel and Philips are now pursuing home health care, with devices that can
 - **monitor a person at home**
 - **Relay information to doctors and family**
 - **And eventually dispense medications and diagnose the onset of diseases, including Alzheimer's and Parkinson's disease**



Medical ID Theft

Firms push new benefit

Press Enterprise: 12/7/06

- ◆ **Five of the nations largest employers to give workers their very own electronic medical record**
 - Take when they travel
 - When change jobs
 - See a new doctor
- ◆ **Simplify process, reduce paperwork**



Medical ID Theft

Firms push new benefit (cont)

Press Enterprise: 12/7/06

- ◆ **Third-party company will gather info from insurers, pharmacists, doctors, other health-care providers**
- ◆ **Companies will have no access or control over the data base**
- ◆ **Patients will be able to update their records**



Medical ID Theft Solution

- ◆ Treat insurance card like a credit card
- ◆ Watch out for “freebies”
- ◆ Read the EOB
- ◆ Check your benefits yearly
- ◆ Request an accounting of disclosures
- ◆ Review your credit report

Child ID Theft





Child ID Theft

Cases soar of children victimized by ID theft

Press Enterprise: 12/6/06

- ◆ **FTC says id theft complaints involving youngsters under 18 have nearly doubled since 2003 – up from 6,512 to more than 11,600 last year.**
- ◆ **Most victimized age is 18-29 – 29% - more than 70,200 cases.**



Child ID Theft

Cases soar of children victimized by ID theft (cont)

Press Enterprise: 12/6/06

- ◆ **Sixth straight year that identity theft has topped the annual report on consumer-fraud complaints filed.**
- ◆ **Fraud complaints filed: from 246,847 in 2004 to 255,500 last year.**



Child ID Theft

Children identity theft

Readers Digest: March/06

- ◆ **Seventeen-year-old identity stolen by estranged father**
- ◆ **Denied first credit card when applied**
- ◆ **Father racked up tens of thousands of dollars from various merchants and vendors and declared bankruptcy in his son's name.**



Child ID Theft

Children identity theft (cont)

Readers Digest: March/06

- ◆ **Identity Theft Resource Center in San Diego estimates that at least 400,000 child identities were stolen in 2005.**



Child ID Theft Solution

When theft of child's identity is suspected

LA Times: 12/25/05

- ◆ **You will need to write to the credit bureaus, and include**
- ◆ **Child's birth certificate listing you as parent**
- ◆ **Child's SSN**
- ◆ **Copy of driver's license**
- ◆ **Bill showing current address**
- ◆ **Cover letter with child's full name and address for last 5 years**

Cyberstalking





Cyberstalking

Spyware that stalks

Consumer Reports, September 2006

- ◆ **DOJ survey: 1 in 4 say have been physically abused by intimate partner**
- ◆ **Such abuse is often preceded by stalking, increasingly taking electronic form**

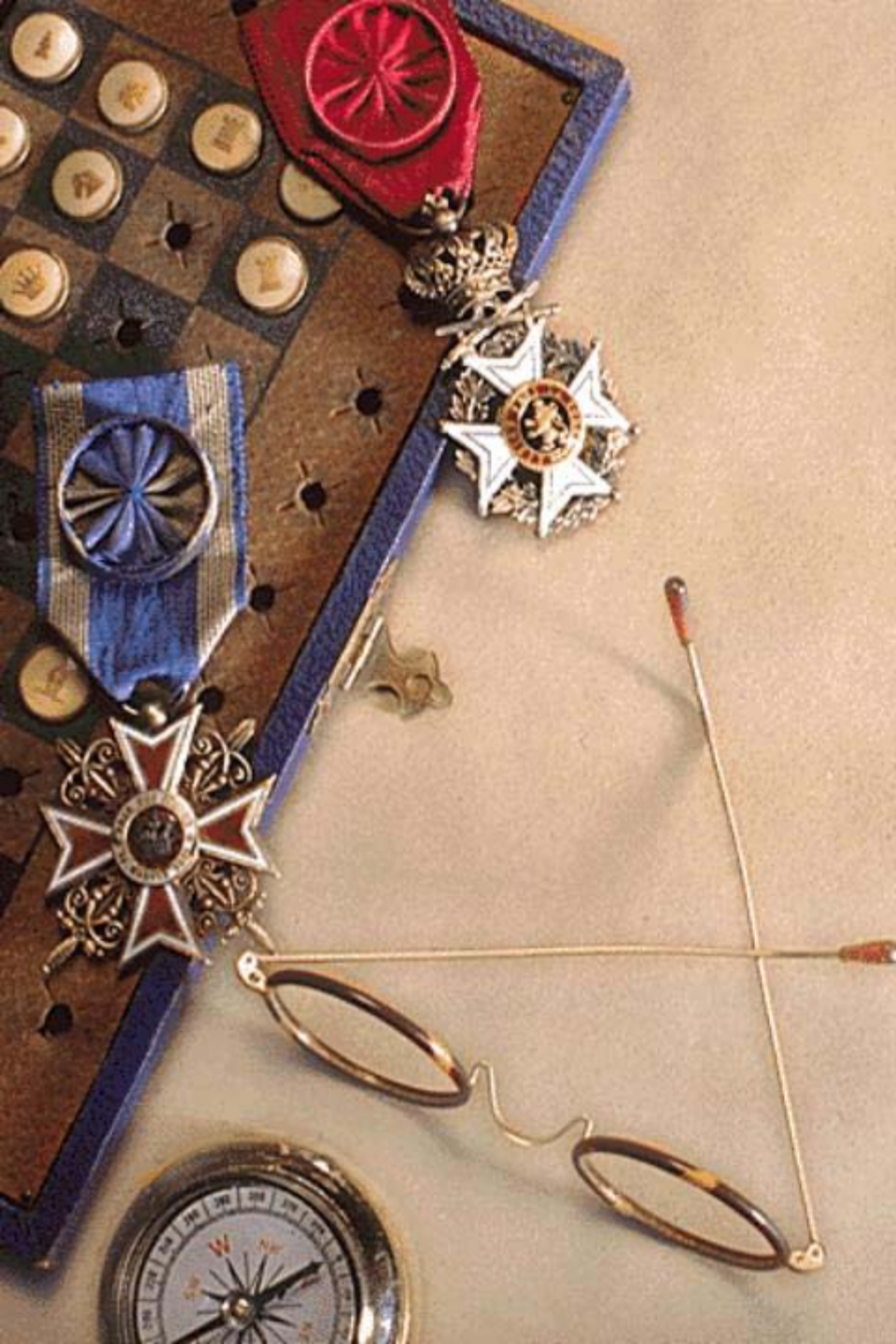


Cyberstalking

Spyware that stalks (cont)

Consumer Reports, September 2006

- ◆ National Network to End Domestic Violence surveyed more than 680,000 homes nationally. They project harassment or harm to someone by a person monitoring activities using spyware on computer



The Future

Cyborgs




Cyborgs

We'll all be cyborgs, scientist says

Press Enterprise: 12/24/06

- ◆ **In 1998, Kevin Warwick, cyberneticist at the Univ. of Reading, England, had a chip surgically implanted into his left arm. The chip announced his presence to computers.**
- ◆ **Office doors swing open, lights flick on, computer says hello, tells number of email waiting.**






Cyborgs

We'll all be cyborgs, scientist says (cont)

Press Enterprise: 12/24/06

- ◆ **In 2002, Warwick had a newer device implanted which connected to median nerves, linking nervous system to computer.**
- ◆ **He moved his hand, the signals went over the Internet to open and close a robotic hand. The hand contained sensors and grasped a sponge or a glasses case.**




Cyborgs

We'll all be cyborgs, scientist says (cont)

Press Enterprise: 12/24/06

- ◆ **Warwick experienced it as signals in his brain.**
- ◆ **Possible applications include helping paralyzed people regain some movement, sensing tremors in people with Parkinson's disease and signaling the brain to stop them.**
- ◆ **Six to 7 years away: attempting thought communication – “brain-to-brain communication”, he said.**



Cyborgs: This just in...

- ◆ **Robot rights?**
 - ◆ Press Enterprise: 1/2/07
- ◆ **Published by the U.K. Office of Science and Innovation, a British government paper, released last month, contains “a proposal to extend rights and entitlements such as healthcare, equal protection of the laws and even government pensions to machines...”.**

Cyborgs: A Thought...

- ◆ I wonder if the day will come when a woman can kick back and relax. Her cyborg, (password-protected, of course) is programmed to cook, clean, do laundry, change diapers, and all that stuff.
- ◆ Will she need to be concerned that hackers will infiltrate her cyborg, and create a botnet with the other cyborgs for some nefarious purpose?
- ◆ And will she need to submit a W-4 to the IRS?



What Else Can
We Do?



Online Shopping Dangers





Online Shopping Dangers

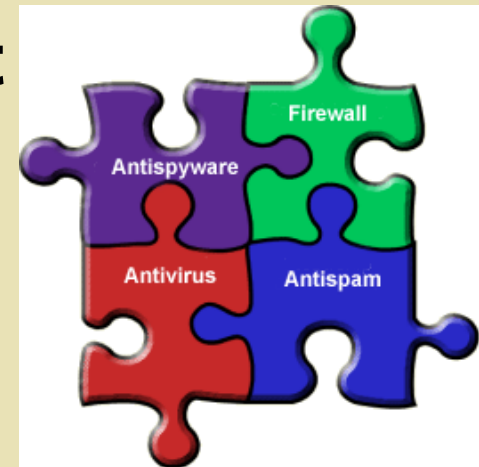
- ◆ **October survey found one in 10 adults victimized by fraud**
Press Enterprise: 11/27/06
- ◆ **Online shoppers spent more than \$32 billion for purchases last November and December.**
- ◆ **Don't use unencrypted or open wireless network**
 - **Secure before you shop**

Online Shopping Dangers

- ◆ **October survey (cont)**

Press Enterprise: 11/27/06

- ◆ **Look for certificate from Verisign or other similar organization**
- ◆ **Be sure antivirus, anti-spyware, firewall, OS current**



Online Shopping Dangers

◆ **October survey (cont)**


Press Enterprise: 11/27/06

- ◆ **Look for security signs**
 - **https:// or shttp://**
 - **Look for padlock in status bar**
 - **Double-click lock; verify same address as in address bar**
 - **Verify address under File/Properties**
 - **Properties should state SSL/encryption**
- ◆ **Use an anonymizer**



Websites of Internet





Websites of Interest

- ◆ **Identity Theft Resource Center**

- idtheftcenter.org

- 858.693.7935

- ◆ **Privacy Rights Clearinghouse**

- privacyrights.org/identity.htm

- ◆ **AARP**

- www.aarp.org

- 800.424.3410

- ◆ **Better Business Bureau**

- www.bbb.org



Websites of Interest

- ◆ **Consumers**

- www.consumer.gov/idtheft/con_resources.htm

- ◆ **Equifax**

- www.equifax.com

- 888.766.0008

- ◆ **Experian**

- www.experian.com

- 800.311.4769

- ◆ **Trans Union**

- www.transunion.com

- 800.680.7289



Who To Contact for Fraud

- ◆ **California State Attorney General**
 - ag.ca.gov/consumers/general.php
 - 800.952.5210
- ◆ **National Fraud Information Center/Internet Fraud Watch**
 - www.fraud.org
 - 800.876.060
- ◆ **Federal Trade Commission**
 - www.ftc.gov
 - 877.FTC.HELP
- ◆ **Internet Crime Complaint Center**
 - www.ic3.gov