Ethical Hacking and Countermeasures

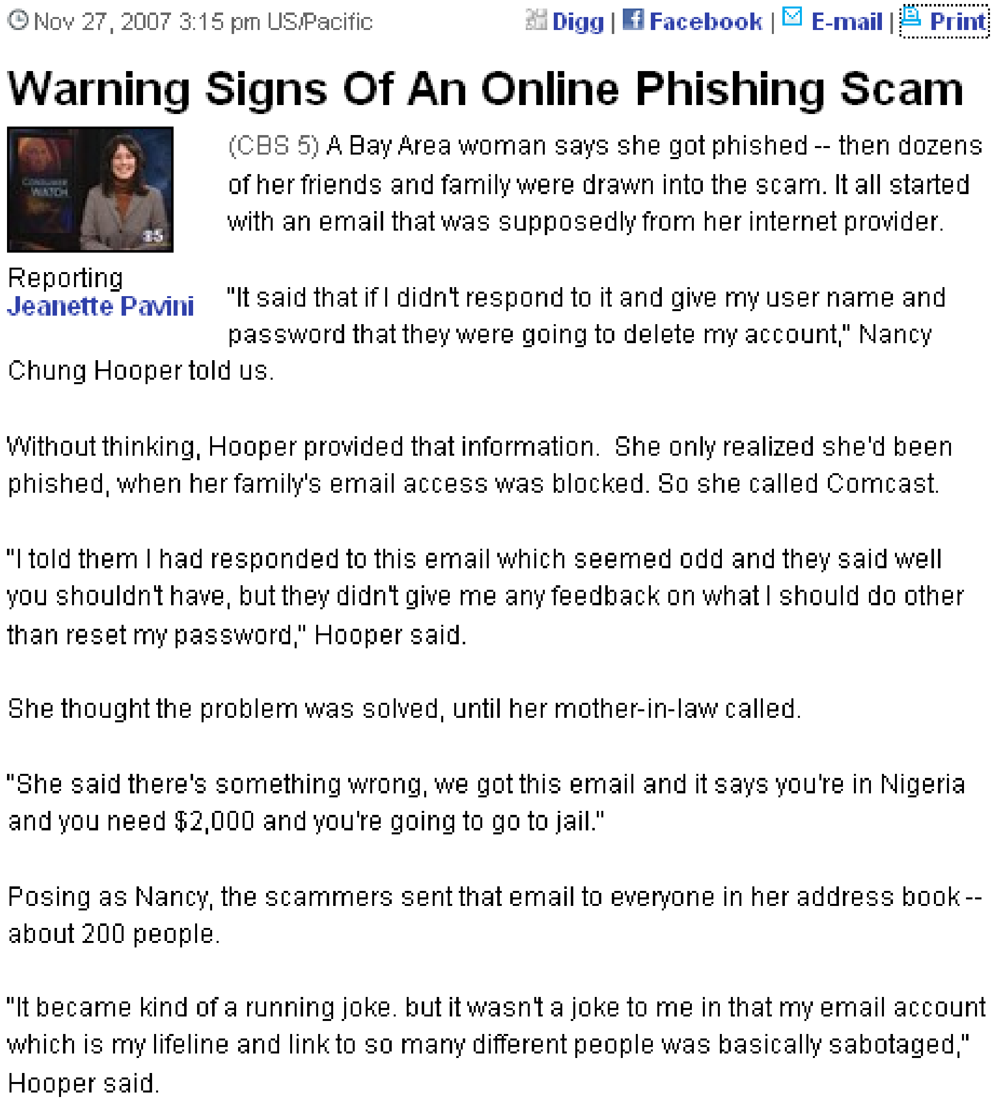
Version 6

Module XII

Phishing

C|EH™
Certified Ethical Hacker

News


Nov 27, 2007 3:15 pm US/Pacific
Digg | Facebook | E-mail | Print

Warning Signs Of An Online Phishing Scam

Reporting
Jeanette Pavini

(CBS 5) A Bay Area woman says she got phished -- then dozens of her friends and family were drawn into the scam. It all started with an email that was supposedly from her internet provider.

"It said that if I didn't respond to it and give my user name and password that they were going to delete my account," Nancy Chung Hooper told us.

Without thinking, Hooper provided that information. She only realized she'd been phished, when her family's email access was blocked. So she called Comcast.

"I told them I had responded to this email which seemed odd and they said well you shouldn't have, but they didn't give me any feedback on what I should do other than reset my password," Hooper said.

She thought the problem was solved, until her mother-in-law called.

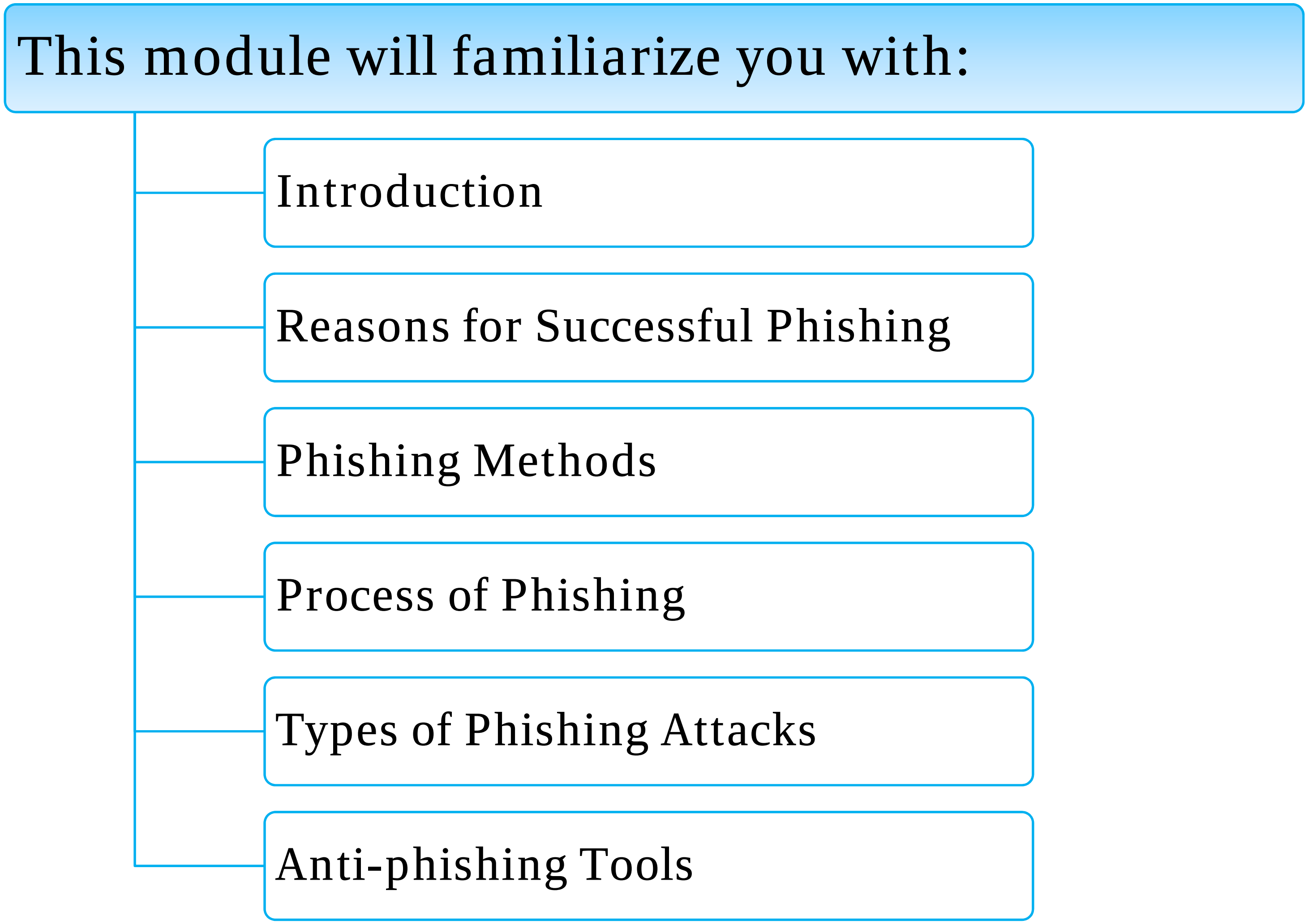
"She said there's something wrong, we got this email and it says you're in Nigeria and you need $2,000 and you're going to go to jail."

Posing as Nancy, the scammers sent that email to everyone in her address book -- about 200 people.

"It became kind of a running joke. but it wasn't a joke to me in that my email account which is my lifeline and link to so many different people was basically sabotaged," Hooper said.

Source: *http://cbs5.com/*

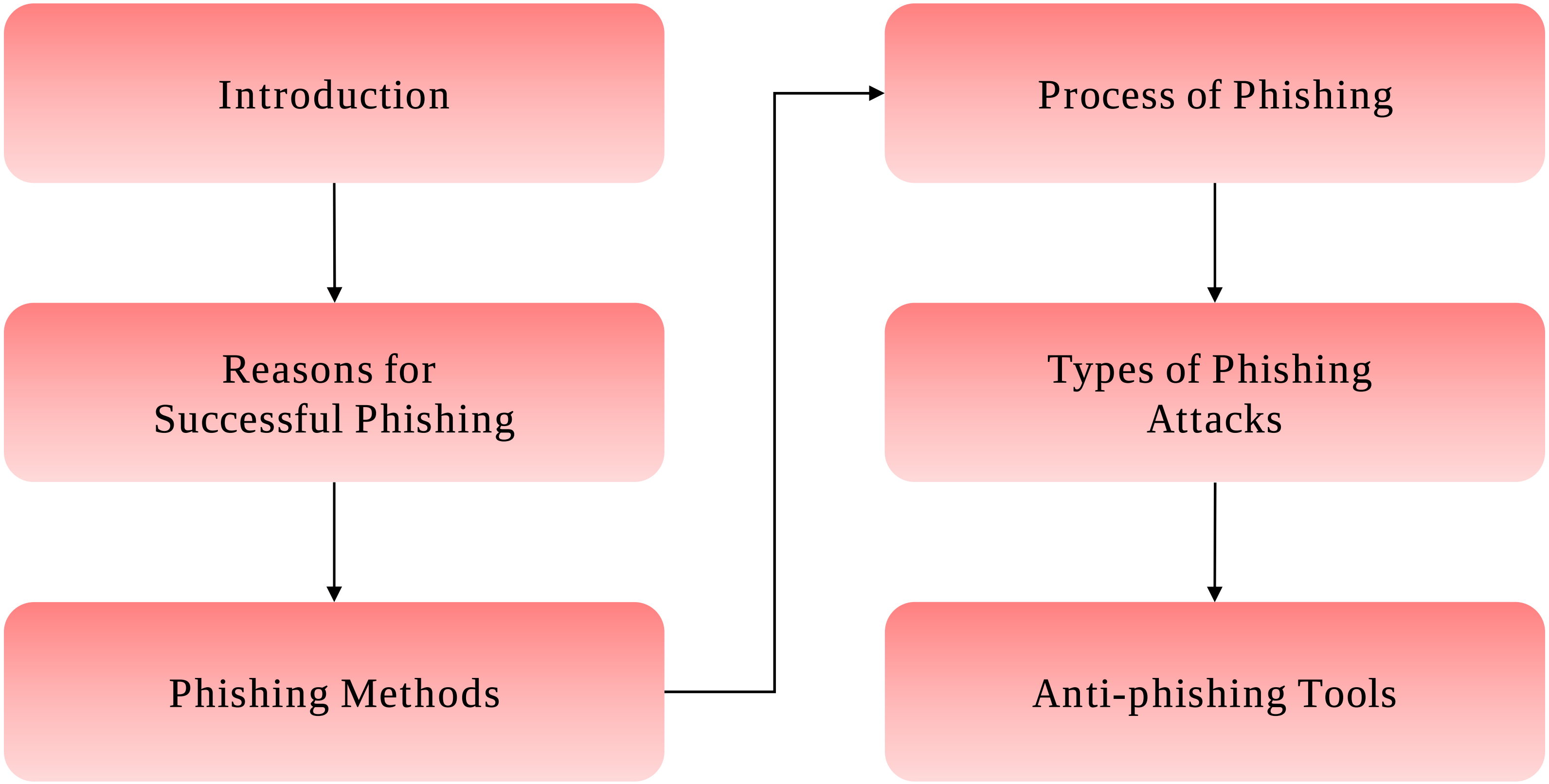
Module Objective



This module will familiarize you with:

- Introduction
- Reasons for Successful Phishing
- Phishing Methods
- Process of Phishing
- Types of Phishing Attacks
- Anti-phishing Tools

Module Flow



Introduction

Reasons for Successful Phishing

Phishing Methods

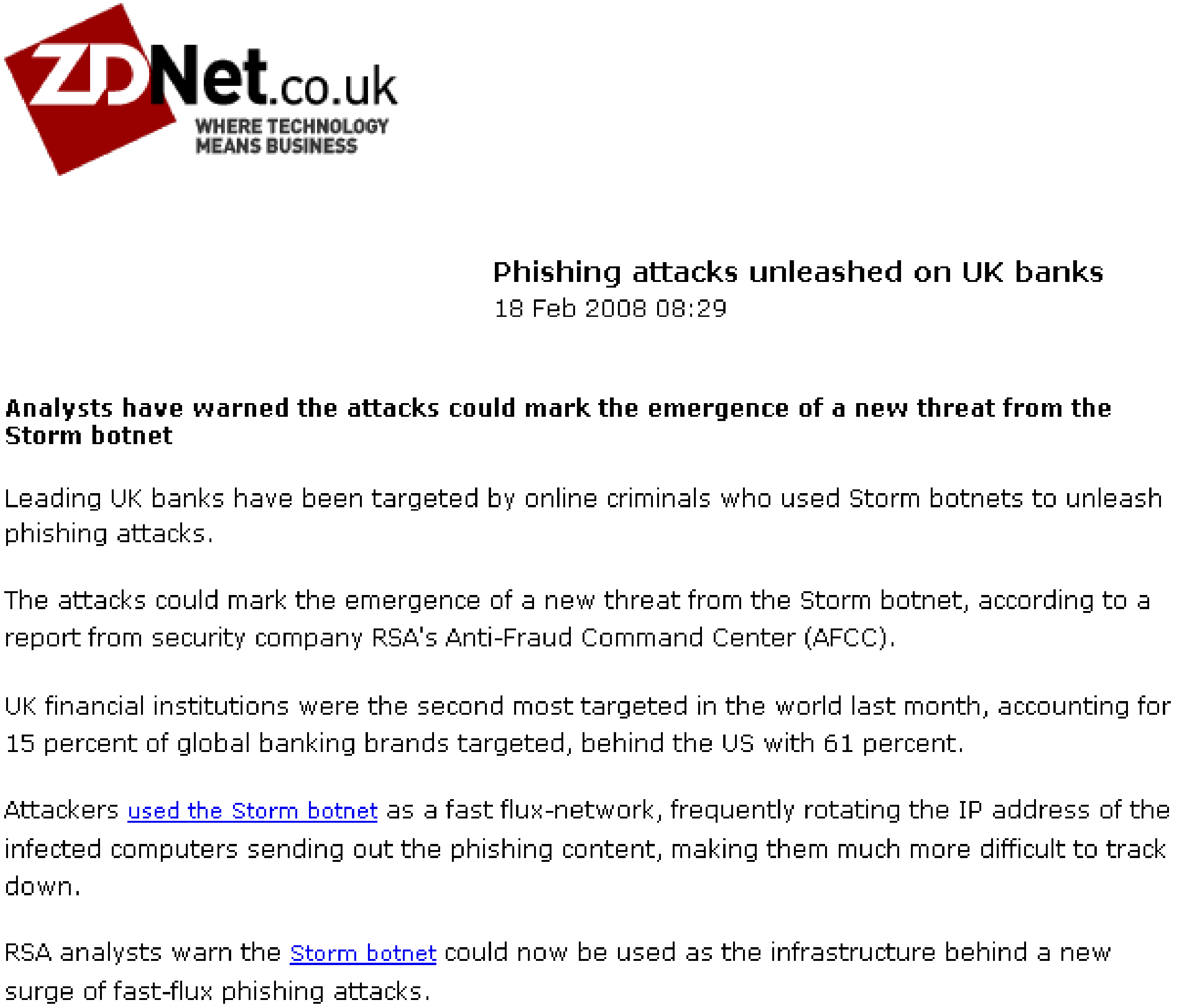
Process of Phishing

Types of Phishing Attacks

Anti-phishing Tools

Phishing- Introduction

News



Phishing attacks unleashed on UK banks

18 Feb 2008 08:29

Analysts have warned the attacks could mark the emergence of a new threat from the Storm botnet

Leading UK banks have been targeted by online criminals who used Storm botnets to unleash phishing attacks.

The attacks could mark the emergence of a new threat from the Storm botnet, according to a report from security company RSA's Anti-Fraud Command Center (AFCC).

UK financial institutions were the second most targeted in the world last month, accounting for 15 percent of global banking brands targeted, behind the US with 61 percent.

Attackers used the Storm botnet as a fast flux-network, frequently rotating the IP address of the infected computers sending out the phishing content, making them much more difficult to track down.

RSA analysts warn the Storm botnet could now be used as the infrastructure behind a new surge of fast-flux phishing attacks.

Source: *http://www.zdnet.co.uk*

Introduction

Phishing is an Internet scam where the user is convinced to give valuable information

Phishing will redirect the user to a different website through emails, instant messages, spywares etc.

Phishers offer illegitimate websites to the user to fill personal information

The main purpose of phishing is to get access to the customer's bank accounts, passwords and other security information

Phishing attacks can target the audience through mass- mailing millions of email addresses around the world

Reasons for Successful Phishing

Lack of knowledge

- Lack of computer system knowledge by the user (as how the emails and web works) can be exploited by the phishers to acquire sensitive information
- Many users lack the knowledge of security and security indicators

Visual deception

- Phishers can fool users by convincing them to get into a fake website with the domain name slightly different from the original website which is difficult to notice
- They use the images of the legitimate hyperlink, which itself helps as a hyperlink to an unauthorized website
- Phishers track the users by using the images in the content of a web page that looks like a browser window
- Keeping an unauthorized browser window on top of, or next to a legitimate window having same looks, will make the user believe that they are from the same source
- Setting the tone of the language same as the original website

Reasons for Successful Phishing (cont'd)

Not giving attention to Security Indicators

- Users don't give proper attention to read the warning messages or security indicators
- In the absence of security indicators it will be easy to insert spoofed images which will go unidentified by the users

Phishing Methods

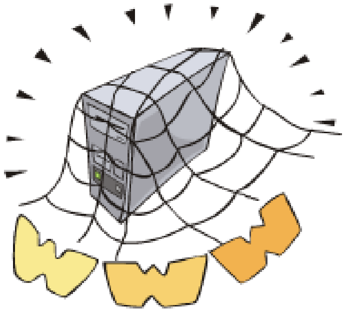
Email and Spam

- Most of the phishing attacks are done through email
- Phishers can send millions of emails to valid email addresses by using the techniques and tools opted by spammers
- Phishing emails provide a sense of urgency in the minds of the user to give the important information
- Phishers take the advantage from SMTP flaws by adding fake “Mail from” header and incorporate any organization of choice
- Minor changes are made in the URL field by sending mimic copies of legitimate emails

Phishing Methods (cont'd)

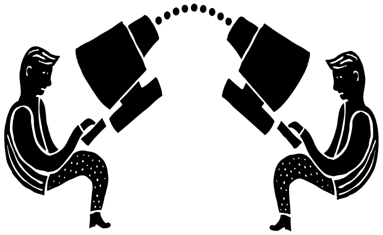
Web-based Delivery

- This type of attack is carried out by targeting the customers through a third party website
- Providing malicious website content is a popular method of phishing attacks
- Keeping fake banner advertisements in some reputed websites to redirect the customers to the phishing website is also a form of web based delivery



IRC and Instant Messaging

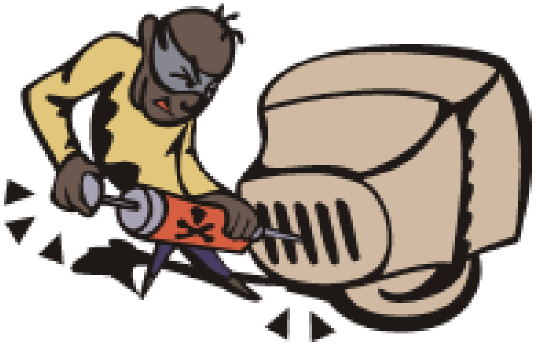
- IRC and IM clients allow for embedded dynamic content
- The attackers send the fake information and links to the users through IRC and IM



Phishing Methods (cont’d)

Trojaned Hosts

- Trojan is a program that gives complete access of host computer to phishers after being installed at the host computer
- Phishers will make the user to install the trojaned software which helps in email propagating and hosting fraudulent websites



Process of Phishing

The process involved in building a successful phishing site is:

Registering a fake domain name

Building a look alike website

Sending emails to many users

Types of Phishing Attacks

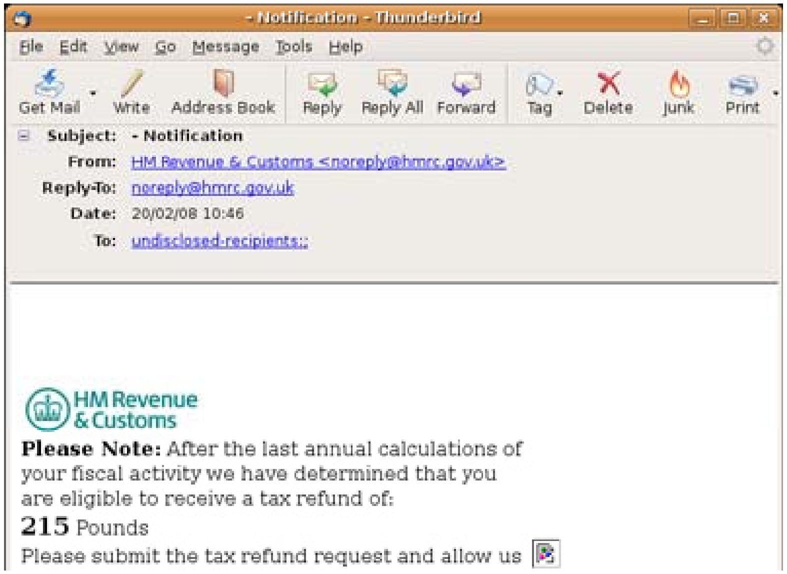
News

HMRC data debacle used to bait phishing lure

By John Leyden
Published Friday 22nd February 2008 13:23 GMT

A phishing attack targeting victims of the HMRC data loss debacle has been spotted on the net. The bogus emails offering recipient the false opportunity to claim a tax refund of £215 from the UK Government over the potential exposure of confidential data. The email contains a web link to a suspect site, reports security firm McAfee, which spotted the ruse.

The ploy takes advantage of the loss of computer discs by HM Revenue and Customs containing the confidential details of 25 million child benefit recipients, including bank and building society details, NI numbers, addresses and child records. The attack follows more than two months after UK Chancellor Alistair Darling announced the loss, so arguably fraudsters have been slow off the mark.



Subject: - Notification
From: HM Revenue & Customs <noreply@hmrc.gov.uk>
Reply-To: noreply@hmrc.gov.uk
Date: 20/02/08 10:46
To: undisclosed-recipients:;

Please Note: After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of:
215 Pounds
Please submit the tax refund request and allow us

Source: *http://www.theregister.co.uk*

Man-in-the-Middle Attacks

In this attack, the attacker's computer is placed between the customer's computer and the real website. This helps the attacker in tracking the communications between the systems

This attack supports both HTTP and HTTPS communications

In order to make this attack successful, the attacker has to direct the customer to proxy server rather than the real server

The following are the techniques used to direct the customer to proxy server:

- Transparent Proxies located at the real server captures all the data by forcing the outbound HTTP and HTTPS traffic towards itself
- DNS Cache Poisoning can be used to disturb the normal traffic routing by establishing false IP address at the key domain names
- Browser proxy configuration is used to set a proxy configuration options by overriding the users web browser settings

URL Obfuscation Attacks

The user is made to follow a URL by sending a message which navigates them to the attacker's server

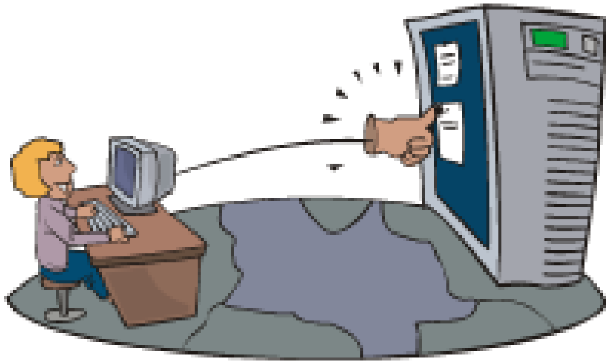
The different methods of URL obfuscation include:

- Making few changes to the authorized URL's which makes difficult to identify it as a phishing site
- Giving friendly login URL's to the users which negates the complexity of authentication that navigates them to the look-a-like target URL
- Many third party organizations offer to design shorter URL's for free of service, which can be used to obfuscate the true URL
- The IP address of a domain name can be used as a part of the URL to obfuscate the host and also to bypass content filtering systems

Cross-site Scripting Attacks

This type of attack makes use of custom URL or code to inject into a valid web-based application URL or imbedded data field

Most of the CSS attacks are carried out using URL formatting



Hidden Attacks

Attacker uses the HTML, DHTML, or other scriptable code to:

- Change the display of rendered information by interpreting with the customers' web browser
- Disguise content as coming from the real site with fake content

Methods used for hidden attacks are:

- Hidden Frame:
  - Frames are used to hide attack content with their uniform browser support and easy coding style
- Overriding Page Content
- Graphical Substitution

Client-side Vulnerabilities

Most customers are vulnerable towards the phishing attacks while they browse the web for any software

These client side vulnerabilities can be exploited in a number of ways similar to the worms and viruses

The anti virus software are not useful for these vulnerabilities as they are harder to identify

Deceptive Phishing

The common method of deceptive phishing is email

Phishser sends a bulk of deceptive emails which command the user to click on the link provided

Phisher's call to action contains daunting information about the recipient's account

Phisher then collects the confidential information given by the user

Malware-Based Phishing

In this method, phishers use malicious software to attack on the user machines

This phishing attack spreads due to social engineering or security vulnerabilities

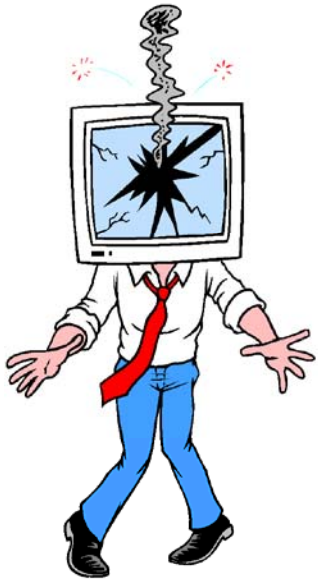
In social engineering, the user is convinced to open an email attachment that attracts the user regarding some important information and download it containing some malwares

Exploiting the security vulnerabilities by injecting worms and viruses is another form of malware based phishing

Malware-Based Phishing (cont'd)

Keyloggers and Screenloggers

- It is a program that installs itself into the web browser or as a device driver that monitors the input data and sends it to the phishing server
- It monitors the data and sends to a phishing server
- The techniques used by keyloggers and screenloggers are:
  - Key logging is used to monitor and record the key presses by the customer
  - The device driver monitoring the keyboard and mouse inputs by the user
  - The screen logger monitoring both the user inputs and the display



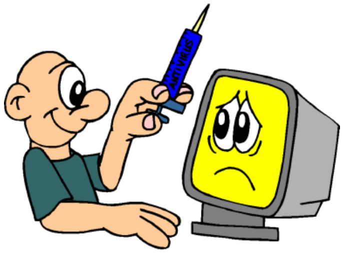
Malware-Based Phishing (cont'd)

Web Trojans

- These malicious programs are popped up over the login screen when the user is entering information on the website
- The information is entered locally rather than on the web site which is later transmitted to the phisher

Hosts File Poisoning

- The Operating systems consists of 'hosts' file which checks the host names before a DNS lookup is performed
- It is the modification of the host file to make the user navigate to an illegitimate website and give confidential information
- This allows the phishers to modify the host file to redirect the user



Malware-Based Phishing (cont'd)

System Reconfiguration Attacks

- This attack is used to reconfigure the setting at the user computer
- The systems DNS server is modified with a faulty DNS information by poisoning the host file
- It Changes the proxy server setting on the system to redirect the user's traffic to other sites

DNS-Based Phishing

DNS based phishing is used to pollute the DNS cache with incorrect information which directs the user to the other location

This type of phishing can be done directly when the user has a misconfigured DNS cache

The user's DNS server can be changed with a system reconfiguration attack

Content-Injection Phishing

In this attack, a malicious content is injected into a legitimate site

This malicious content can direct the user to some other site or it can install malwares on the computer

Types of content-injection phishing are:

- Hackers replace the legitimate content with malicious content by compromising a server through security vulnerability
- Malicious content can be injected into a site using a cross-site scripting vulnerability
- Illegitimate actions can be performed on a site using an SQL injection vulnerability

Search Engine Phishing

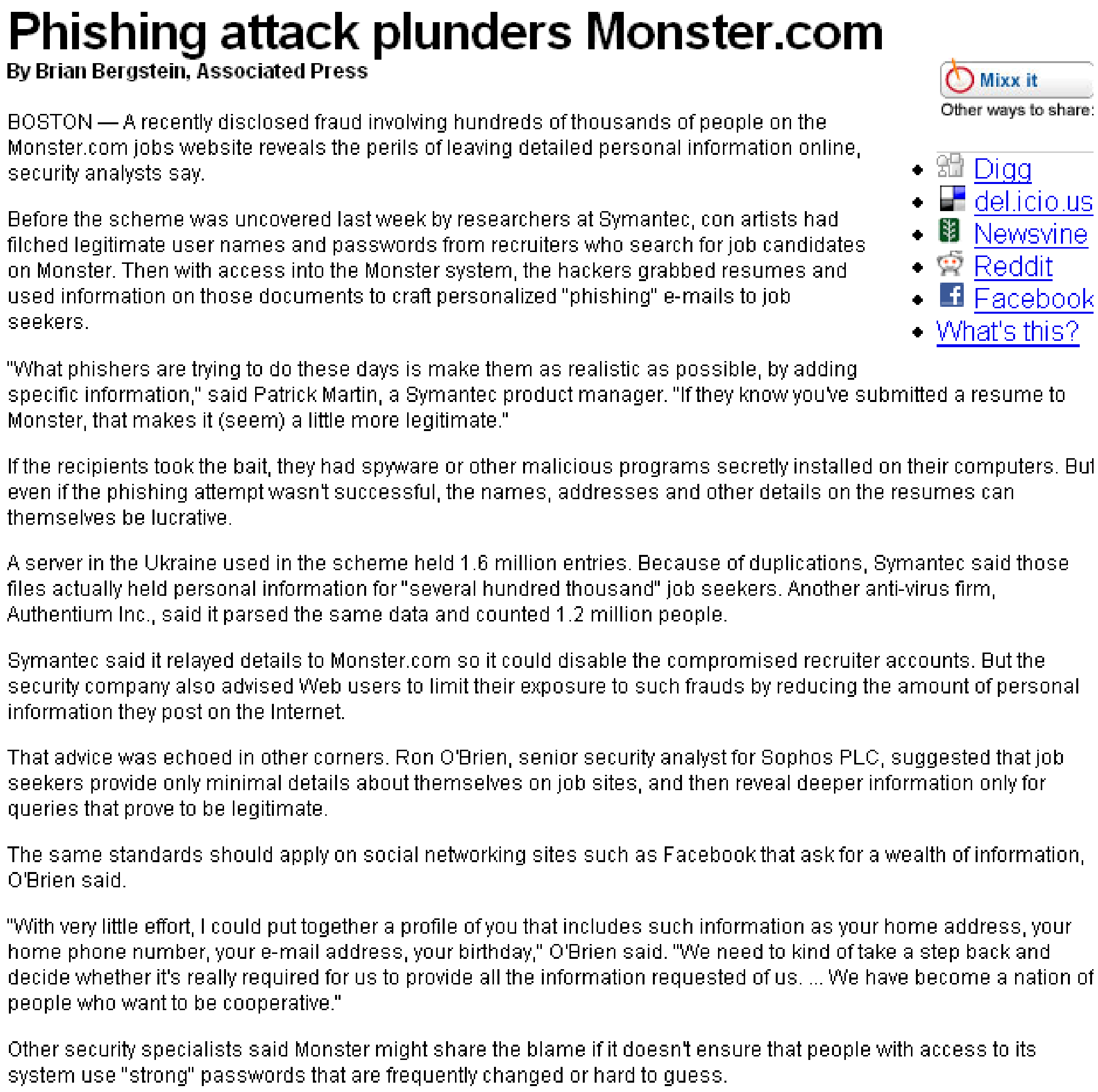
The phishers create an identical websites for fake products and get the pages indexed by the search engine

Phishers convince the user to give their confidential information by providing interesting offers

The major success in search engine phishing comes from online banking and online shopping

CEH™ Certified Ethical Hacker

News



Phishing attack plunders Monster.com

By Brian Bergstein, Associated Press

BOSTON — A recently disclosed fraud involving hundreds of thousands of people on the Monster.com jobs website reveals the perils of leaving detailed personal information online, security analysts say.

Before the scheme was uncovered last week by researchers at Symantec, con artists had filched legitimate user names and passwords from recruiters who search for job candidates on Monster. Then with access into the Monster system, the hackers grabbed resumes and used information on those documents to craft personalized "phishing" e-mails to job seekers.

"What phishers are trying to do these days is make them as realistic as possible, by adding specific information," said Patrick Martin, a Symantec product manager. "If they know you've submitted a resume to Monster, that makes it (seem) a little more legitimate."

If the recipients took the bait, they had spyware or other malicious programs secretly installed on their computers. But even if the phishing attempt wasn't successful, the names, addresses and other details on the resumes can themselves be lucrative.

A server in the Ukraine used in the scheme held 1.6 million entries. Because of duplications, Symantec said those files actually held personal information for "several hundred thousand" job seekers. Another anti-virus firm, Authentium Inc., said it parsed the same data and counted 1.2 million people.

Symantec said it relayed details to Monster.com so it could disable the compromised recruiter accounts. But the security company also advised Web users to limit their exposure to such frauds by reducing the amount of personal information they post on the Internet.

That advice was echoed in other corners. Ron O'Brien, senior security analyst for Sophos PLC, suggested that job seekers provide only minimal details about themselves on job sites, and then reveal deeper information only for queries that prove to be legitimate.

The same standards should apply on social networking sites such as Facebook that ask for a wealth of information, O'Brien said.

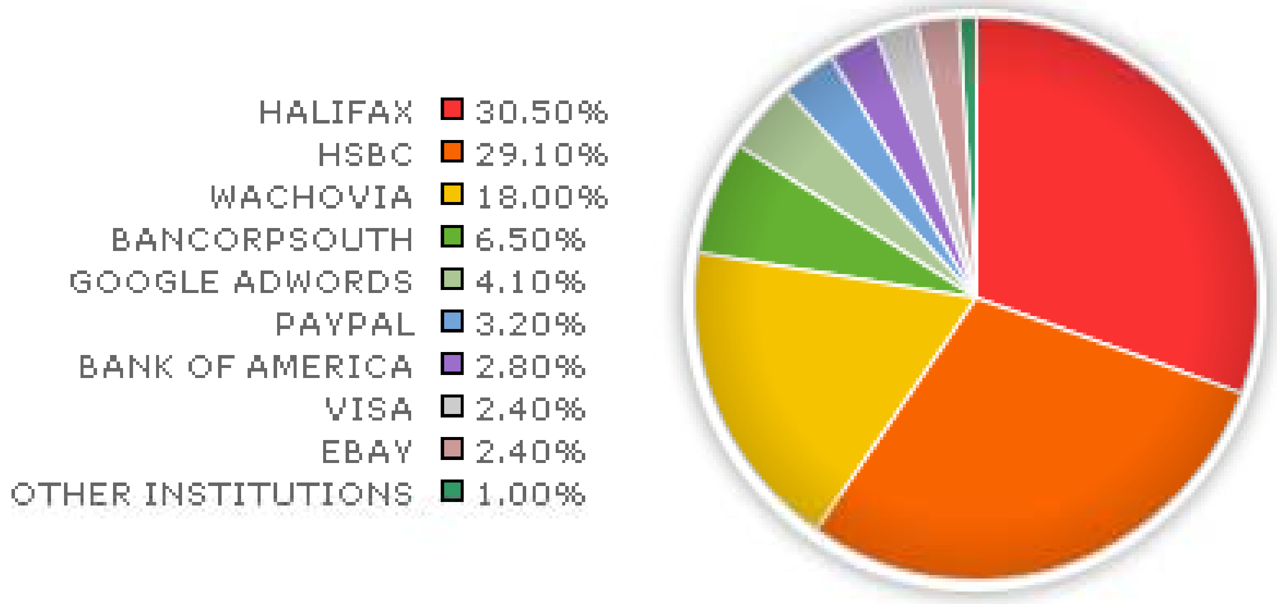
"With very little effort, I could put together a profile of you that includes such information as your home address, your home phone number, your e-mail address, your birthday," O'Brien said. "We need to kind of take a step back and decide whether it's really required for us to provide all the information requested of us. ... We have become a nation of people who want to be cooperative."

Other security specialists said Monster might share the blame if it doesn't ensure that people with access to its system use "strong" passwords that are frequently changed or hard to guess.

Source: *http://www.usatoday.com*

Phishing Statistics: March 2008

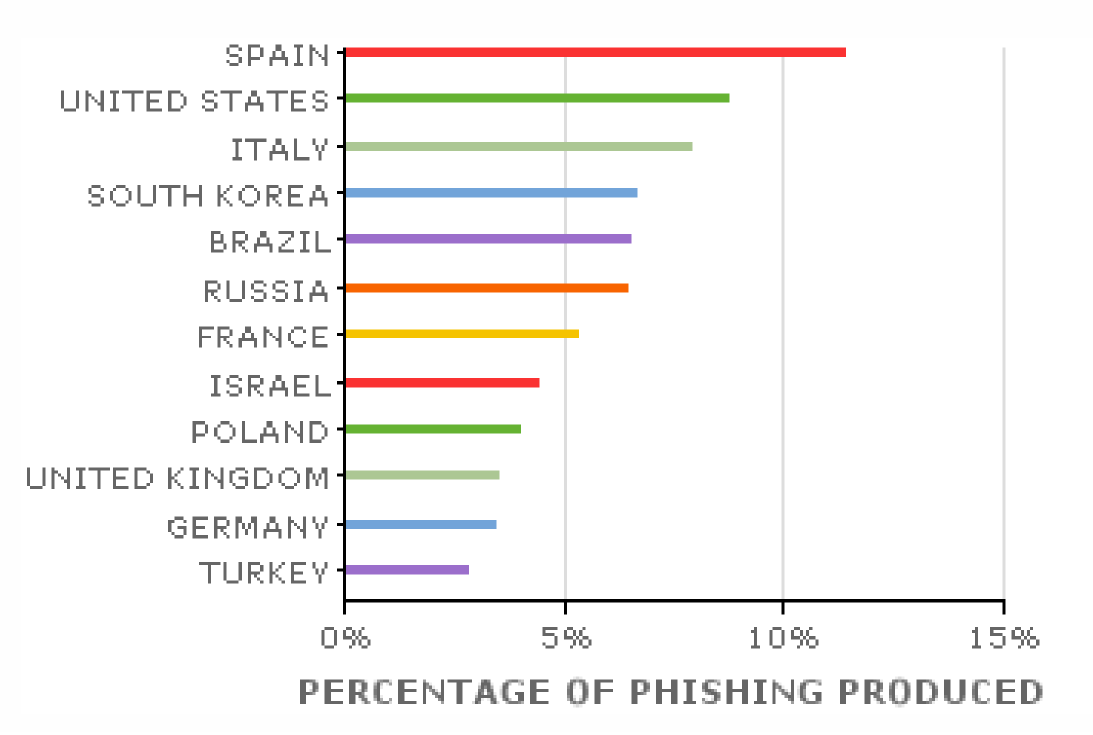
Current Phishing Targets



Source: *http://www.marshal.com/*

Phishing Statistics: March 2008 (cont'd)

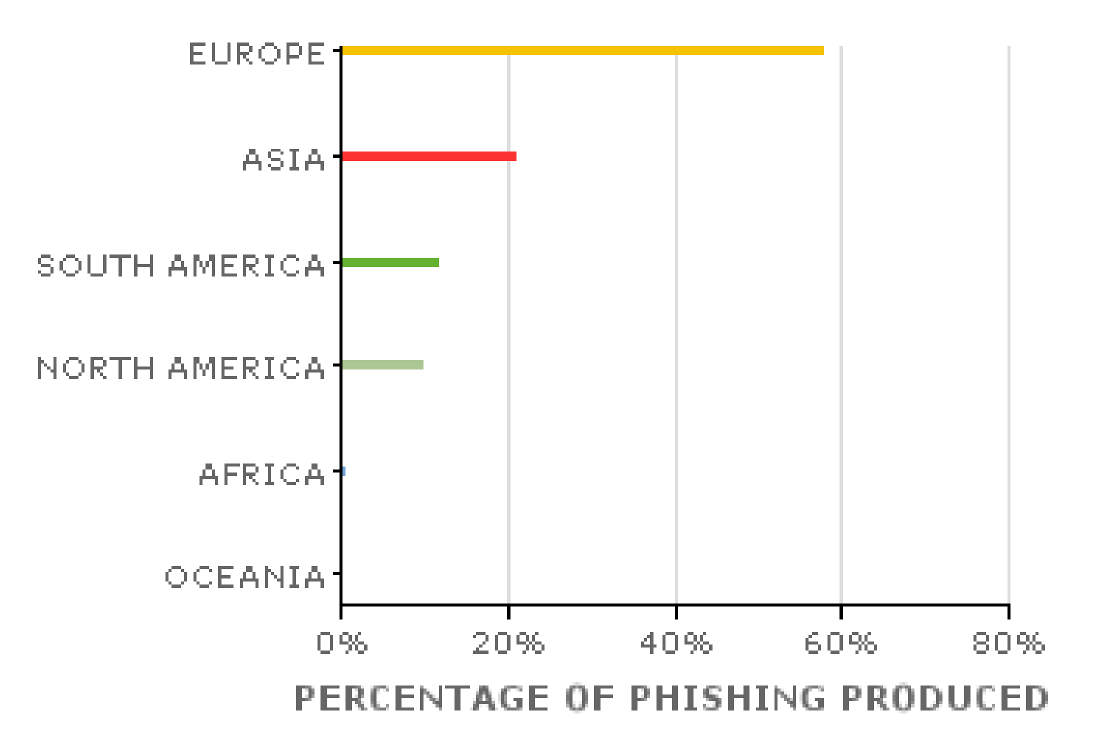
Phishing Sources by Country



Source: *http://www.marshal.com/*

Phishing Statistics: March 2008 (cont'd)

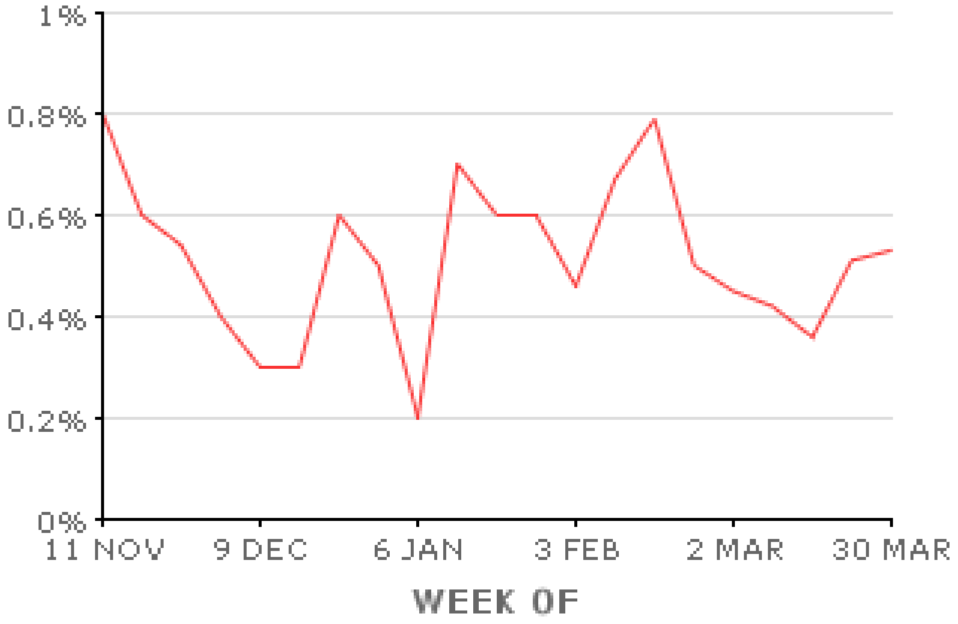
Phishing Sources by Continent



Source: *http://www.marshal.com/*

Phishing Statistics: March 2008 (cont'd)

Phishing Percentage over Time



Source: *http://www.marshal.com/*

Anti-Phishing

Phishing attacks are prevented by anti-phishing software

Anti-Phishing Software detects the phishing attacks in the website or in the customer's email

These software's display the real website domain that the customer is visiting by residing at the web browsers and email servers, as an integral tool

Phishing attacks can be prevented both at the server side and at the client side

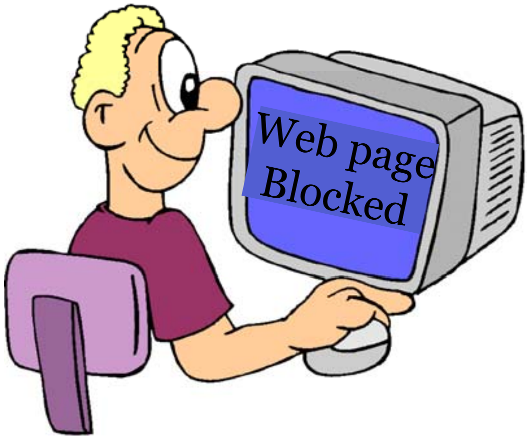
Anti-Phishing Tools

PhishTank SiteChecker

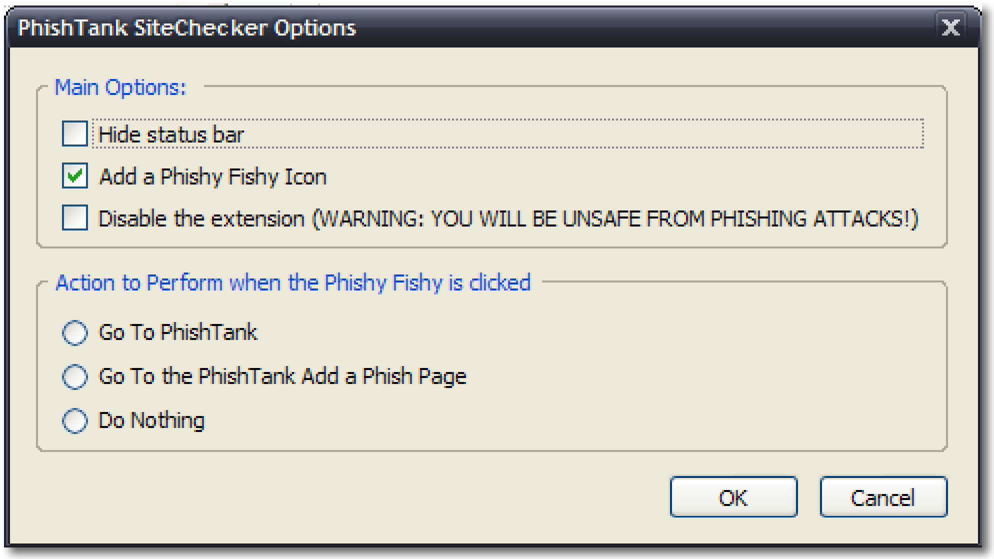
PhishTank SiteChecker blocks the phishing pages with reference to the data present in the phish tank

It is an extension of firefox, SeaMonkey, Internet Explorer, Opera, Mozilla, and Flock

The SiteChecker checks the current site the user is in, against a database of PhishTank



PhishTank SiteChecker: Screenshot



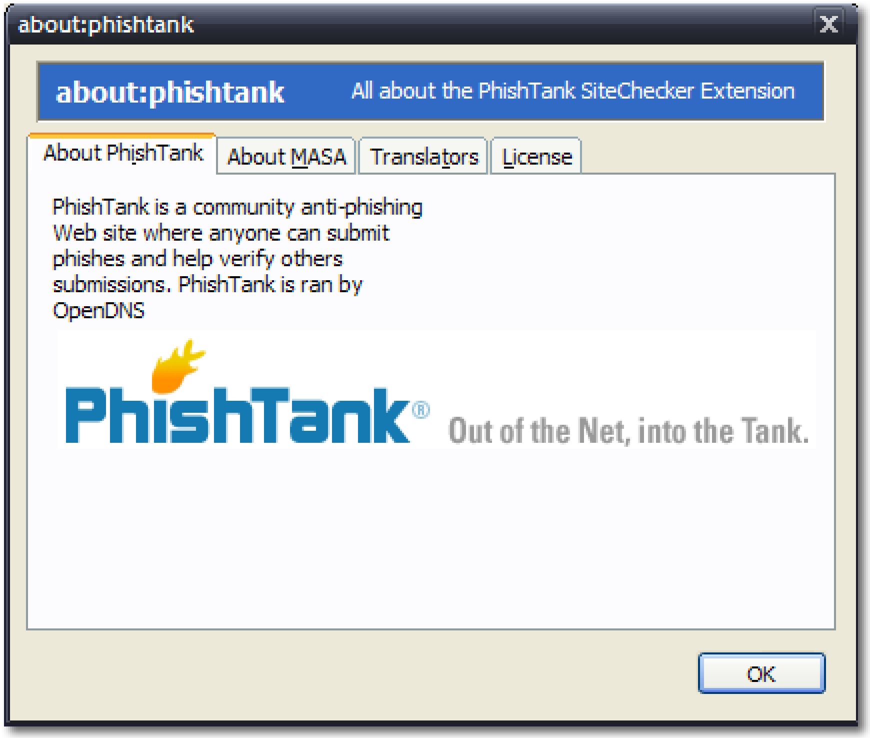
PhishTank SiteChecker Options

Main Options:

- ☐ Hide status bar
- ☑ Add a Phishy Fishy Icon
- ☐ Disable the extension (WARNING: YOU WILL BE UNSAFE FROM PHISHING ATTACKS!)

Action to Perform when the Phishy Fishy is clicked

- ○ Go To PhishTank
- ○ Go To the PhishTank Add a Phish Page
- ○ Do Nothing



about:phishtank

about:phishtank All about the PhishTank SiteChecker Extension

PhishTank is a community anti-phishing Web site where anyone can submit phishes and help verify others submissions. PhishTank is ran by OpenDNS

NetCraft

NetCraft tool alerts the user when connected to the phishing site

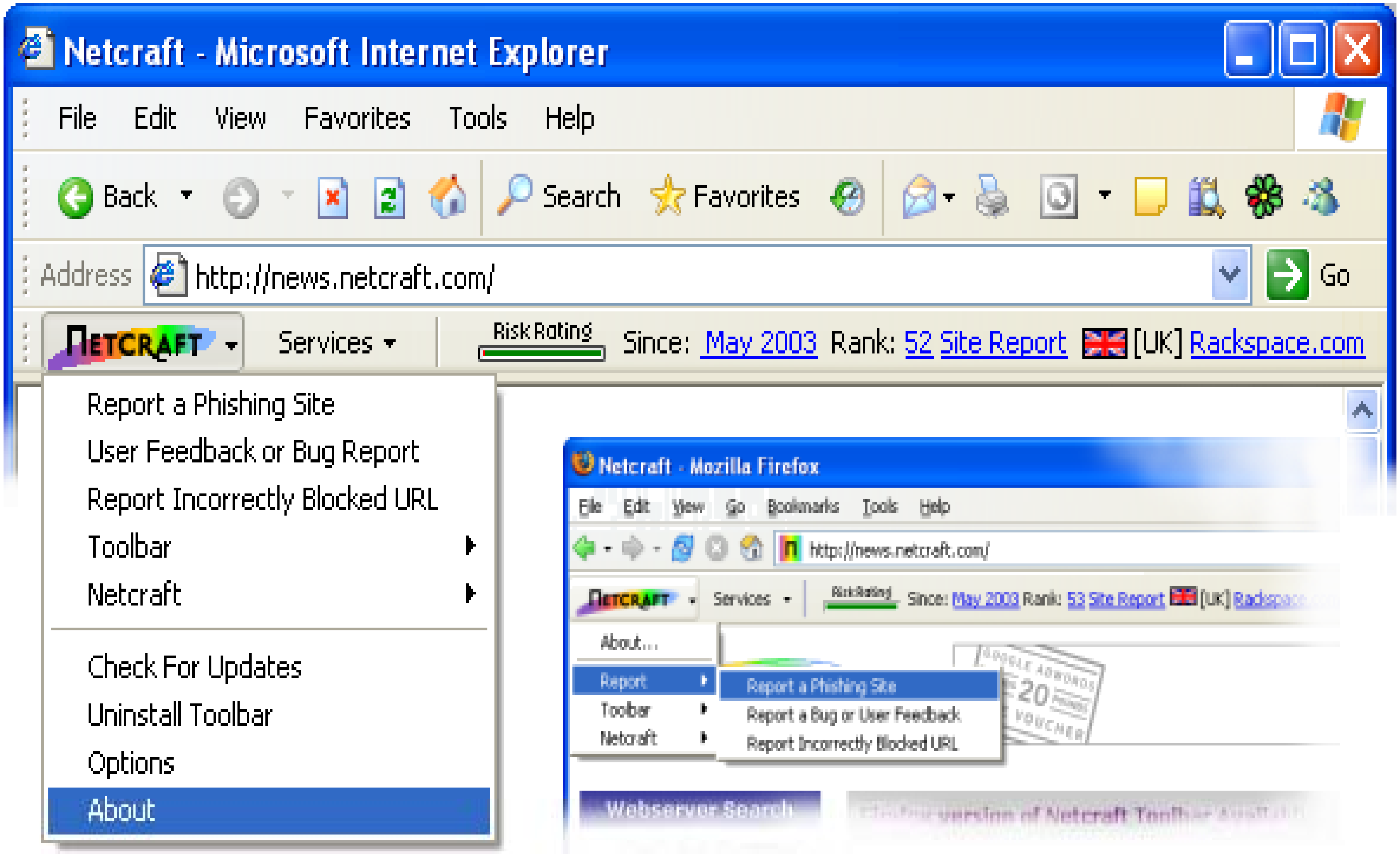
When the user connects to a phishing site it blocks the user by showing a warning sign

It traps suspicious URLs in which the characters have no common purpose other than to deceive the user

It imposes the browser navigational controls in all windows to protect against the pop ups which hides the navigational controls

It displays the countries hosting the sites to detect fraudulent URLs

NetCraft: Screenshot

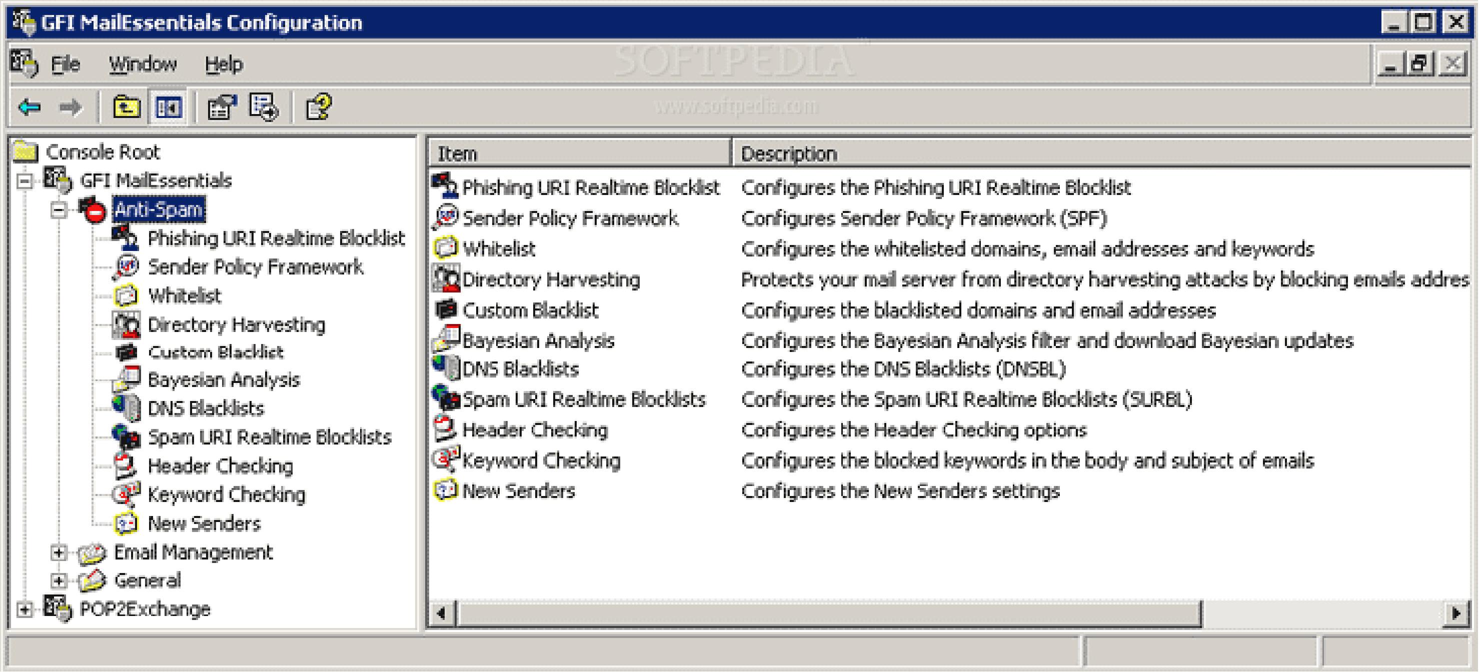

Netcraft - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://news.netcraft.com/ Go
NETCRAFT Services Risk Rating Since: May 2003 Rank: 52 Site Report [UK] Rackspace.com
Report a Phishing Site
User Feedback or Bug Report
Report Incorrectly Blocked URL
Toolbar
Netcraft
Check For Updates
Uninstall Toolbar
Options
About
Netcraft - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://news.netcraft.com/
NETCRAFT Services Risk Rating Since: May 2003 Rank: 53 Site Report [UK] Rackspace
About...
Report
Toolbar
Netcraft
Report a Phishing Site
Report a Bug or User Feedback
Report Incorrectly Blocked URL
Webserver Search

GFI MailEssentials

GFI MailEssentials' anti-phishing module detects and blocks threats posed by phishing emails

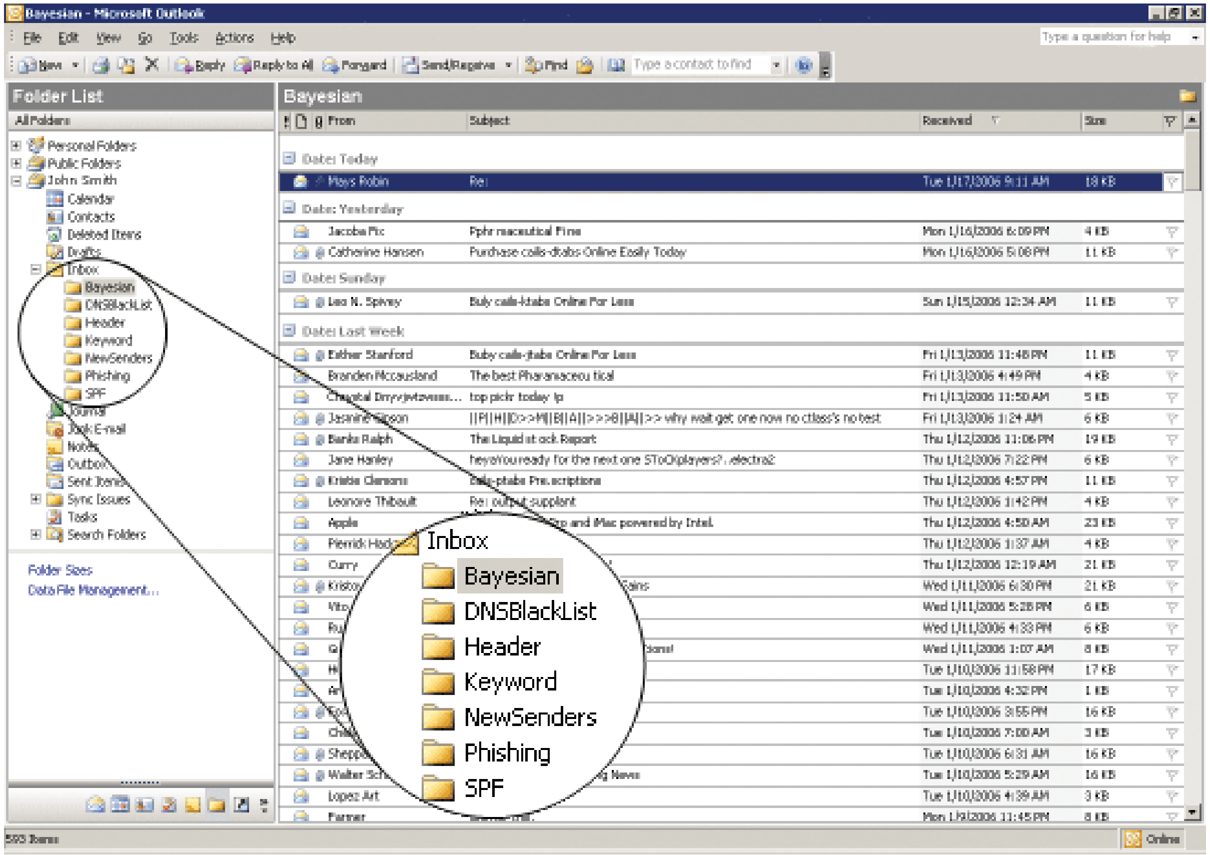
It updates the database of blacklisted mails which ensures the capture of all latest phishing mails

It also checks for typical phishing keywords in every email sent to the organization



Item	Description
Phishing URI Realtime Blocklist	Configures the Phishing URI Realtime Blocklist
Sender Policy Framework	Configures Sender Policy Framework (SPF)
Whitelist	Configures the whitelisted domains, email addresses and keywords
Directory Harvesting	Protects your mail server from directory harvesting attacks by blocking emails addres
Custom Blacklist	Configures the blacklisted domains and email addresses
Bayesian Analysis	Configures the Bayesian Analysis filter and download Bayesian updates
DNS Blacklists	Configures the DNS Blacklists (DNSBL)
Spam URI Realtime Blocklists	Configures the Spam URI Realtime Blocklists (SURBL)
Header Checking	Configures the Header Checking options
Keyword Checking	Configures the blocked keywords in the body and subject of emails
New Senders	Configures the New Senders settings

GFI MailEssentials: Screenshot



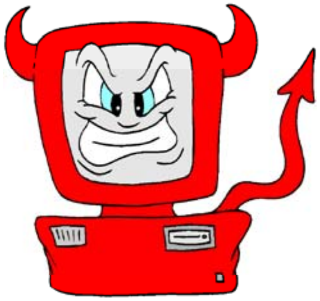
From	Subject	Received	Size
Date: Today			
Mays Robin	Re:	Tue 1/17/2006 9:11 AM	18 KB
Date: Yesterday			
Jacoba Pic	Pphr rmaceutical Fine	Mon 1/16/2006 6:09 PM	4 KB
Catherine Hansen	Purchase calis-dtabs Online Easily Today	Mon 1/16/2006 5:08 PM	11 KB
Date: Sunday			
Lea N. Spivey	Buly cails-ktabs Online For Less	Sun 1/15/2006 12:34 AM	11 KB
Date: Last Week			
Esther Stanford	Buby cails-jtabs Online For Less	Fri 1/13/2006 11:48 PM	11 KB
Branden Mccausland	The best Pharamaceou tical	Fri 1/13/2006 4:49 PM	4 KB
Chantal Dmyvjevtavsas...	top pickr today lp	Fri 1/13/2006 11:50 AM	5 KB
Jasmine Gibson	||P||H||D>>M||B||A||>>>B||A||>> why wait get one now no ctlass's no test	Fri 1/13/2006 1:24 AM	6 KB
Banks Ralph	The Liquid st ock Report	Thu 1/12/2006 11:06 PM	19 KB
Jane Hanley	heyaYou ready for the next one SToOKplayers? .electra2	Thu 1/12/2006 7:22 PM	6 KB
Kristie Clemons	Calis-ptabs Pre.scriptions	Thu 1/12/2006 4:57 PM	11 KB
Leonore Thibault	Re: output supplant	Thu 1/12/2006 1:42 PM	4 KB
Apple	op and iMac powered by Intel.	Thu 1/12/2006 4:50 AM	23 KB
Pierrick Had		Thu 1/12/2006 1:37 AM	4 KB
Curry		Thu 1/12/2006 12:19 AM	21 KB
Kristo	ains	Wed 1/11/2006 6:30 PM	21 KB
Vito		Wed 1/11/2006 5:28 PM	6 KB
Ru		Wed 1/11/2006 4:33 PM	6 KB
Q	tions!	Wed 1/11/2006 1:07 AM	8 KB
H		Tue 1/10/2006 11:58 PM	17 KB
Ar		Tue 1/10/2006 4:32 PM	1 KB
Ed		Tue 1/10/2006 3:55 PM	16 KB
Cha		Tue 1/10/2006 7:00 AM	3 KB
Shepp		Tue 1/10/2006 6:31 AM	16 KB
Walter Sch	g News	Tue 1/10/2006 5:29 AM	16 KB
Lopez Art		Tue 1/10/2006 4:39 AM	3 KB
Farmer	[illegible]	Mon 1/9/2006 11:45 PM	8 KB

SpoofGuard

spoofGuard prevents a form of malicious attacks, such as web spoofing and phishing

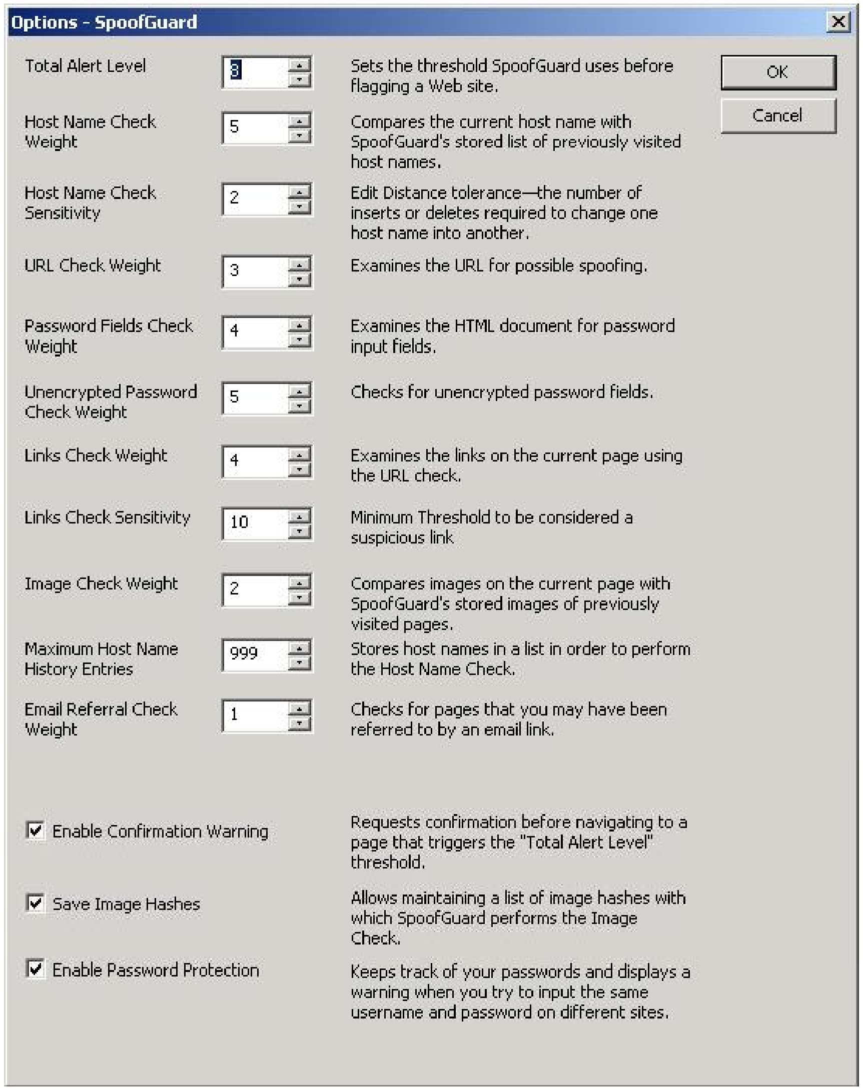
It places a traffic light at the users browser toolbar that turns from green to yellow to red when navigated to a spoof site

When the user enters private data into a spoofed site, spoofguard saves the data and warns the user



C|EH™ Certified Ethical Hacker

SpoofGuard: Screenshot 1



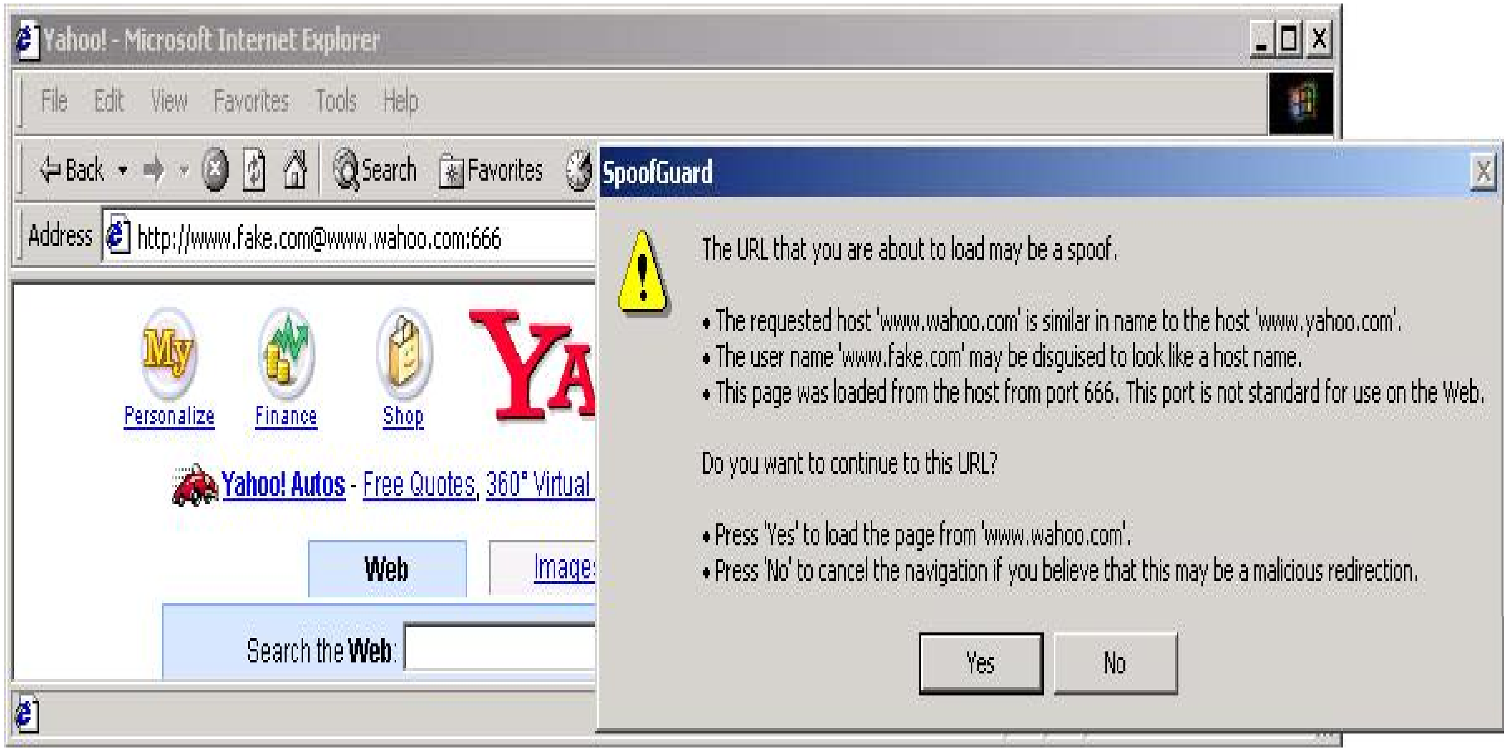
Options - SpoofGuard

Total Alert Level	3	Sets the threshold SpoofGuard uses before flagging a Web site.
Host Name Check Weight	5	Compares the current host name with SpoofGuard's stored list of previously visited host names.
Host Name Check Sensitivity	2	Edit Distance tolerance—the number of inserts or deletes required to change one host name into another.
URL Check Weight	3	Examines the URL for possible spoofing.
Password Fields Check Weight	4	Examines the HTML document for password input fields.
Unencrypted Password Check Weight	5	Checks for unencrypted password fields.
Links Check Weight	4	Examines the links on the current page using the URL check.
Links Check Sensitivity	10	Minimum Threshold to be considered a suspicious link
Image Check Weight	2	Compares images on the current page with SpoofGuard's stored images of previously visited pages.
Maximum Host Name History Entries	999	Stores host names in a list in order to perform the Host Name Check.
Email Referral Check Weight	1	Checks for pages that you may have been referred to by an email link.

☑ Enable Confirmation Warning	Requests confirmation before navigating to a page that triggers the "Total Alert Level" threshold.
☑ Save Image Hashes	Allows maintaining a list of image hashes with which SpoofGuard performs the Image Check.
☑ Enable Password Protection	Keeps track of your passwords and displays a warning when you try to input the same username and password on different sites.

EC-Council

SpoofGuard: Screenshot 2


Yahoo! - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.fake.com@www.wahoo.com:666
Personalize
Finance
Shop
Yahoo! Autos - Free Quotes, 360° Virtual
Web
Images
Search the Web:
SpoofGuard

The URL that you are about to load may be a spoof.

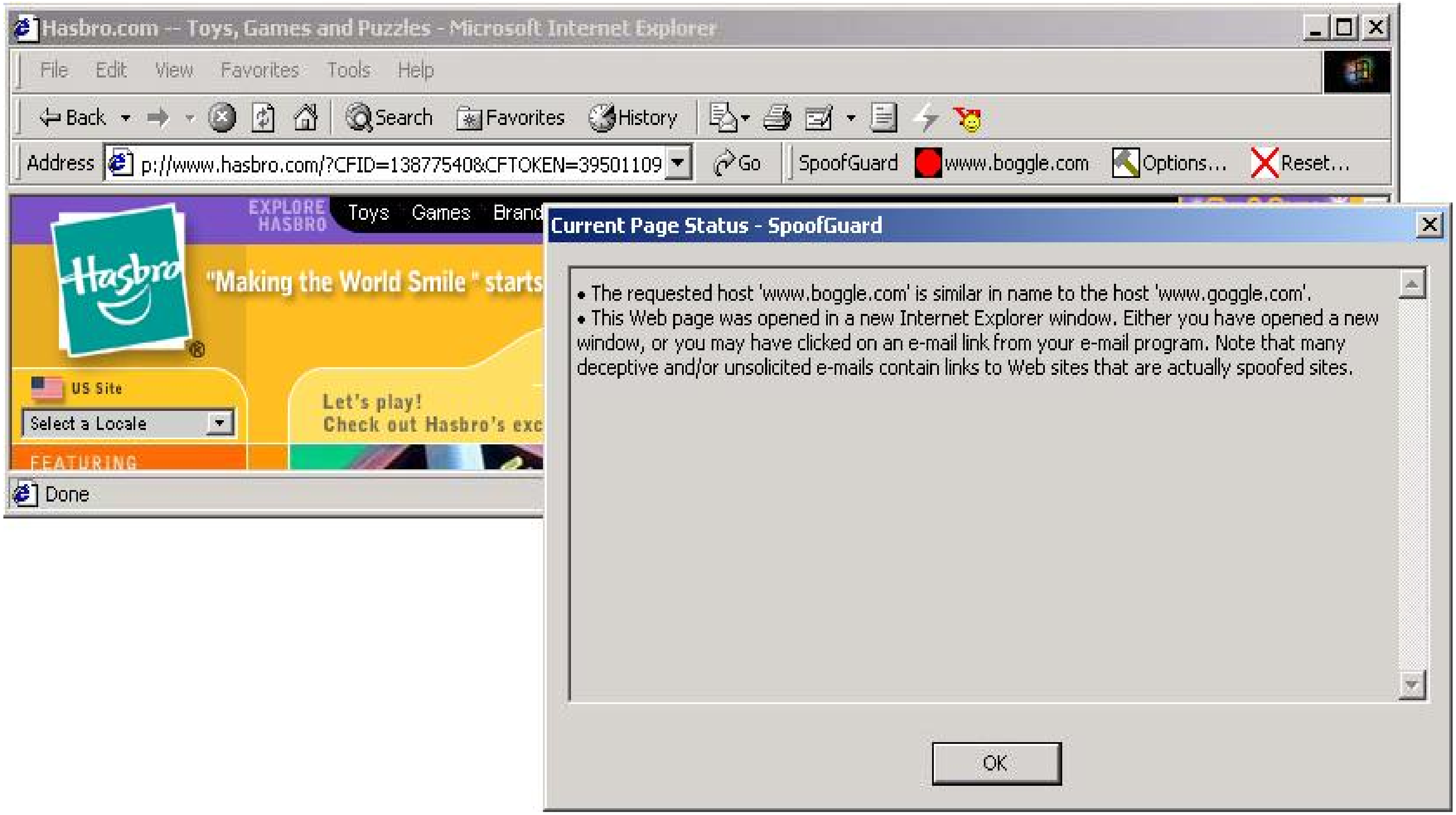
- The requested host 'www.wahoo.com' is similar in name to the host 'www.yahoo.com'.
- The user name 'www.fake.com' may be disguised to look like a host name.
- This page was loaded from the host from port 666. This port is not standard for use on the Web.

Do you want to continue to this URL?

- Press 'Yes' to load the page from 'www.wahoo.com'.
- Press 'No' to cancel the navigation if you believe that this may be a malicious redirection.

EC-Council

SpoofGuard: Screenshot 3



Hasbro.com -- Toys, Games and Puzzles - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address p://www.hasbro.com/?CFID=1387754&CFTOKEN=39501109 Go
SpoofGuard www.boggle.com Options... Reset...
EXPLORE HASBRO Toys Games Brand
Hasbro
"Making the World Smile" starts
US Site
Select a Locale
Let's play!
Check out Hasbro's exc
FEATURING
Done
Current Page Status - SpoofGuard

- The requested host 'www.boggle.com' is similar in name to the host 'www.goggle.com'.
- This Web page was opened in a new Internet Explorer window. Either you have opened a new window, or you may have clicked on an e-mail link from your e-mail program. Note that many deceptive and/or unsolicited e-mails contain links to Web sites that are actually spoofed sites.

Phishing Sweeper Enterprise

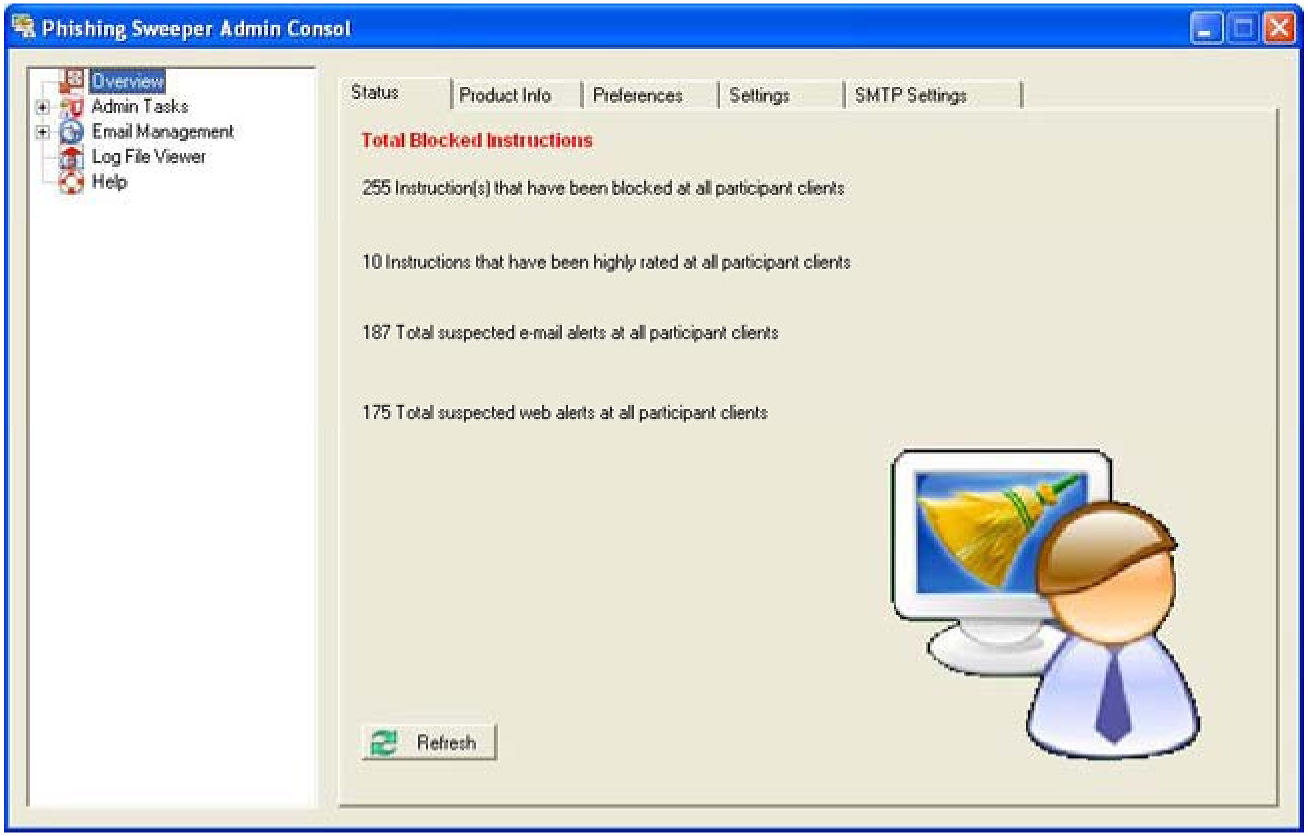
It installs phishing sweeper products throughout the organization

It is an effective utility for spam and spoofed emails

It allows to create groups of users with different policies, produce customized reports, install phishing updates, and view the status of all clients

It provides mail protection, WebSite Protection, Alerts, and Logs

Phishing Sweeper Enterprise: Screenshot



Total Blocked Instructions

255 Instruction(s) that have been blocked at all participant clients

10 Instructions that have been highly rated at all participant clients

187 Total suspected e-mail alerts at all participant clients

175 Total suspected web alerts at all participant clients

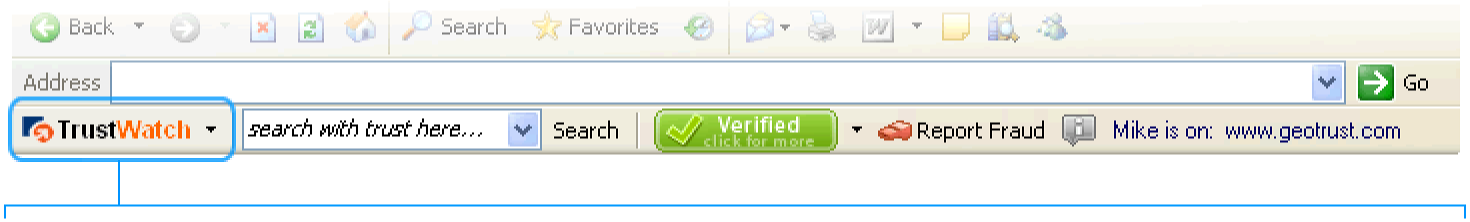
TrustWatch Toolbar

TrustWatch performs a trusted search with built in search box

Intimates the user whether the site is verified and warns for the caution

It provides personal security ID to prevent from toolbar spoofing

Reports the suspected fraudulent sites and indicates the real site the user is in

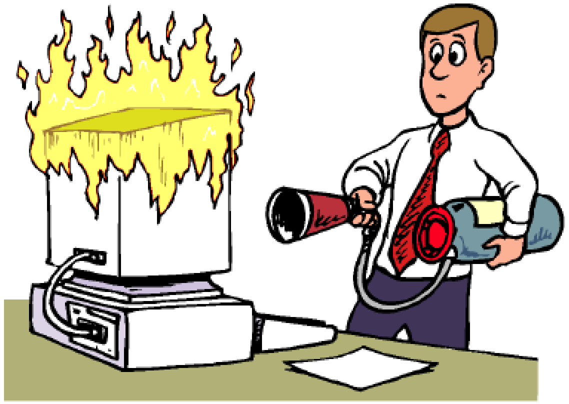


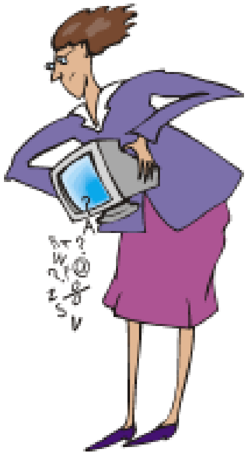
ThreatFire

ThreatFire provides behavior based security monitoring solution protecting from unsafe programs

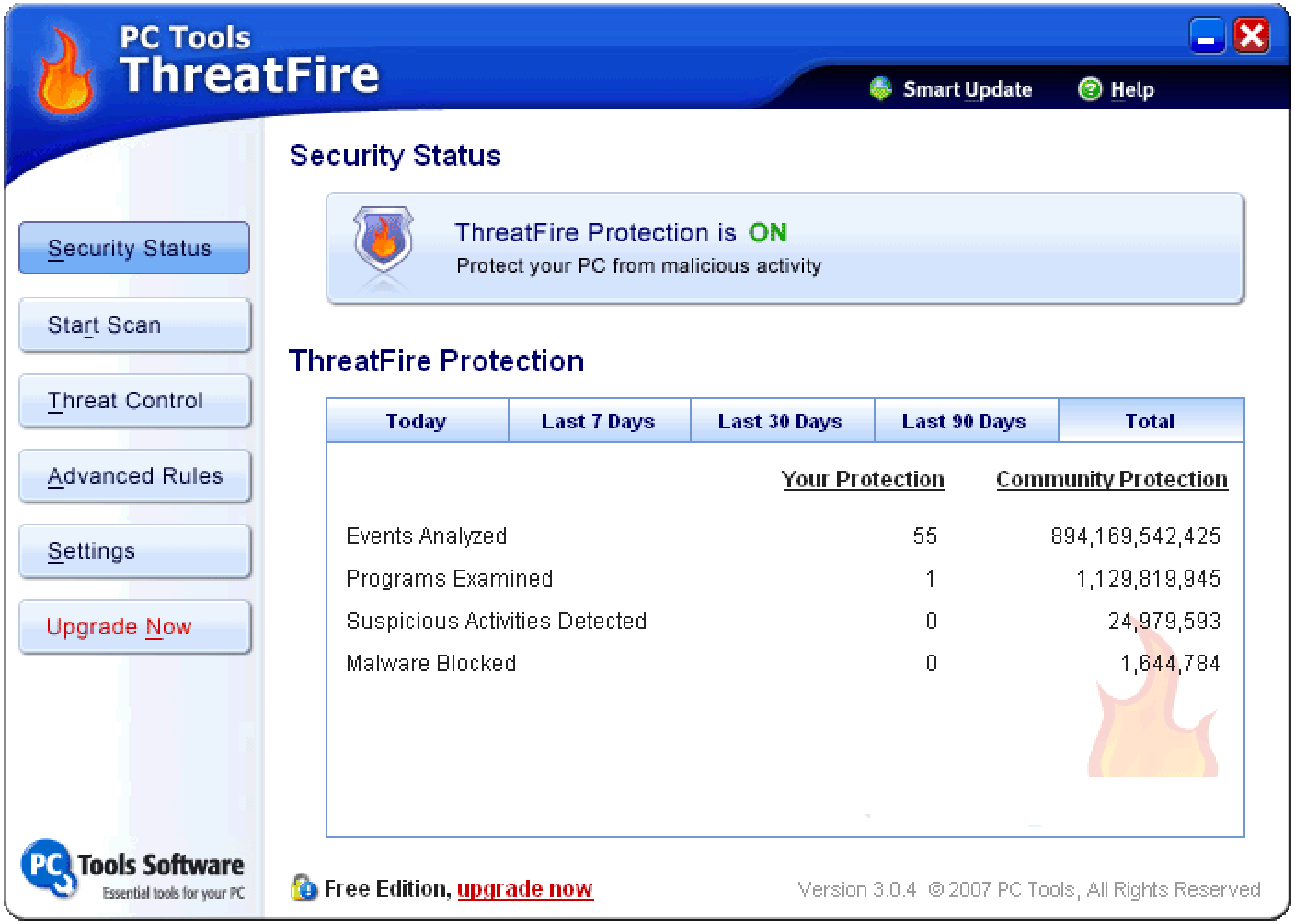
It continuously analyses the programs and processes on the system and if it finds any suspicious actions, it alerts the user

It can be used with the normal antivirus programs or firewalls which adds an additional level of security for the system





ThreatFire: Screenshot



Security Status

ThreatFire Protection is ON
Protect your PC from malicious activity

ThreatFire Protection

Today	Last 7 Days	Last 30 Days	Last 90 Days	Total

	Your Protection	Community Protection
Events Analyzed	55	894,169,542,425
Programs Examined	1	1,129,819,945
Suspicious Activities Detected	0	24,979,593
Malware Blocked	0	1,644,784

Free Edition, upgrade now

Version 3.0.4 © 2007 PC Tools, All Rights Reserved

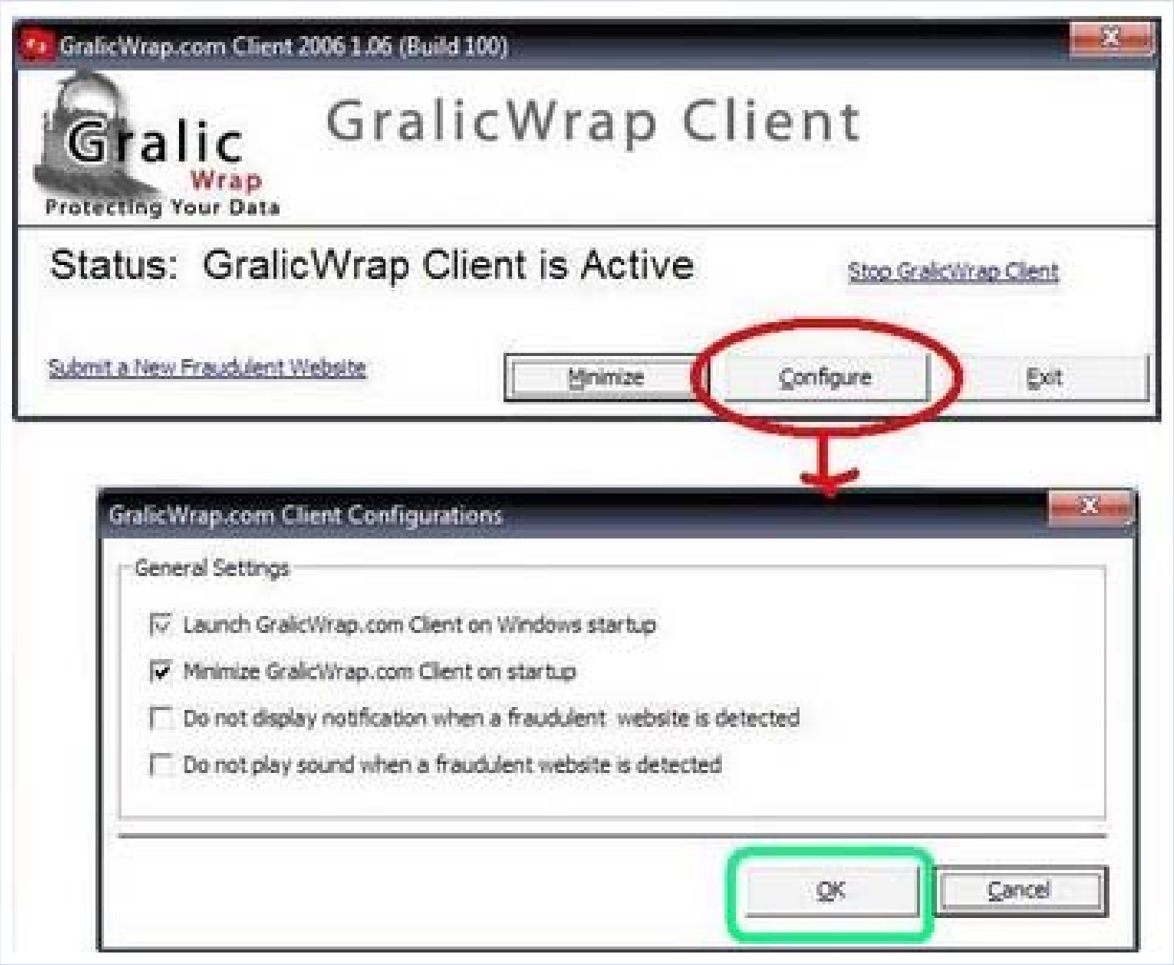
GralicWrap

GralicWrap automatically stops loading the fraudulent websites to prevent data theft

The private data of the user is protected from distributing it to the third party

It updates the fraudulent database automatically at the users system

GralicWrap: Screenshot



Status: GralicWrap Client is Active

Stop GralicWrap Client
Submit a New Fraudulent Website
Minimize
Configure
Exit
GralicWrap.com Client Configurations
General Settings

☑ Launch GralicWrap.com Client on Windows startup

☑ Minimize GralicWrap.com Client on startup

□ Do not display notification when a fraudulent website is detected

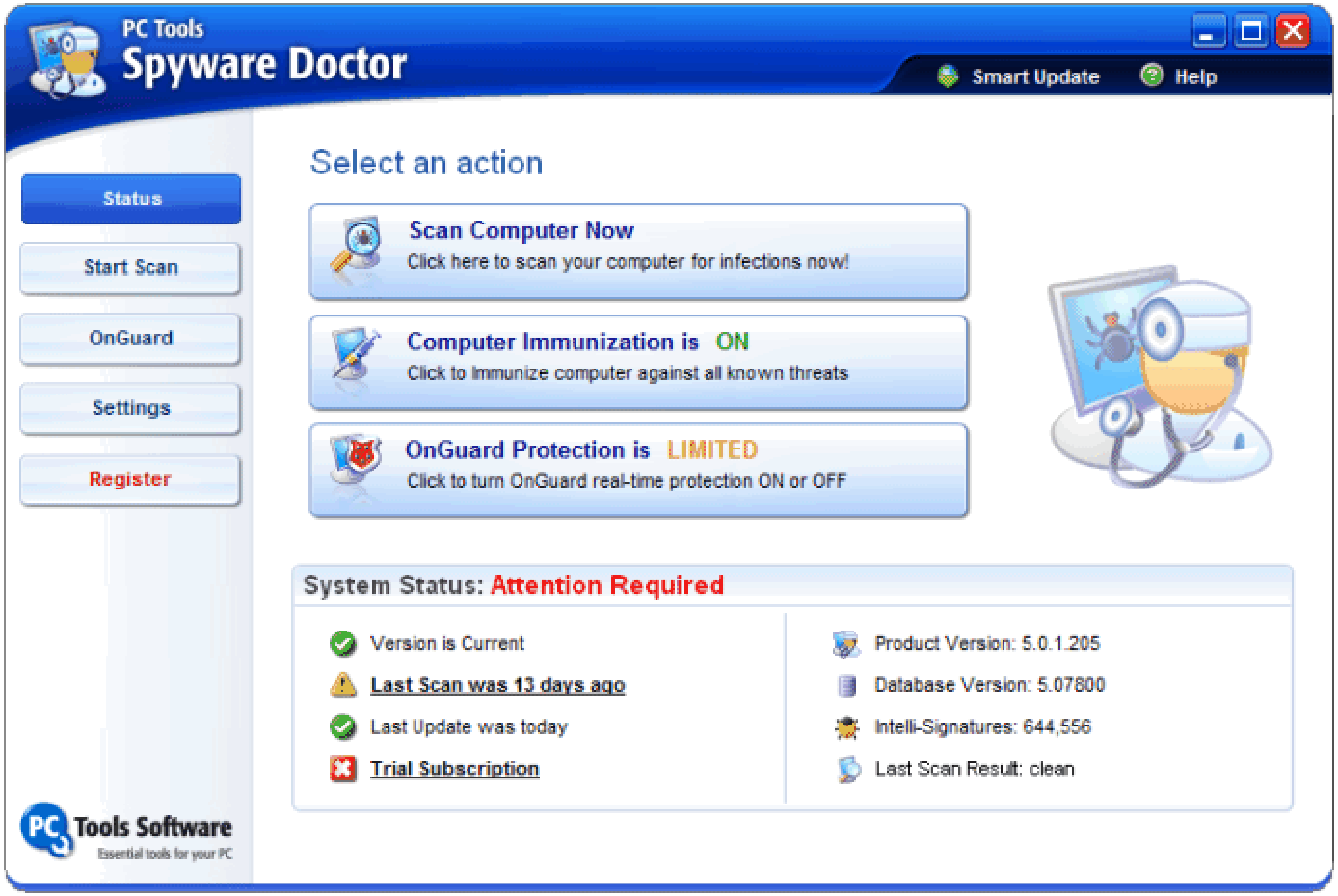
□ Do not play sound when a fraudulent website is detected

Spyware Doctor

Spyware Doctor is an adware and spyware utility which identifies and clears many potential adware, trojans, keyloggers, spyware and other malware of the system

It also features browser monitoring, immunization against ActiveX controls, and automatic cookie deletion

Spyware Doctor: Screenshot



Select an action

Scan Computer Now
Click here to scan your computer for infections now!

Computer Immunization is ON
Click to Immunize computer against all known threats

OnGuard Protection is LIMITED
Click to turn OnGuard real-time protection ON or OFF

System Status: Attention Required

✓ Version is Current	Product Version: 5.0.1.205
⚠ Last Scan was 13 days ago	Database Version: 5.07800
✓ Last Update was today	Intelli-Signatures: 644,556
☒ Trial Subscription	Last Scan Result: clean

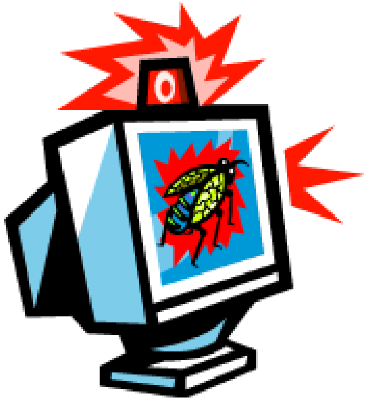
Certified Ethical Hacker

Track Zapper Spyware-Adware Remover

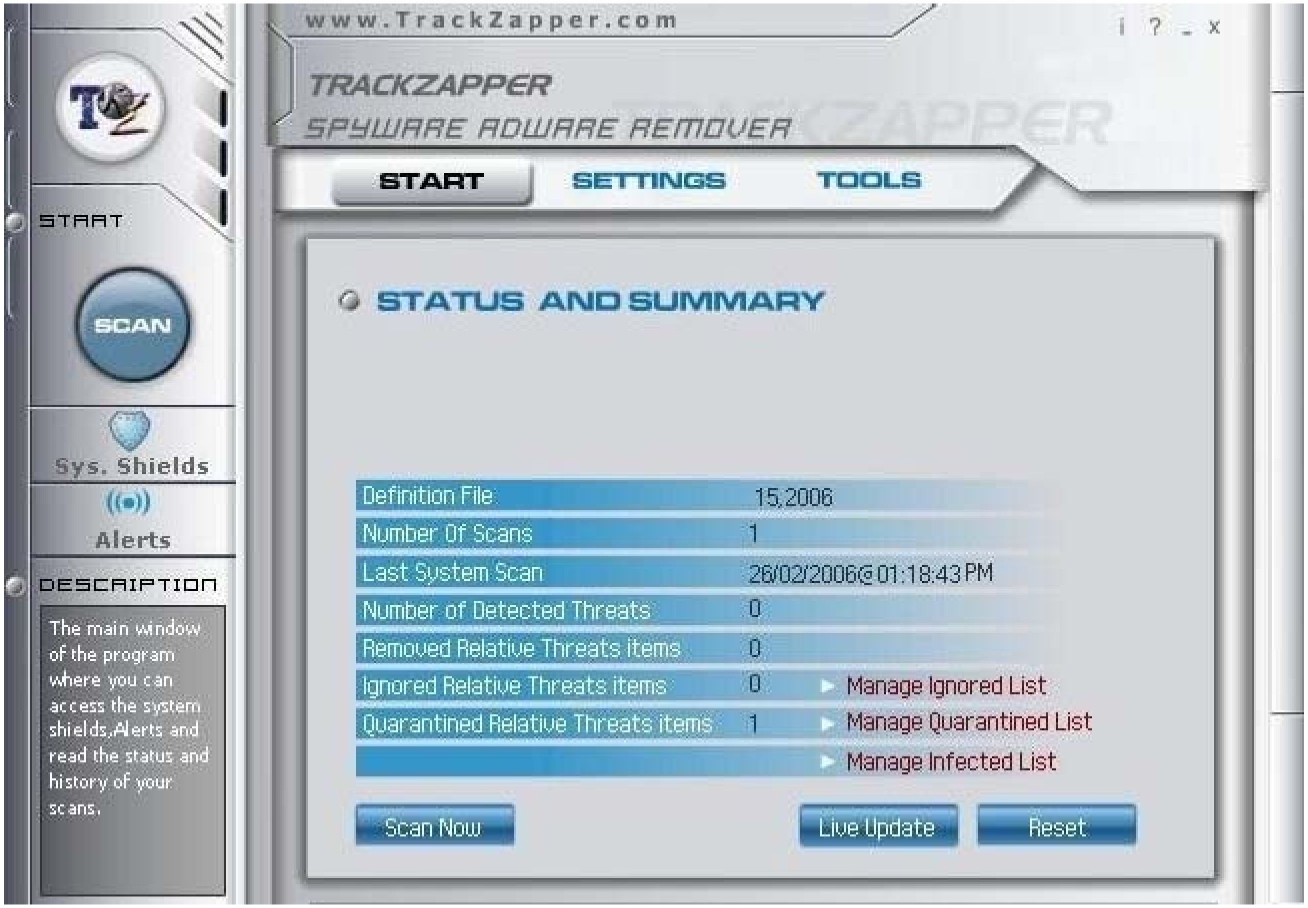
Spyware remover is an Adware, SpyWare, Key Loggers, Trojans, Dialers, Hijackers, Trackware, and Thiefware removal utility with multi-language support

It scans the primary memory, registry, and drives for the known adwares and spywares and lets the user to remove safely from the system

It also features spywatch which monitors and watches the memory



Track Zapper Spyware-Adware Remover: Screenshot



The main window of the program where you can access the system shields,Alerts and read the status and history of your scans.

STATUS AND SUMMARY

Definition File	15,2006	
Number Of Scans	1	
Last System Scan	26/02/2006@01:18:43 PM	
Number of Detected Threats	0	
Removed Relative Threats items	0	
Ignored Relative Threats items	0	▸ Manage Ignored List
Quarantined Relative Threats items	1	▸ Manage Quarantined List
		▸ Manage Infected List

EC-Council

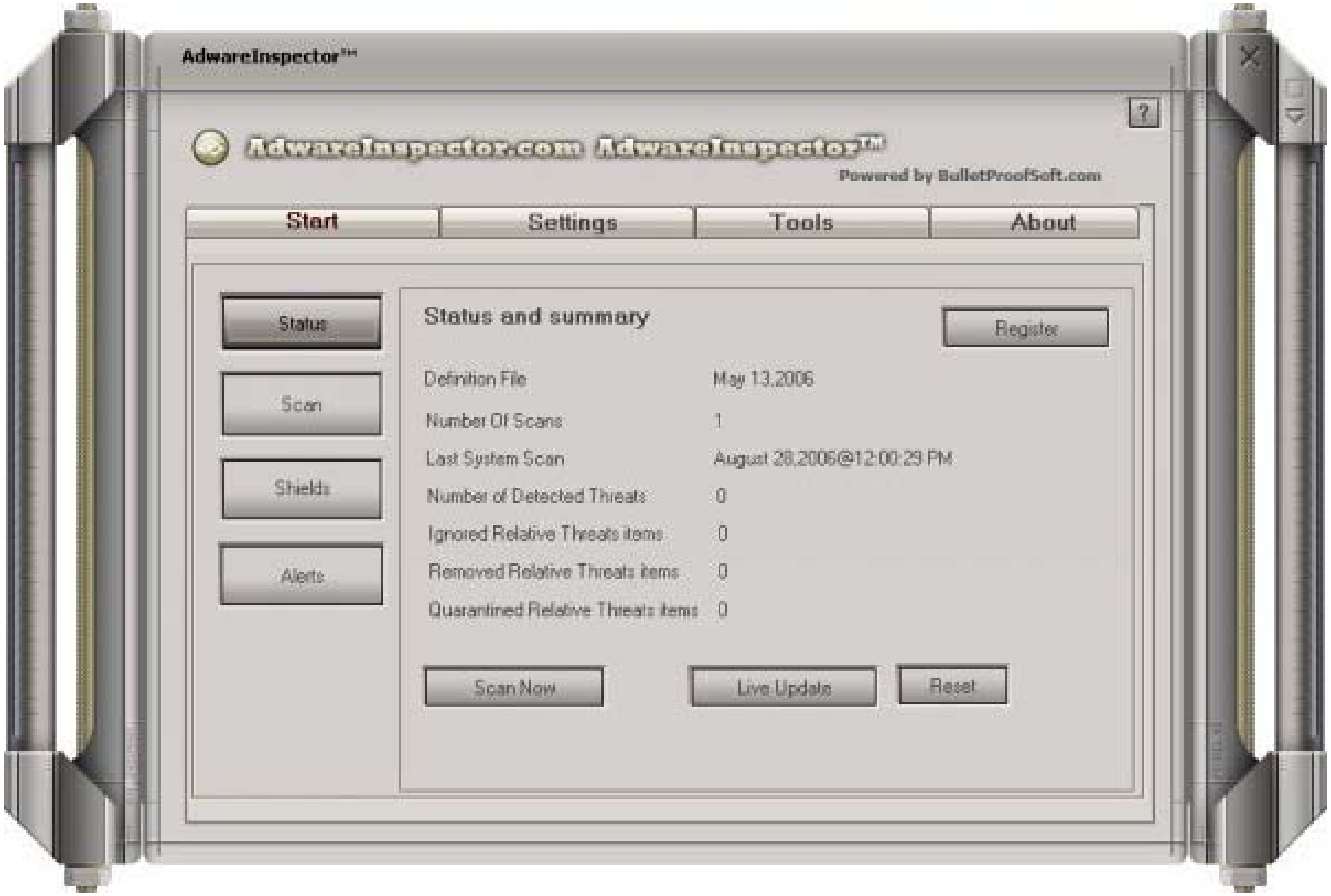
AdwareInspector

Adwareinspector is a program which removes all adwares, spywares, viruses, Dialers, and hijackers that are present in the user's computer

It consists of a database of many fingerprints of spyware adware, trojans, and worms that are updated automatically to alert from latest dangers

It can be set for automatic updating or manual updating

AdwareInspector: Screenshot



Status and summary

Definition File	May 13,2006
Number Of Scans	1
Last System Scan	August 28,2006@12:00:29 PM
Number of Detected Threats	0
Ignored Relative Threats items	0
Removed Relative Threats items	0
Quarantined Relative Threats items	0

Email-Tag.com

Email-Tag.com is used to protect the email accounts, protect the computer, and hide the email address

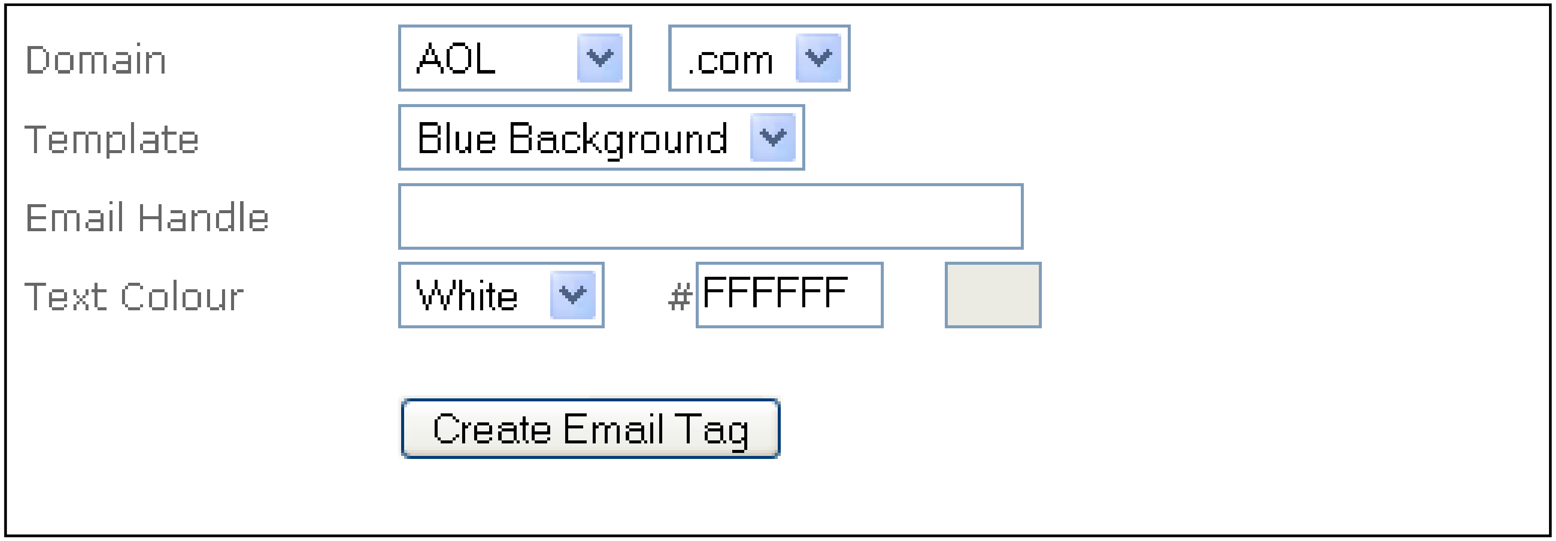
Using this technique, the user’s accounts will be invisible for the spammers

It will generate an email-tag image using the preset templates

Automated email harvesters will read the text and recognizes email address formats and adds them to their spam database

The spammers can be deceived by using images instead of text for email address as email harvesters cannot read images

Email-Tag.com: Screenshot



Domain	AOL	.com
Template	Blue Background	
Email Handle		
Text Colour	White	# FFFFFF

C|EH™ Certified Ethical Hacker

Summary

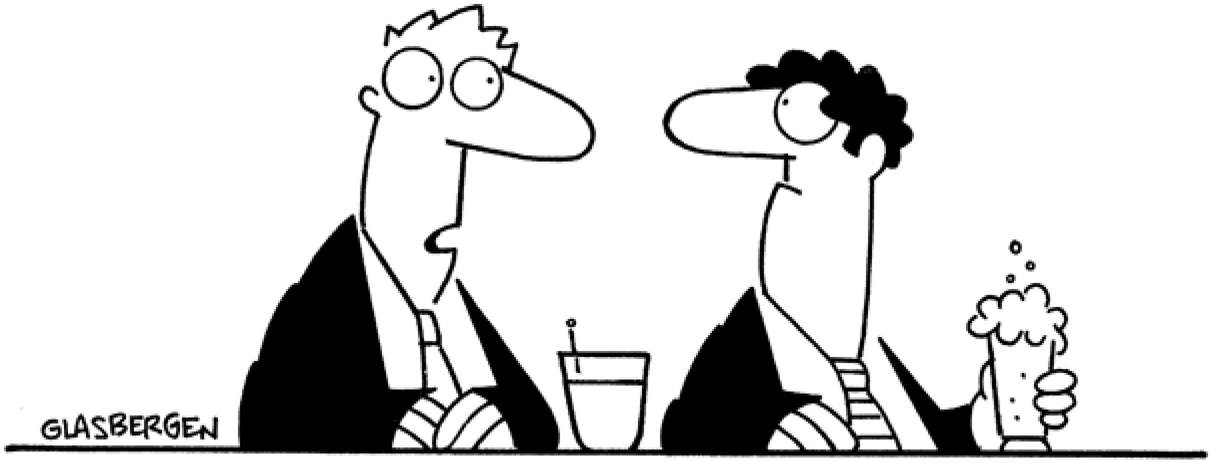
Phishing is an Internet scam where the user is convinced to give valuable information

Lack of computer system knowledge by the user (as how the emails and web works) can be exploited by the phishers to acquire sensitive information

Most of the phishing attacks are done through email

Trojan hosts is a software that is installed at the customer's computer which allows the phishers to access the user's information

Phishing attacks are prevented by anti-phishing software



"While I was thinking outside of the box, someone changed the password and now I can't get back in!"

"We found a solution to your spam problem.
We replaced all of the keys with 'delete' buttons."