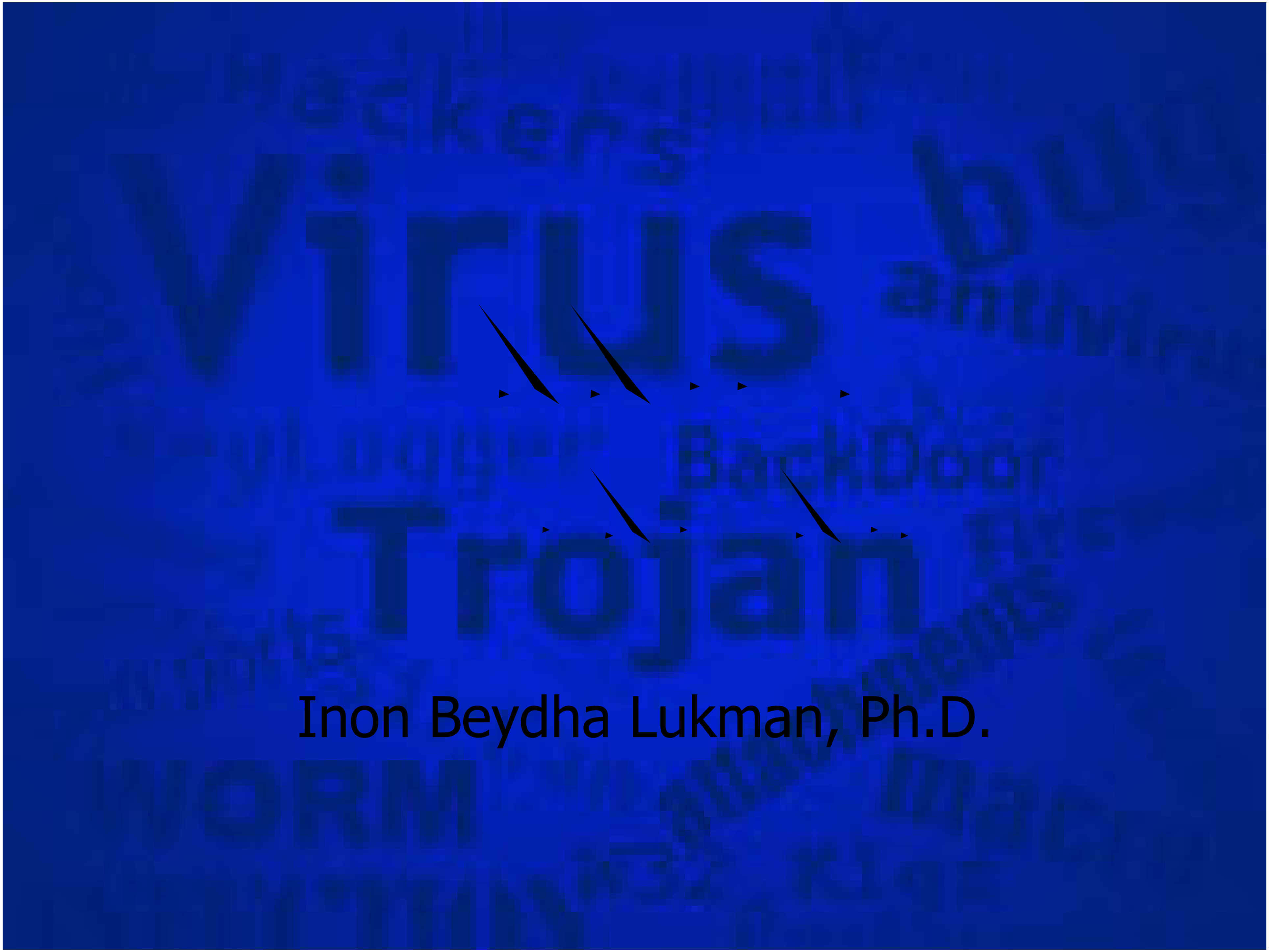


Inon Beydha Lukman, Ph.D.

INFORMATION SYSTEMS SECURITY

A discipline that protects the

☺**C**onfidentiality,

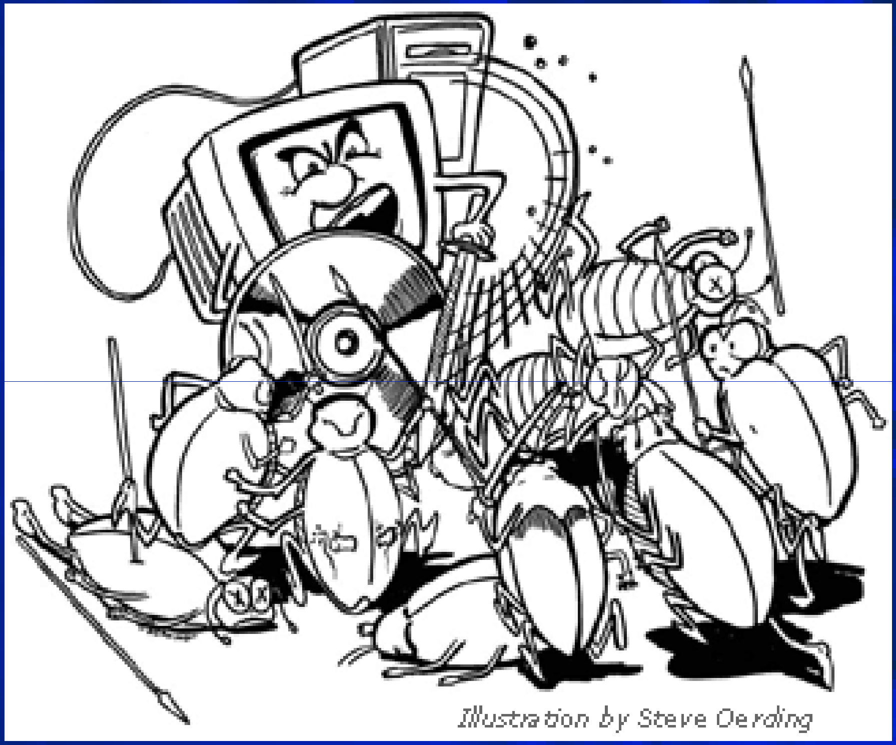
☺**I**ntegrity and

☺**A**vailability

of information and information services

aka: Network Security, Computer Security, Information Assurance, Cyber Warfare

Cyber Warfare



Sides have been taken:

By June 2006, 180,292 unique computer viruses had been identified. **

There are approximately 150-250 new viruses identified every month *

* Source: Cybercrime by Steven Furnell (2002) p 154

** Source: (2006) www.sophos.com

Threats: Illicit Activities

Hackers: enjoy intellectual challenges of overcoming software limitations and how to increase capabilities of systems

Crackers: illegally break into other people’s secure systems and networks

Cyber Terrorists: threaten and attack other people’s computers to further a social or political agenda

Motivation for Hackers:

☺The challenge… ‘because it’s there!’

☺Ego

☺Espionage

☺Ideology

☺Mischief

☺Money (extortion or theft)

☺Revenge

From Cybercrime by Steven Furnell (2002) p 55

21 January 2003

Two years jail for UK virus writer who infected 27,000 PCs

Simon Vallor, the twenty-two year old web designer from North Wales who, in December 2002, pleaded guilty to writing and distributing three computer viruses, was today sentenced at Southwark Crown Court, London to a two year custodial sentence. His viruses - Gokar, Redesi and Admirer – were proven to have infected 27,000 PCs in 42 countries.

"Vallor's actions were comparable to those of a vandal gaining illegal entry to businesses across the world and then interfering with thousands of their PCs. His sentence reflects the severity of his crime and it's reassuring to computer users that the UK courts are treating cybercriminals on a par with more traditional offenders," said Graham Cluley, senior technology consultant, Sophos Anti-Virus. "Around 800 new viruses are cropping up each month - this level of activity requires a lot of virus writers. Perhaps Vallor's sentence will focus some minds and make virus writers think twice before unleashing their malicious code."

Source: www.sophos.com

Threats:
Illicit Activities

Malware Writers: responsible for the creation of malicious software

Samurai: hackers hired to legally enter secure computer/network environments

‘Phreakers’: Focus on defeating telephone systems and associated communication technologies

Threats:
Illicit Activities

- ‘Phishing’: sending out ‘scam’ e-mails with the criminal intent of deceit and extortion
- Spam: unsolicited and/or undesired bulk e-mail messages, often ‘selling’ a product (See also SPIM – targeting of instant messaging services)
- Zombie Computers: Yours?

Real Time Analysis

Spam

Zombie BotNets

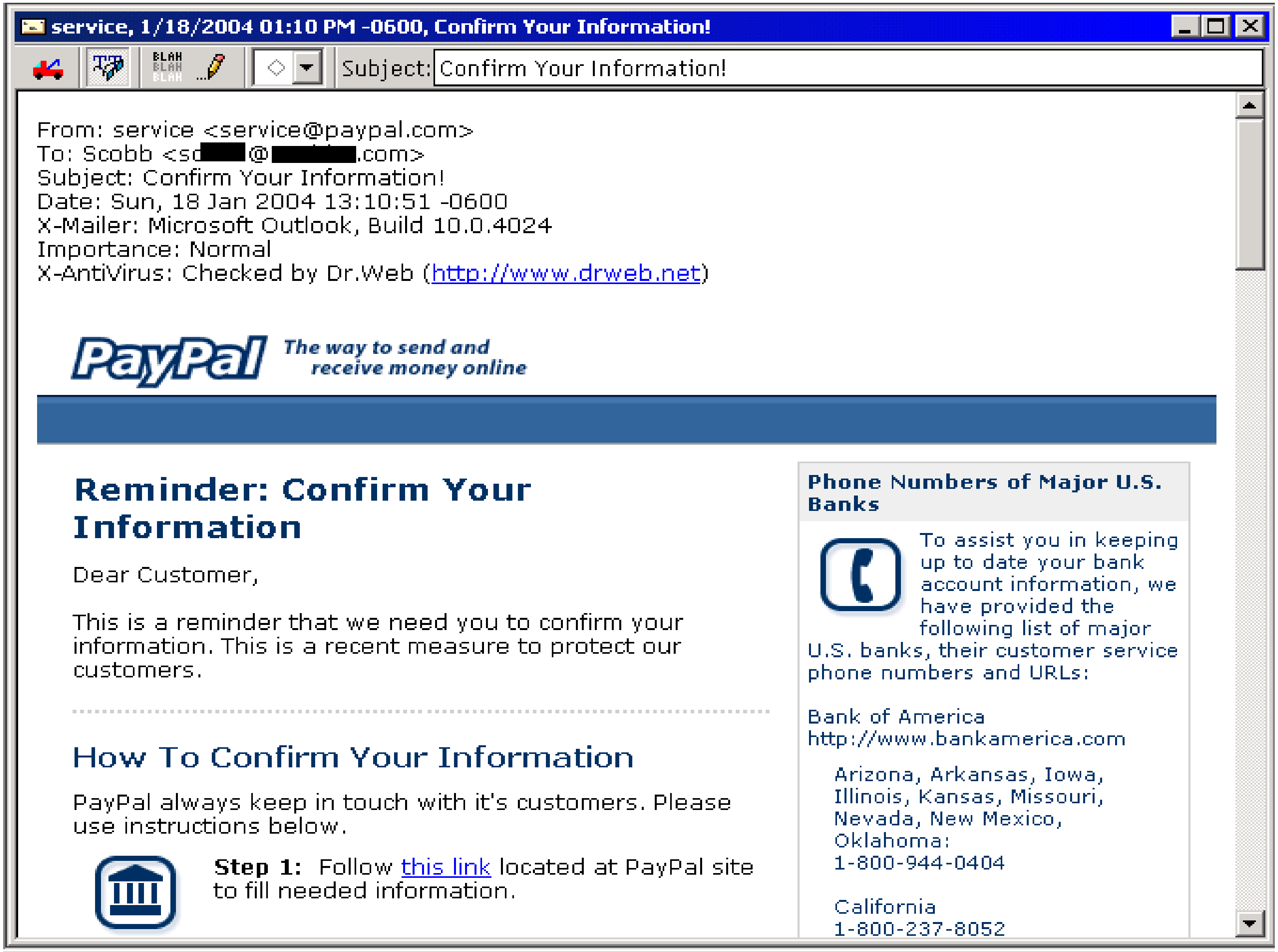
Botnet is a jargon term for a collection of software robots, or ‘bots, which run autonomously. This can also refer to the network of computers using distributed computing software.

While the term "botnet" can be used to refer to any group of bots, the word is generally used to refer to a collection of compromised machines (zombies) running programs, usually referred to as worms, Trojan horses, or backdoors, under a common command and control infrastructure. A botnet's originator (aka "bot herder") can control the group remotely, and usually for nefarious purposes such as the sending of mass spam.

Source: www.wikipedia.org

Phishing

Phishing is a technique used by strangers to "fish" for information about you, information that you would not normally disclose to a stranger, such as your bank account number, PIN, and other personal identifiers such as your National Insurance number. These messages often contain company/bank logos that look legitimate and use flowery or legalistic language about improving security by confirming your identity details.



service, 1/18/2004 01:10 PM -0600, Confirm Your Information!

Subject: Confirm Your Information!

From: service <service@paypal.com>
To: Scobb <sd[redacted]@[redacted].com>
Subject: Confirm Your Information!
Date: Sun, 18 Jan 2004 13:10:51 -0600
X-Mailer: Microsoft Outlook, Build 10.0.4024
Importance: Normal
X-AntiVirus: Checked by Dr.Web (http://www.drweb.net)

PayPal *The way to send and receive money online*

Reminder: Confirm Your Information

Dear Customer,

This is a reminder that we need you to confirm your information. This is a recent measure to protect our customers.

How To Confirm Your Information

PayPal always keep in touch with it's customers. Please use instructions below.

Step 1: Follow this link located at PayPal site to fill needed information.

Phone Numbers of Major U.S. Banks

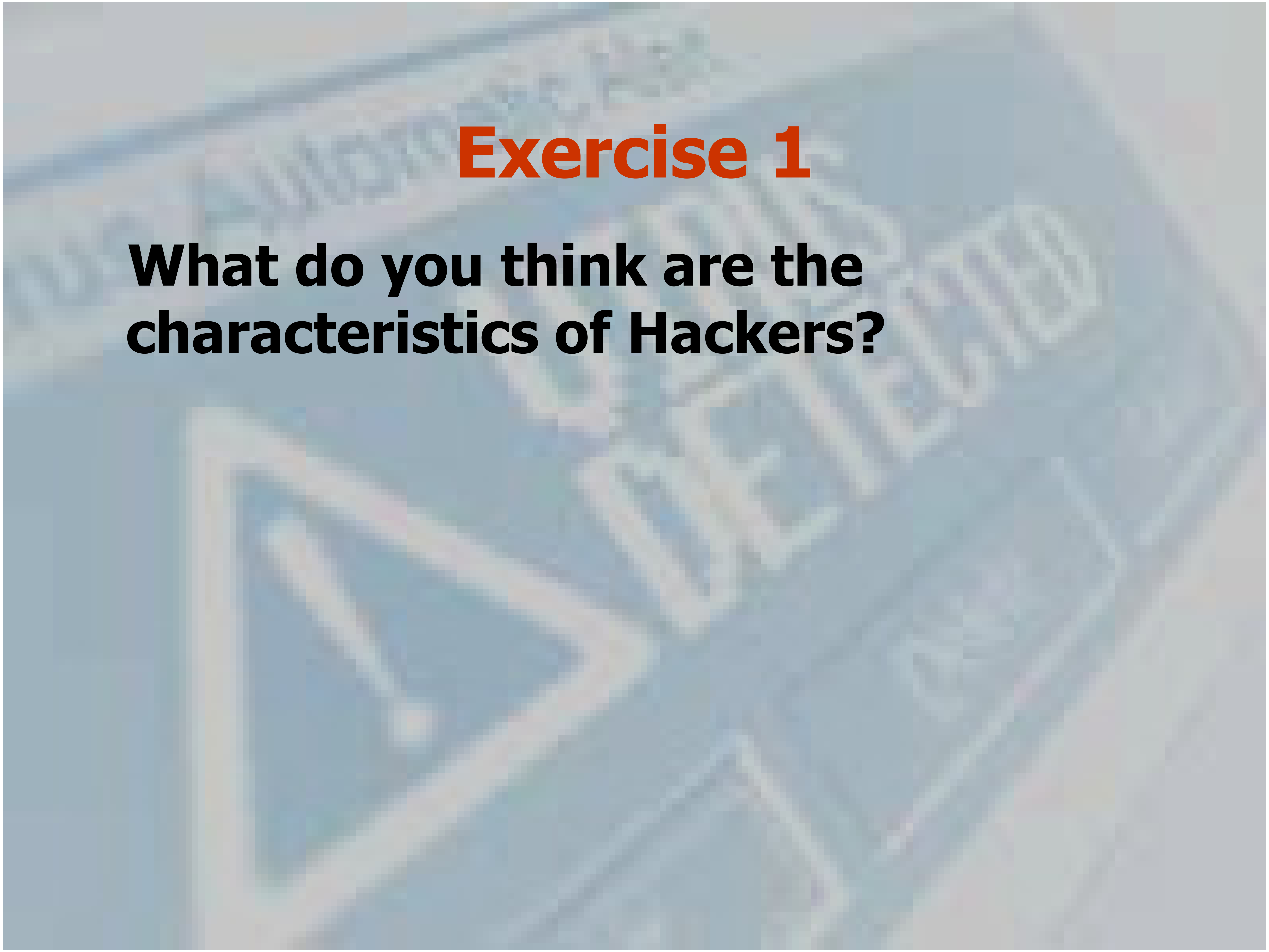
To assist you in keeping up to date your bank account information, we have provided the following list of major U.S. banks, their customer service phone numbers and URLs:

Bank of America
http://www.bankamerica.com

Arizona, Arkansas, Iowa, Illinois, Kansas, Missouri, Nevada, New Mexico, Oklahoma:
1-800-944-0404

California
1-800-237-8052

Phishing example



Exercise 1

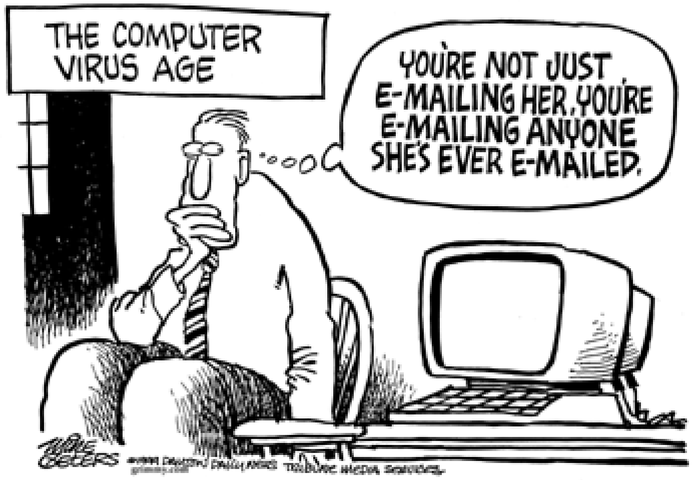
What do you think are the characteristics of Hackers?

Hacker Characteristics

- ☺Predominantly male
- ☺Aged from mid-teens to mid-twenties
- ☺Lacking in social skills
- ☺Fascination or obsession with computers
- ☺Underachiever in other areas who sees computing as a means of being important or powerful

Source: Cybercrime by Steven Furnell (2002) p 47

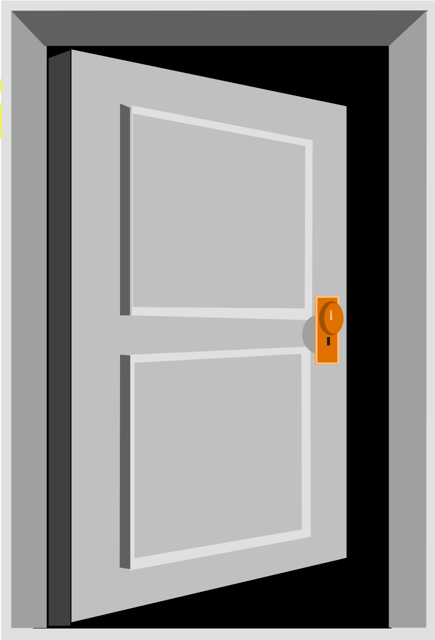
Threats: MALWARE


THE COMPUTER VIRUS AGE
YOU'RE NOT JUST E-MAILING HER, YOU'RE E-MAILING ANYONE SHE'S EVER E-MAILED.
MIKE PETERS
DAYTON DAILY NEWS TRIBUNE MEDIA SERVICES

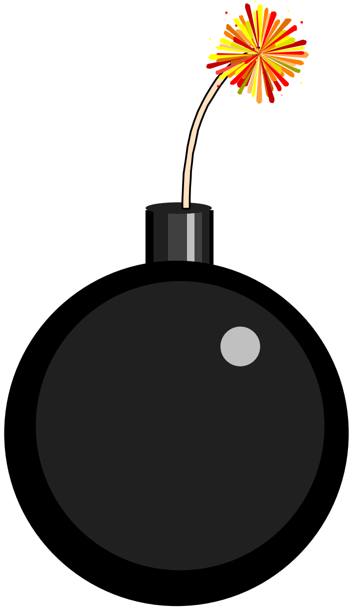
Malware Types

Malware Types

Malware Types

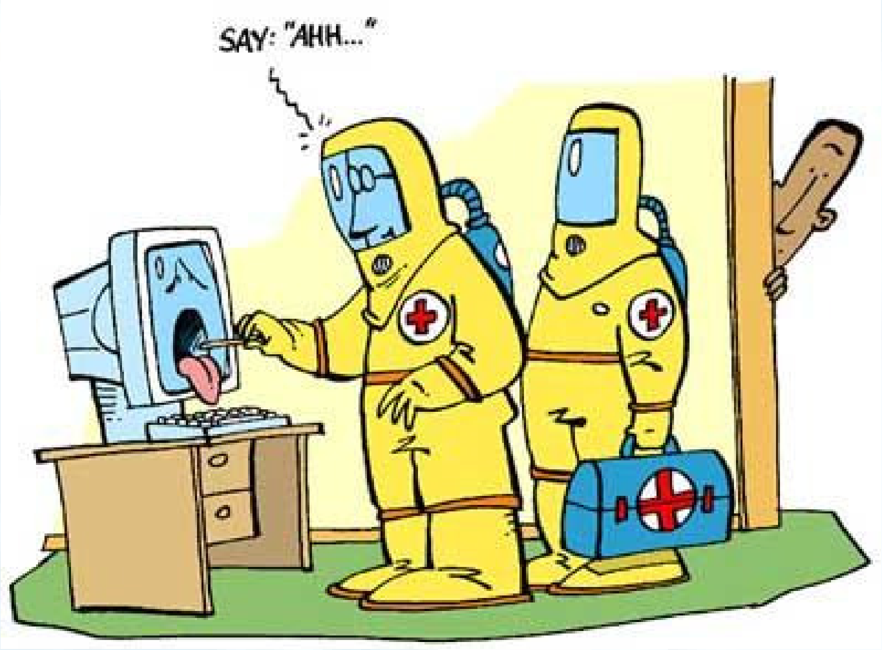


Malware Types



Exercise 2

What do you think motivates Malware writers to create and unleash these attacks?



Malware Writer Motivations

- ☺To see how far the virus can spread
- ☺To cause damage and destruction to a targeted individual or organisation
- ☺To achieve a feeling of superiority/power
- ☺To leverage some form of personal gain
- ☺To provide a ‘lesson’ in Internet security
- ☺To conduct an experiment

Source: Cybercrime by Steven Furnell (2002) p 150

Threats:
DEFACING WEBSITES

Hackers can leave their ‘graffiti’ on other people’s websites. Many sites have fallen foul of this activity:

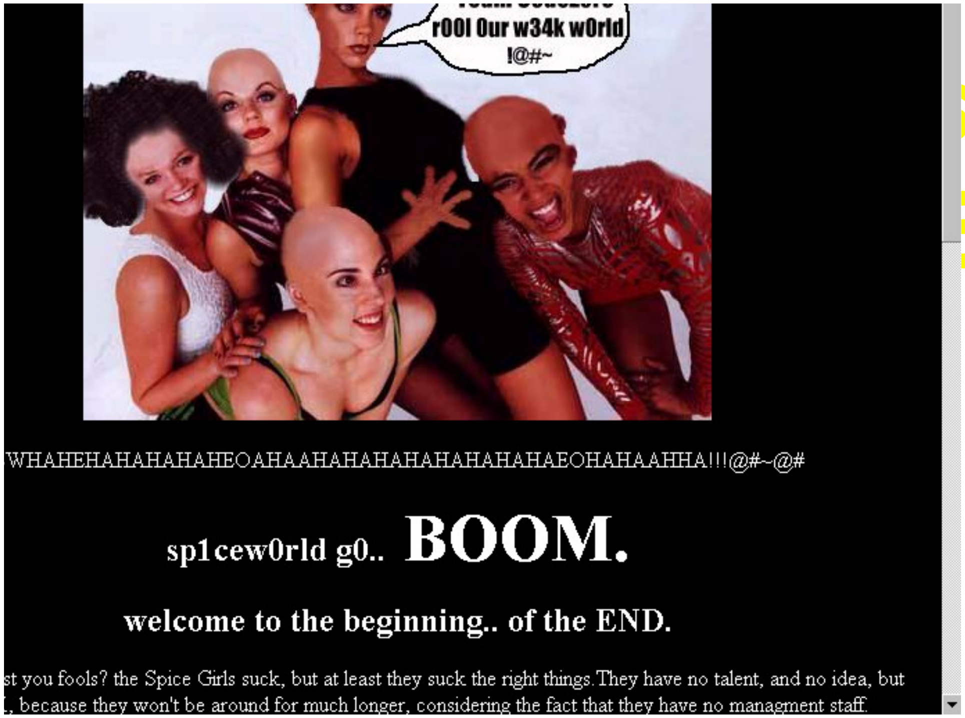
☺FBI and CIA

☺NASA

☺British Labour and Conservative Parties

☺New York Times

S:
EBSITES



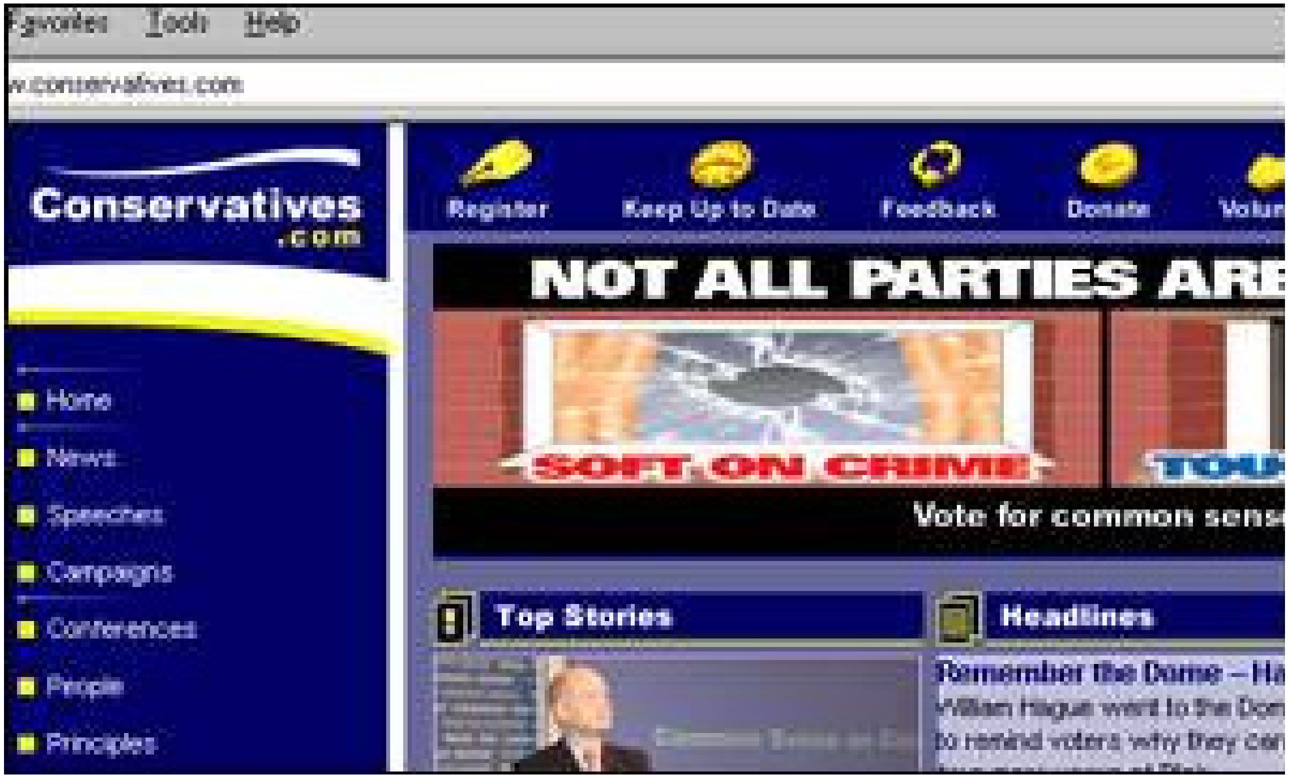
WHAHEHAHAHAHAHEOAHAAHAHAHAHAHAHAHAHAHAEOHAHAAHHA!!!@#~@#

sp1cew0rld g0.. **BOOM.**

welcome to the beginning.. of the END.

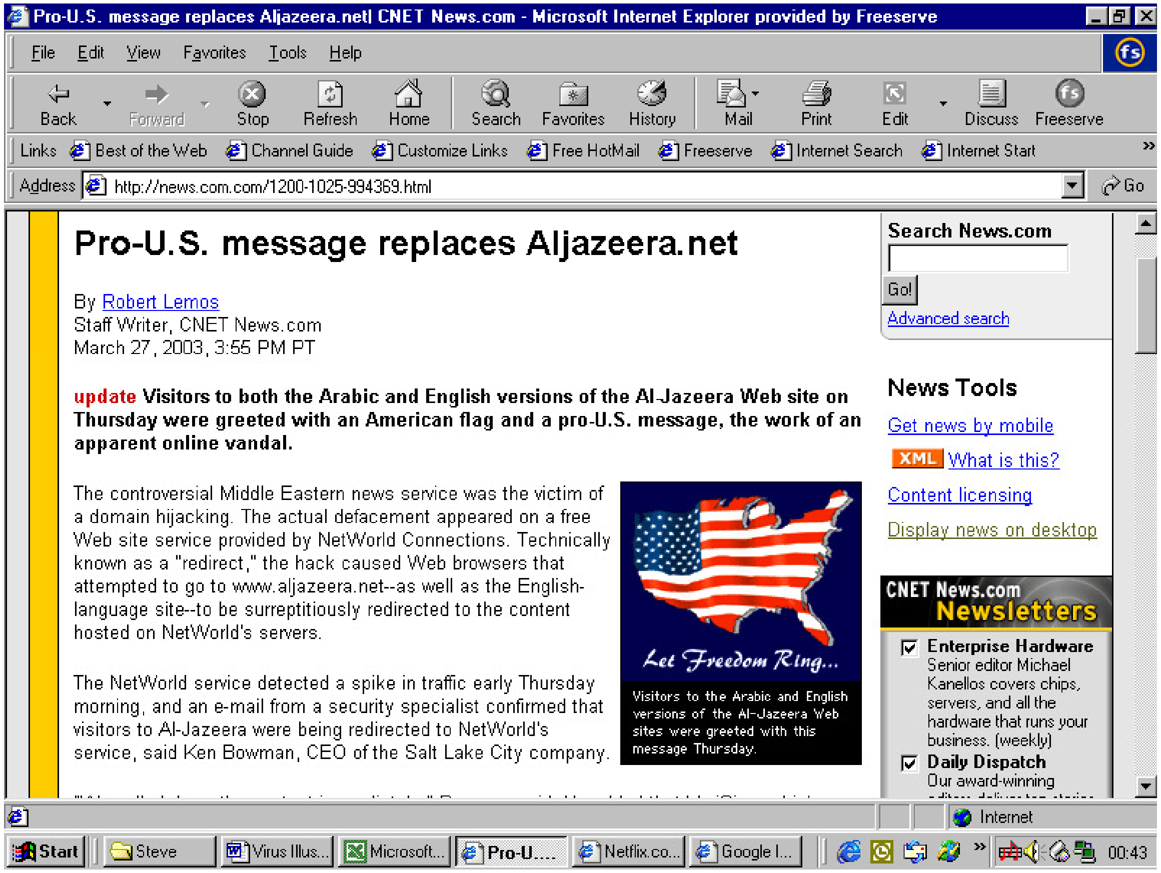
st you fools? the Spice Girls suck, but at least they suck the right things.They have no talent, and no idea, but
, because they won't be around for much longer, considering the fact that they have no managment staff.

Threats:
DEFACING WEBSITES



Remember the Dome – Ha
William Hague went to the Dom
to remind voters why they can

Threats:
DOMAIN HACKING


Pro-U.S. message replaces Aljazeera.net| CNET News.com - Microsoft Internet Explorer provided by Freeserve
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss Freeserve
Links Best of the Web Channel Guide Customize Links Free HotMail Freeserve Internet Search Internet Start
Address http://news.com.com/1200-1025-994369.html
Go
Search News.com
Go!
Advanced search
News Tools
Get news by mobile
XML What is this?
Content licensing
Display news on desktop
CNET News.com Newsletters
Let Freedom Ring...
Internet
Start
Steve
Virus Illus...
Microsoft...
Pro-U....
Netflix.co...
Google I...
00:43

Pro-U.S. message replaces Aljazeera.net

By Robert Lemos
Staff Writer, CNET News.com
March 27, 2003, 3:55 PM PT

update Visitors to both the Arabic and English versions of the Al-Jazeera Web site on Thursday were greeted with an American flag and a pro-U.S. message, the work of an apparent online vandal.

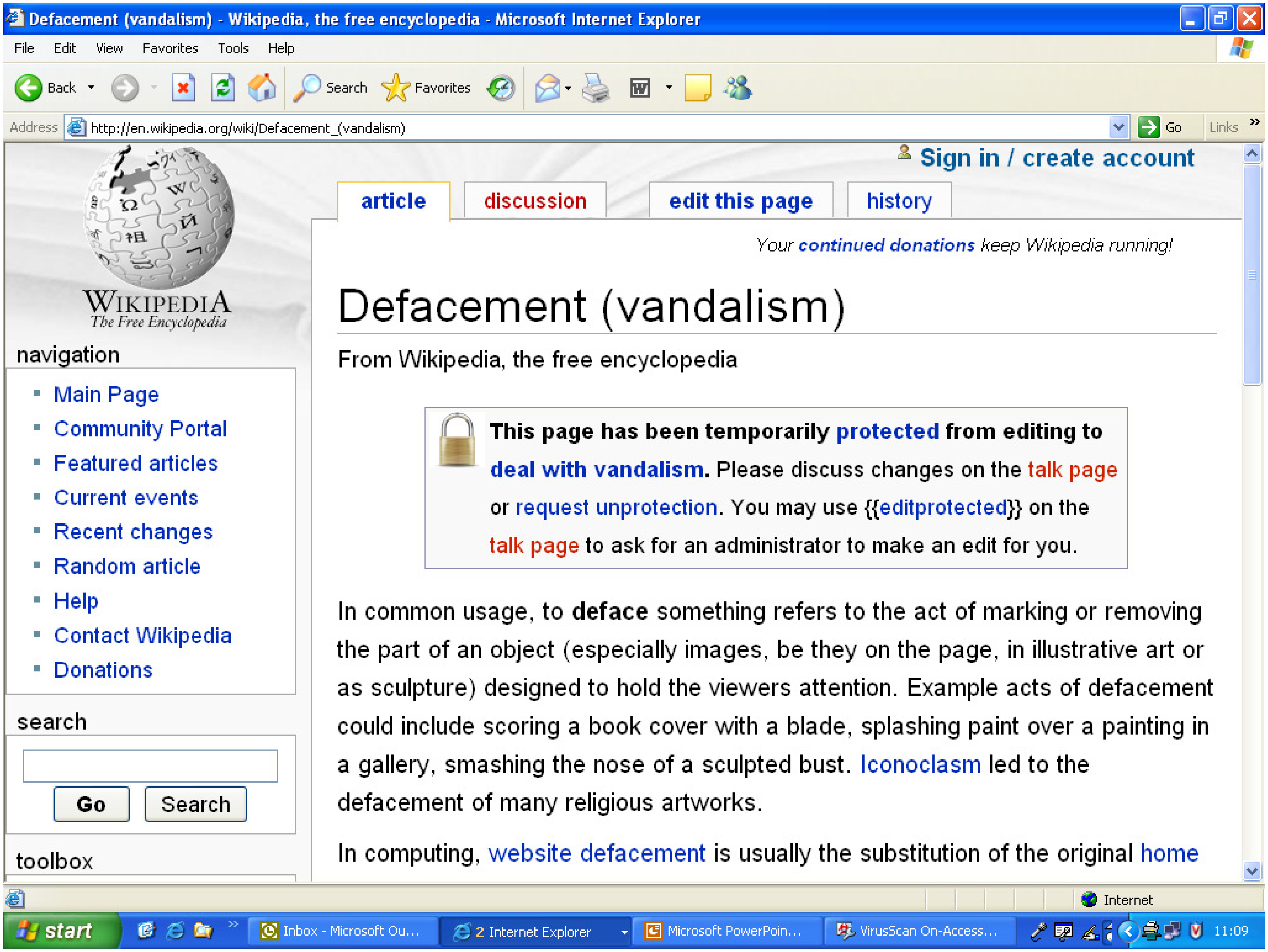
The controversial Middle Eastern news service was the victim of a domain hijacking. The actual defacement appeared on a free Web site service provided by NetWorld Connections. Technically known as a "redirect," the hack caused Web browsers that attempted to go to www.aljazeera.net--as well as the English-language site--to be surreptitiously redirected to the content hosted on NetWorld's servers.

Visitors to the Arabic and English versions of the Al-Jazeera Web sites were greeted with this message Thursday.

The NetWorld service detected a spike in traffic early Thursday morning, and an e-mail from a security specialist confirmed that visitors to Al-Jazeera were being redirected to NetWorld's service, said Ken Bowman, CEO of the Salt Lake City company.

☑ **Enterprise Hardware**
Senior editor Michael Kanellos covers chips, servers, and all the hardware that runs your business. (weekly)

☑ **Daily Dispatch**
Our award-winning



Your ***continued donations*** *keep Wikipedia running!*

Defacement (vandalism)

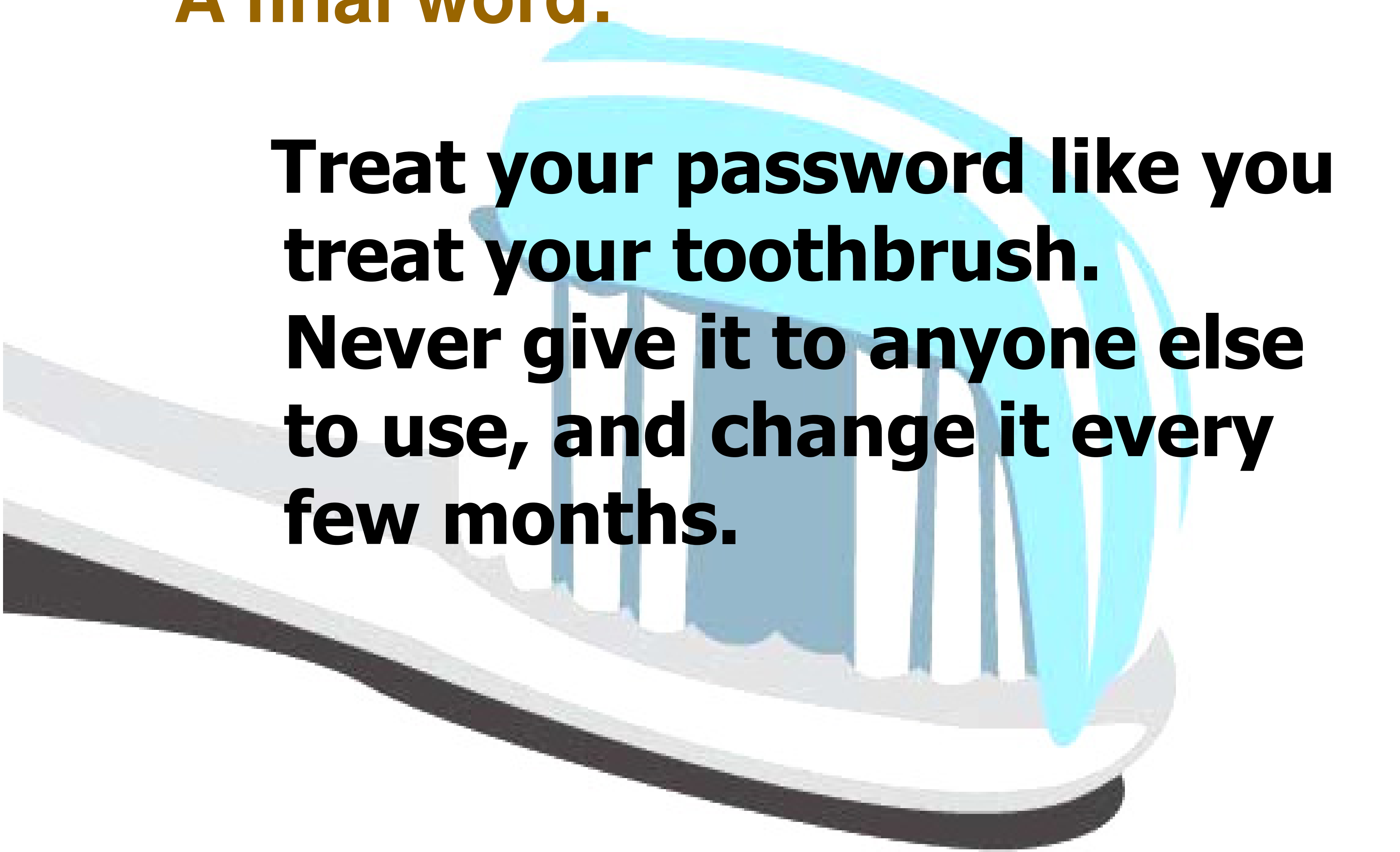
From Wikipedia, the free encyclopedia

This page has been temporarily protected from editing to deal with vandalism. Please discuss changes on the talk page or request unprotection. You may use {{editprotected}} on the talk page to ask for an administrator to make an edit for you.

In common usage, to **deface** something refers to the act of marking or removing the part of an object (especially images, be they on the page, in illustrative art or as sculpture) designed to hold the viewers attention. Example acts of defacement could include scoring a book cover with a blade, splashing paint over a painting in a gallery, smashing the nose of a sculpted bust. Iconoclasm led to the defacement of many religious artworks.

In computing, website defacement is usually the substitution of the original home

A final word:



Treat your password like you treat your toothbrush. Never give it to anyone else to use, and change it every few months.

design by Daniel Fogelqvist