Exploring and Investigating New Dimensions In Phishing

Muhammad HAroon

CEO

Sybers Security Solutions

WARNING!

Contents of this presentation are for educational purposes only. Please do not use this knowledge for illegal purposes!

Agenda

Introduction

- **Lesson to Learn**
- **Phishing A Tool Of Identity Theft**
- **Phishing**
  - **Phishing Phacts**
  - **Why Phishing Works?**
  - **Key Findings**
  - **Technical Trickery**
  - **Basic Approach of Attack**
  - **Real life Example**

Continue…

- **What's New Perspective?**
  - **Spear Phishing Using:**
    - Vulnerabilities in Target Application
      - URL redirection bug
      - URL Inclusion bug
    - Address bar Spoofing
- **Real Life Example with Address bar Spoofing**
- **Anti Phishing**
- **Conclusion**
- **Question and Queries**

Introduction

- In computing, **phishing** is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. eBay, PayPal and online banks are common targets. (Wikipedia)
- Fraudsters send fake emails or set up fake web sites that mimic Yahoo!'s sign-in pages (or the sign-in pages of other trusted companies, such as eBay or PayPal) to trick you into disclosing your user name and password. This practice is sometimes referred to as "**phishing**" — a play on the word "fishing" — because the fraudster is fishing for your private account information. (Yahoo)

Lesson To Learn

PHISHING EXPOSED

NO ONE HACK U IF U KNOW

HOW THEY DO IT……

Phishing A Tool Of Identity Theft


http://www.sybers.org

Phishing Phacts

- **Phishtank.com**, a volunteer effort to identify phishing e-mails and associated Web sites, released its first annual report,
- Out of nearly 300,000 sites submitted as suspect, the community verified some 220,000 as phishing scams (more than 70,000 went unverified.)
- Overall, the United States was far and away the country that played host to the largest number of phishing sites in the past few years.

Continue…

- It's important to mention the ISPs because most phishing sites these days are hosted on personal computers that have been hacked by criminals.

Reference: Article By Brian Krebs on Computer Security

Summary December 2007

- No. of unique phishing reports: **15,529**
- Number of unique phishing sites: **11,247**
- Country hosting the most phishing websites in
- December 2007 : United States **30%**
- Contain some form of target name in URL: **46%**
- Average time online for site: **4.8** days
- Most Popular Target: eBay, Inc.

Top 10 Best & Worst Anti-Phishing Web Registrars 2007

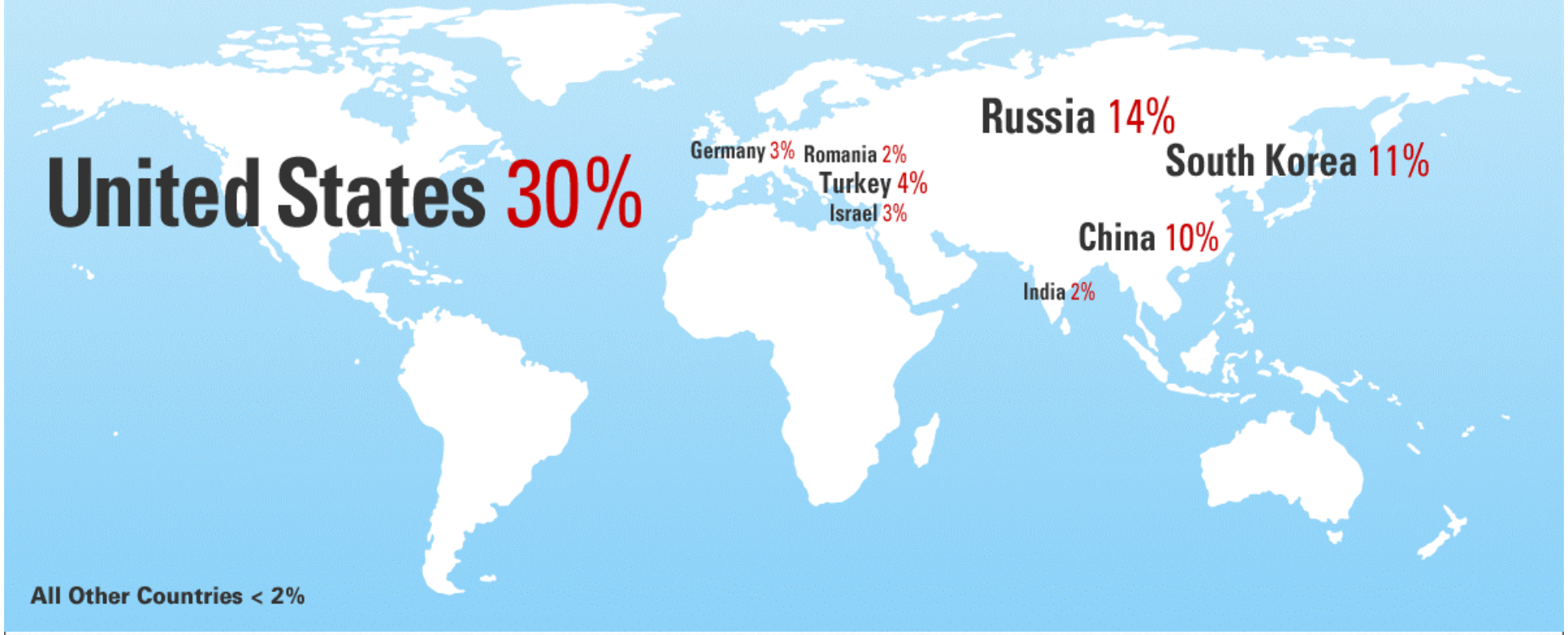
Best Performance	
Registrar	**Avg. Shutdown (hh:mm)**
1. ABR PRODUCTS INC. DBA MISK.COM	0:09
2. NETWORKSOLUTIONS INC.	0:33
3. NAUNET-REG-RIPN	0:40
4. KEY-SYSTEMS GMBH	0:44
5. ALLINDOMAINS LLC	0:48
6. SINCODIA LTD	0:50
7. XENAT	0:51
8. ECURE B.V.	0:52
9. TEPUCOM B.V.	0:52
10. US LOCALITY	0:59

Reference: http://blog.washingtonpost.com/securityfix/2007/12/top_10_best_worst_antiphishing.html

Worst Performance	
Registrar	**Avg. Shutdown (hh:mm)**
1. ELB GROUP INC.	331:17
2. REGISTER.COM	313:00
3. GANDI SARL	264:00
4. 1970930010	264:00
5. REGISTER.COM INC. GUANGDONG TIMES	217:01
6. INTERNET TECH LTD.	217:01
7. WEBRUIMTEHOSTING	216:00
8. DOTNETNAME KOREA CORP	192:00
9. MR MATTHEW BRYANT T/A IDEAL HOSTING	168:00
10. GABIA INC. HTTP://WWW.GABIA.CO.KR	155:16

Phishing Sites By Country of Host, December 2007

PhishTank®



Why Phishing Work??

Just Three Points

- Lack of Knowledge
- Visual Deception
- Sophisticated Attacks

- A usability study in which 22 participants were shown 20 web sites and asked to determine which ones were fraudulent. We found that
- 23% of the participants did not look at browser-based cues such as the address bar, status bar and the security indicators,
- leading to incorrect choices 40% of the time. We also found that some visual deception attacks can fool even the most sophisticated users.

Key Findings

- Good phishing websites fooled 90% of participants.
- Existing anti-phishing browsing cues are ineffective. 23% of participants in our study did not look at the address bar, status bar, or the security indicators.
- On average, our participant group made mistakes on our test set 40% of the time.
- Popup warnings about fraudulent certificates were ineffective: 15 out of 22 participants proceeded without hesitation when presented with warnings.

Reference: Why Phishing Works By Rachna Dhamija Harvard University

Technical Trickery

Deception Methods

Visual Deception

- Does not depends on a specific vulnerability but exploits The Human Element
- Misunderstanding of URLs with trivial modification.
- For example

PAYPAI VS PAYPAI

CITIBANK VS CITIBANK

Continue..

- **Can you read this ?**

  Phishers use ‘fzuzy’ domians to tirck the eye in a smiilar mnaner to tihs apporach.It is less obvuios, but proves effcetive when attacking the viitcm. Tihs is jsut one of the mnay mehtods phihsers exlpoit for web spiofnog.

- Yes I can !

Browser Deception

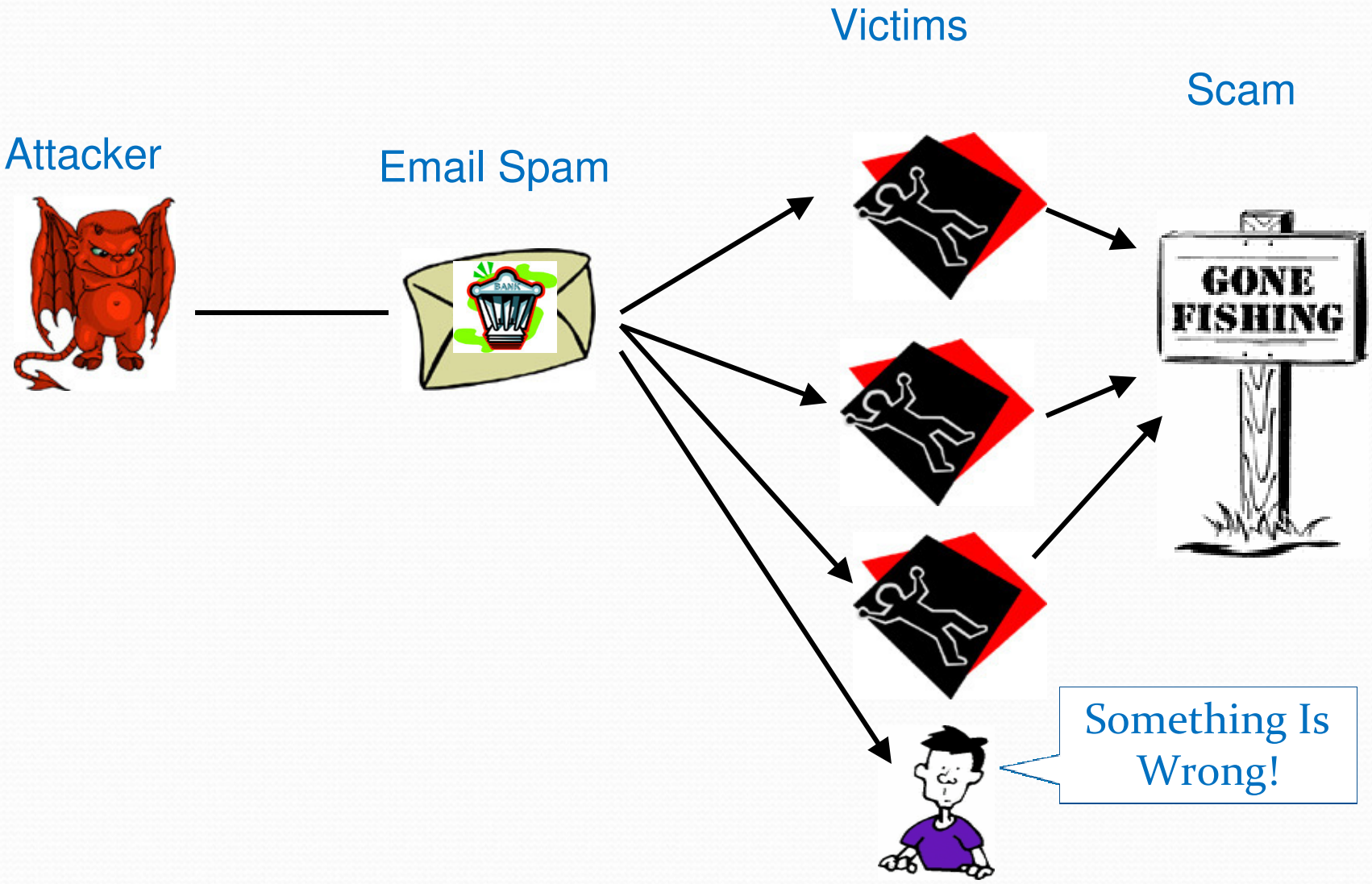
- %@2F in URL is decoded when IE calculates the domain, but not decoded while downloading a page. So, for example,

http://www.yahoo.com%2F@www.somefakepage.com

leads to www.somefakepage.com instead of www.yahoo.com

Basic Approach of Attack

- Attacker sends an email that appears to be from a source the user might trust
- User clicks on an apparently innocuous link in the email and is taken to a site that looks like the right one – but which is actually the attacker's
- User discloses passwords and other sensitive information, e.g. Bank account numbers, credit card information and other personal information

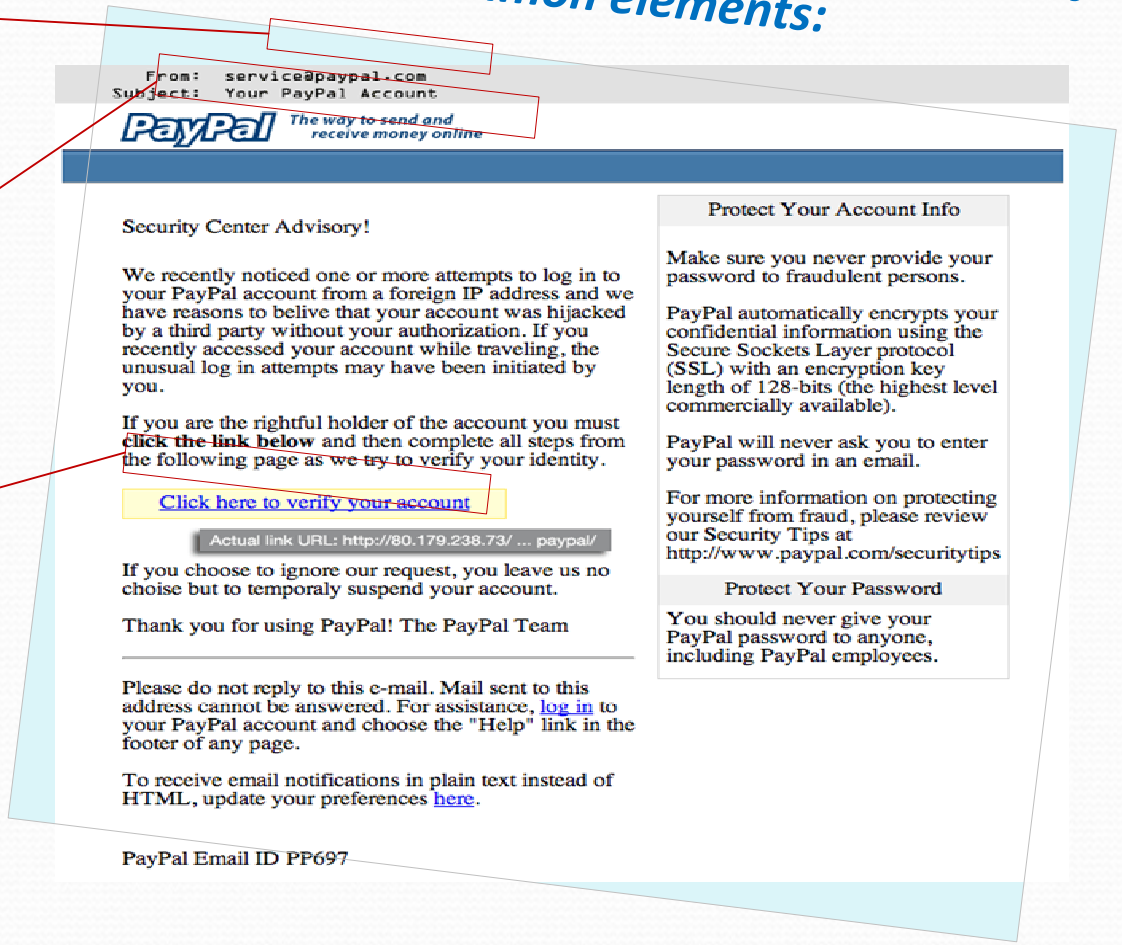

Victims
Scam
Attacker
Email Spam
BANK
GONE FISHING
Something Is Wrong!

Phishing e-mails will contain some of these common elements:

1. Valid Looking Email Address service@paypal.com

2. Genuine Logo To Deceive User

3. Hidden Link! Actually URL is "http://80.179.238.73/...paypal"



From: service@paypal.com
Subject: Your PayPal Account

PayPal The way to send and receive money online

Security Center Advisory!

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to belive that your account was hijacked by a third party without your authorization. If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you.

If you are the rightful holder of the account you must **click the link below** and then complete all steps from the following page as we try to verify your identity.

Click here to verify your account

Actual link URL: http://80.179.238.73/ ... paypal/

If you choose to ignore our request, you leave us no choise but to temporaly suspend your account.

Thank you for using PayPal! The PayPal Team

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

PayPal Email ID PP697

Protect Your Account Info

Make sure you never provide your password to fraudulent persons.

PayPal automatically encrypts your confidential information using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available).

PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at http://www.paypal.com/securitytips

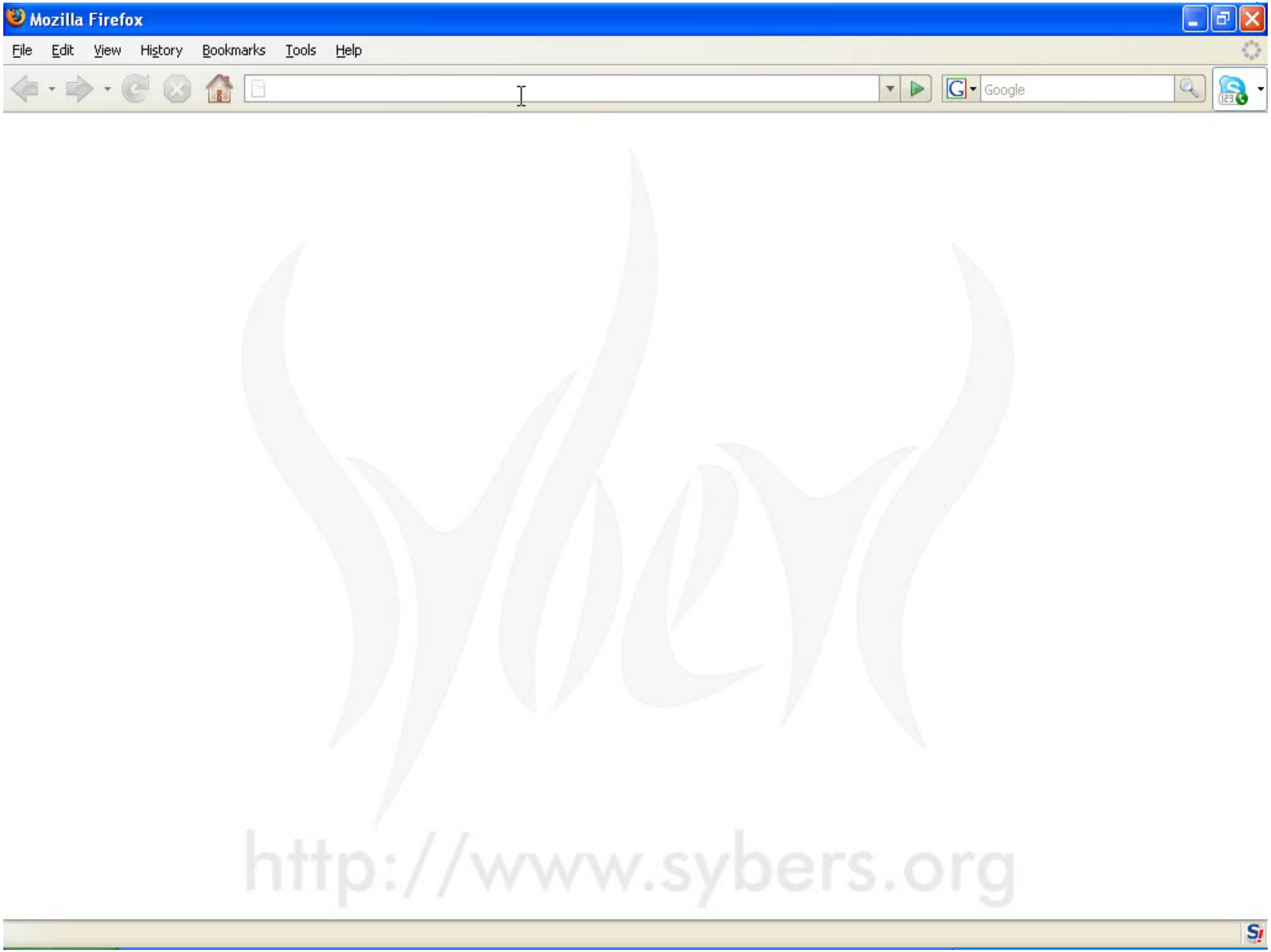
Protect Your Password

You should never give your PayPal password to anyone, including PayPal employees.

The URL Decomposition

- in Phishing email you people looks @ a phake URL send to the victim that is “http://www.somebank.com/verify.php
- The Code Goes Like this:
- www.somebank.com/verify.php

Real Life Example


Mozilla Firefox
File Edit View History Bookmarks Tools Help
Google
http://www.sybers.org

What's New Perspective?

Spear Phishing

- **Spear Phishing is a GREATER threat!!!**
- **Spear Phishing is a highly targeted phishing attempt.**
- **The attacker selectively chooses the recipient (target) and usually has a thorough understanding of the target's command or organization.**

Continue…

- It is carried out with the target of corporate websites or the business companies
- employees of an business organization may be targeted in a group
- the attack on a specific website by sending spoofing emails and ask the other mail users to provide their account information / to click a link
- Using the response, they gain entry into the website and carry out their fraudulent activities.
- the spear phishing aims at gaining access to the business company's complete profile and sensitive business information.

Vulnerabilities in Target Application

- URL Redirection Bug
- URL Inclusion Bug

URL Redirection Flaw

Basic Concepts

- After a user instructs the browser to visit a URL (the primary URL), the browser may visit other URLs (secondary URLs) automatically. The secondary URLs may contribute to inline contents (e.g., Google AdSense ads) on the primary page, or may replace the primary page entirely (i.e., they replace the URL in the address bar)

- **URL redirection** flaw in any application may cause phishiers to pull up even the smartest computer user.

- Examples
- http://somebanksite.com?site=http://www.fakesite.com

Real Life Example


Google - Microsoft Internet Explorer
http://www.google.com.pk/
Google
File Edit View Favorites Tools Help
Links
Web Images News Groups Books Gmail more
iGoogle
Google
Pakistan
Advanced Search
Preferences
Language Tools
Google Search
I'm Feeling Lucky
Search: the web pages from Pakistan
Google.com.pk offered in: اردو
Advertising Programs - About Google - Go to Google.com
©2008 Google
http://www.sybers.org
Internet

Remote URL Inclusion

Basic Concept

- **Remote URL inclusion** that's the best rather worst part of the game.
- Web applications may have the flaw to allow phishers to add there respective URL within the application.
- example.
- http://www.somebank.com/acc.aspx?src=http://www.fakesite.com
- **Confused??**
- Do not mix remote URL inclusion with remote file inclusion.
- Because in RFI:

  The attacker is allowed to include his own malicious code in the space provided for PHP programs on a web page.
- URL inclusion just displays the page content

Real Life Example

MSN.com - Microsoft Internet Explorer

http://localhost/url.php?src=http://www.msn.com

MSN Search

MSN.com

File Edit View Favorites Tools Help

Links

Need a break? Play Chicktionary

Monday, December 31, 2007

Make this your homepage

msn

Web | MSN | Images | News | Maps | Shopping | Video

RSS | Español

Search Web

Popular Searches: Brunch recipes | USC vs. Illinois | Baby New Year

Live Search

Change your page

Welcome

Sign in

Page options

Hotmail
Messenger
My MSN
MSN Directory

Air Tickets/Travel
Autos
Careers & Jobs
City Guides
Dating & Personals

Extra
Games
Green NEW
Health & Fitness
Horoscopes

Lifestyle
Maps & Directions
Money
Movies
Music

News
Real Estate/Rentals
Shopping
Spaces
Sports

Tech & Gadgets
TV
Weather
White Pages
Yellow Pages

NFL Sunday

collapse

Live scores | Stat leaders
Expert picks | Pics: NE vs. NY
Playoff picture | Full coverage

- Patriots keep it perfect
- NFL season awards
- Live: CLE vs. SF

MORE ON MSN

- Holiday booze blunders to avoid
- College hoops scores
- Mysterious flu still baffles after 10 years
- Birth control myths
- Get the most out of small home spaces

< Previous Next >

MSNBC News

- **Huckabee: Romney not trustworthy**
- Bhutto's son, husband to lead party
- Should officials force care on mentally ill?
- Cheap surgeries can carry heavy cost
- Kenya riots as leader re-elected

FOX Sports

- **Live: Follow everything from Week 17**
- Pats are perfect because of Brady, Moss
- 7 hurt in escalator incident at Giants game
- Neuheisel new UCLA coach | Analysis
- St. Pierre wins via submission at UFC 79

Money

- **Desperate stores slash prices**
- Wal-Mart kills its video download service
- Last chance: Cut your '07 tax bill
- What to watch in 2008 stock market
- Don't make Anna Nicole's mistakes

Offer: **Lowest rates** in 2 years! **$400.000**

Why is the MSN homepage wider? Find out

Shopping

- Sexy pumps – put your party shoes on
- Hot gadgets: GPS, iPods, cameras & more

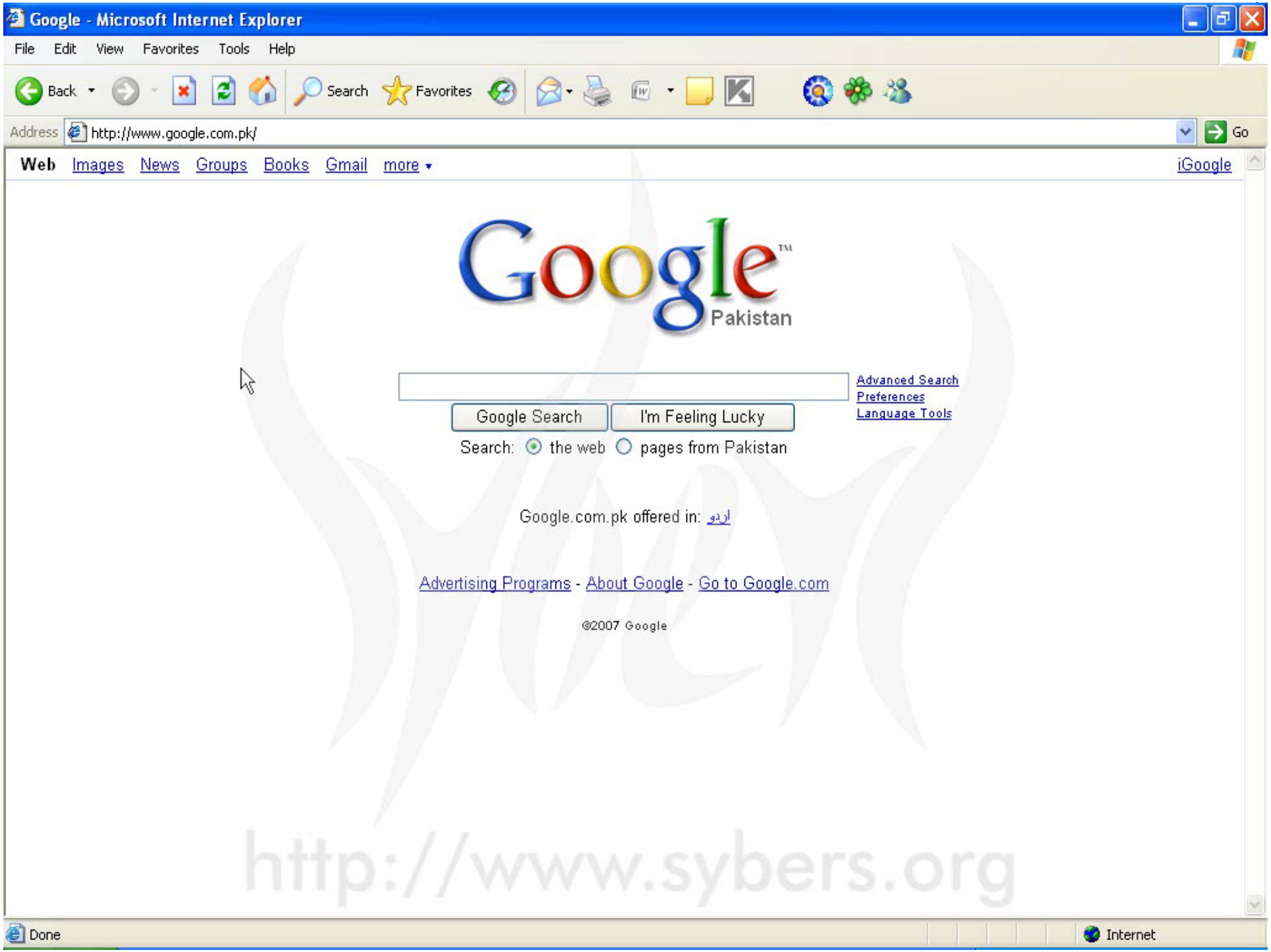
http://search.live.com/results.aspx?q=December+31&mkt=en-us&FORM=MSNHPT

Local intranet

Address Bar Spoofing Example

Web & Address bar Spoofing

- IE Address Bar Spoofing
- This allow attacker to inject a malicious shockwave-flash application into Internet Explorer while it is display another URL (even trusted sites).
- The vulnerability has been confirmed on a fully patched system with Internet Explorer 6.0 + Microsoft Windows XP SP2 and previous versions.


Google - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.google.com.pk/
Go
Web Images News Groups Books Gmail more
iGoogle
Google
Pakistan
Advanced Search
Preferences
Language Tools
Google Search
I'm Feeling Lucky
Search: the web pages from Pakistan
Google.com.pk offered in: اردو
Advertising Programs - About Google - Go to Google.com
©2007 Google
http://www.sybers.org
Done
Internet

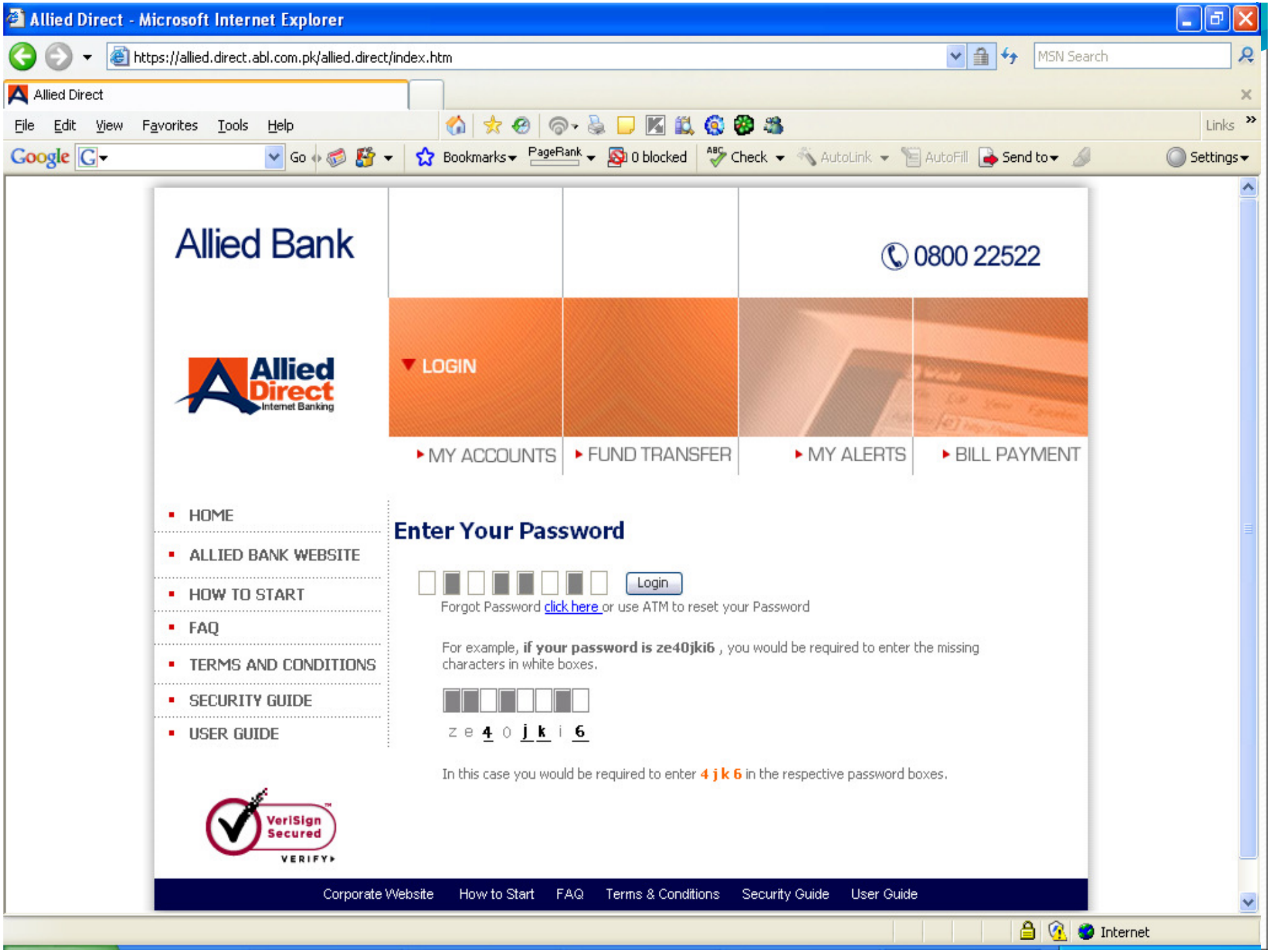
Anti Phishing

Social responses

- Train people to recognize phishing Attempt
- Genuine website can be typed into the address bar of the browser, rather than trusting any hyperlinks
- Contact the company to check that the email is legitimate

Technical responses

- Features embedded in browsers
- Usage of Firefox is recommended
- Browsers alerting users to fraudulent websites
- http://www.mozilla.com/firefox/its-a-trap.html
- As extensions or toolbars for browsers
- The **petname** extension for Firefox lets users type in their own labels for websites, so they can later recognize when they have returned to the site.
- As part of website login procedures
- Augmenting password logins
- https://allied.direct.abl.com.pk/allied.direct/index.htm


Allied Direct - Microsoft Internet Explorer
https://allied.direct.abl.com.pk/allied.direct/index.htm
MSN Search
Allied Direct
File Edit View Favorites Tools Help
Links
Google
Go
Bookmarks
PageRank
0 blocked
Check
AutoLink
AutoFill
Send to
Settings
Allied Bank
0800 22522
Allied Direct
Internet Banking
LOGIN
MY ACCOUNTS
FUND TRANSFER
MY ALERTS
BILL PAYMENT
HOME
ALLIED BANK WEBSITE
HOW TO START
FAQ
TERMS AND CONDITIONS
SECURITY GUIDE
USER GUIDE
Enter Your Password
Login
Forgot Password click here or use ATM to reset your Password
For example, if your password is ze40jki6 , you would be required to enter the missing characters in white boxes.
z e 4 0 j k i 6
In this case you would be required to enter 4 j k 6 in the respective password boxes.
VeriSign Secured
VERIFY
Corporate Website
How to Start
FAQ
Terms & Conditions
Security Guide
User Guide
Internet

Conclusion

The continuing growth in the number of Phishing scams is a serious concern for the entire Internet community. Any individual with access to email or performing on-line business transactions is a potential victim of a Phishing attack. As time goes by, these Phishing scams are becoming more sophisticated and use smarter deception methods.

Phishing attacks exploit Active Content to take advantage of vulnerabilities in web browsers, which offer a plethora of opportunities for malicious/inappropriate behavior. The sophistication of today's attacks requires an intelligent solution that can analyze the actual behavior of that content and determine whether it is malicious/inappropriate or appropriate.

Question
&
Queries??