



# ***Understanding and Preventing Phishing Attacks***

***Feb, 2007***

***by Yoon, Young(Coderant@gmail.com)***

### 1. 피싱(Phishing)의 의미

피싱(Phishing)은 일반적으로 Private Data를 낚시하듯 낚아 채다는 뜻에서 유래된 온라인 사기 기법을 말한다. 피싱은 1996년 처음 등장했으며 공신력있는 단체나 기관의 이름을 사칭한 메일 혹은 메시지를 통해 수신자의 개인정보 혹은 금융정보를 수집하는 사기범죄 수법이다. AOL(American Online) 계정을 훔치기 위해 해커가 불특정 다수의 AOL 회원에게 가짜 인스턴트 메시지를 보내 피해를 입힌 사건이 대표적이라 할 수 있다. 또한 피싱 목적으로 설치되는 피싱 백도어 프로그램을 "Crimeware"라고 한다.

- 피싱용 키로그 백도어(PBK : Phishing-Based Keylogger)
- 강제 URL Redirector(PBR : Phishing-Based Redirector)
- 스니핑(MITM : Man-In-The-Middle Phishing, DNS Cache Poisoning(Pharming))
- Typo-Attack : 유명한 도메인 이름과 유사하게 만든 사이트로 사용자의 Mistyping 를 악용하여 피싱을 유도하는 기술

### 2. Phishing Attacks 기법

피싱은 보편적으로 "당신의 은행계좌가 제3자에게 노출됐다"는 등의 급박한 상황을 강조하면서 개인 정보를 입력하라는 내용의 메일 등으로 개인정보를 요구하는 형식이며 다음과 같은 다양한 방법으로 나타날 수 있다.

Phishing Attack은 사용자를 속이기 위한 각가지 다양한 방법들이 사용된다. 가장 많이 사용되는 공격방법은 다음과 같다.

- URL Obfuscation Attacks
- Man-in-the-middle Attacks
- Cross-site Scripting Attacks
- Preset Session Attacks
- Observing Customer Data
- Client-side Vulnerability Exploitation

### 2.1 URL Obfuscation Attacks

#### 가) URL Address Spoofing

대부분 URL Address Spoofing 기법은 Microsoft 의 Internet Explorer 의 취약점을 이용한 것이 가장 많다. 예를 들면 아래와 같은 IE 의 %01, %00 처리를 못해서 발생하는 취약점으로 인해 Windows 상태창에서 클릭시피싱 사이트 URL 이 보이지 않게할 수 있는 해킹 공격이 가능하다.

##### [사례-1]

사용자는 앞단 링크로 보이지만 실제로는 @뒤에 URL 페이지를 방문하게 된다.

`http://www.trusted_site.com%01%00@phishing_site.com/fakepages.html`

##### [사례-2] Null Byte(%00) 링크

▶ `http://www.microsoft.com %00@phishing_site.com/fakepages.html`

##### [사례-3] Escape Encoding

예를 들면 ASCII 문자의 스페이스(빈공간)는 8진수 코드로 32, Hex 코드는 20, URL-encoded으로는 %20로 표현됨

##### [사례-4] UTF-8 Encoding 방식

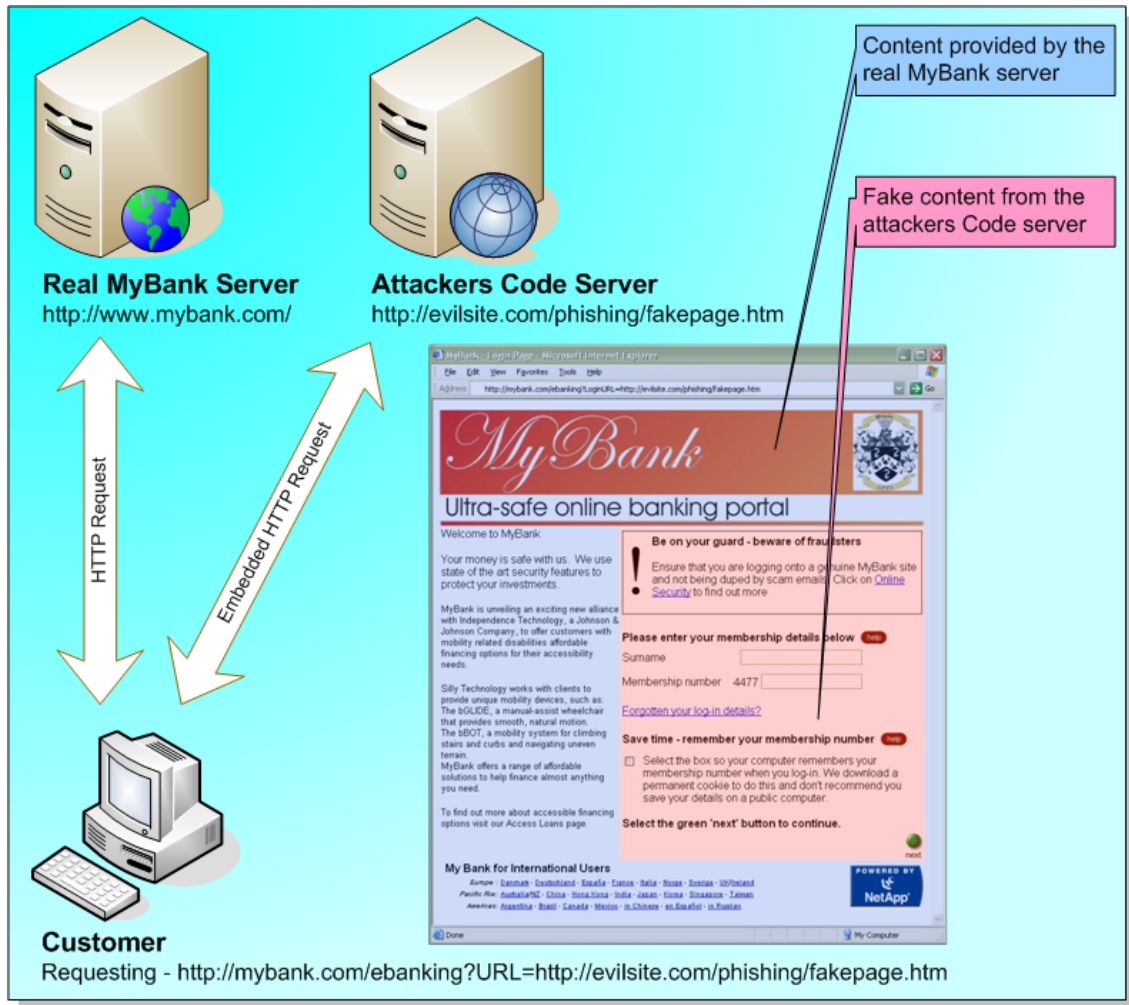
가장 일반적으로 사용하는 피싱 방식중에 하나로 유니코드형태로 URL를 표현하는 방식 예를 들면 "."는 %2E 또는 %C0%AE, 또는 %E0%80%AE, 또는 %F0%80%80%AE, 또는 %F8%80%80%80%AE, 또는 %FX%80%80%80%80%AE로 표현하는 방식

##### [사례-5] Multiple Encoding 방식

예를 들면, back-slash인 "\" 문자는 %25로 인코딩이 된다. 그러나 더블 인코딩 시켜서 %255C, 또는 %35C, 또는r %%35%63, 또는 %25%35%63 이러식으로 변환 시킨다.

#### 나) URL Redirection

URL를 조작하는 피싱공격 방법중 URL Redirection를 활용하는 방법도 많이 사용된다. URL Redirection기법중에서도 구글 검색엔진의 Redirection 기능을 이용하여 Long URL 형태로 공격하는 것이 일반적이다.



[그림] URL Redirection 공격의 구성

[사례-1] URL Redirection 기능을 이용하여 Phisher 사이트로 유도하는 방식

▶ <http://www.google.com/pagead/iclk?sa=l&ai=x&adurl=http://www.hacker.com>

아래의 사례는 URL Redirection를 이용한 Phishing의 경우이다. 첫번째 링크는 그냥 사용자를 속이기 위한 것이다.

- Visible Link : <http://www.citizensbankonline.com/logon/securesurvey.asp>
- Actual Link : <http://review-data.org/go.html>
- Phishing Link : [http://83.16.123.18/icons/pp/update.htm?=https://www.paypal.com/=cmd\\_login\\_access\\_account\\_up](http://83.16.123.18/icons/pp/update.htm?=https://www.paypal.com/=cmd_login_access_account_up)

**PayPal®** [Help](#)

**My Account** | **Send Money** | **Request Money** | **Merchant Tools** | **Auction Tools**

**Overview** | **Add Funds** | **Withdraw** | **History** | **Profile**

### Update your Credit Card or Debit Card

Debit Cards (also called check cards, ATM cards or banking cards) are accepted if they have a Visa or MasterCard logo.






Email Address:

Password:

First Name:

Last Name:

Card Type:

Card Number:      

Expiration Date: MM / YY

Card Verification Number:  (On the back of your card, find the last 3 digits) [Help finding your Card Verification Number](#)

Name On Card:

Mothers Maiden Name:

Social Security Number:

Date Of Birth: Month / Day / Year

Card Pin:  4 Digit code used in ATMs. (For verification with bank)

Billing Address

Enter the address where you receive monthly billing statements for this card:

**Enter billing address**

Address 1:

Address 2:  (optional)

City:

Phone Number:

State:

Zip Code:  (5 or 9 digits)

Country:

**For your protection, we verify credit card and debit card billing addresses.**  
The process normally takes about 30 seconds, but it may take longer during certain times of the day.  
Please click **Continue** to update your information. When your card has been successfully added, you will see a confirmation page.

[Continue](#)

[Mobile](#) | [Mass Pay](#) | [Money Market](#) | [ATM/Debit Card](#) | [BillPay](#) | [Referrals](#) | [About Us](#) | [Accounts](#) | [Fees](#) | [Privacy](#) | [Security Center](#) | [User Agreement](#) | [Developers](#) | [Shops](#) | [Gift Certificates/Points](#)

**an eBay Company**

Copyright © 1999-2004 PayPal. All rights reserved.  
[Information about FDIC pass-through insurance](#)

실제 Phishing 사이트는 아래 주소로 정보를 전송한다.

Address  [http://83.16.123.18/icons/pp/update.htm?https://www.paypal.com/cmd\\_login\\_access\\_account\\_uptead\\_currency%%%di](http://83.16.123.18/icons/pp/update.htm?https://www.paypal.com/cmd_login_access_account_uptead_currency%%%di)

[사례-2] XSS(Cross Site Scripting)를 이용한 URL Redirection 기법

스크립트에 Inline embedding 코드를 숨긴다.

▶ [http://bank.com/banking?page=1&client=<SCRIPT>document.location\(evilcode\)](http://bank.com/banking?page=1&client=<SCRIPT>document.location(evilcode))

외부 스크립트를 실행시켜 강제로 웹페이를 피싱사이트로 유도시킨다.

▶ <http://mybank.com/banking?page=1&response=fake.com%21evilcode.js&go=2>

결국 사용자는 아래 예에서 보는 것처럼 다음과 같은 URL을 클릭하게 된다.

▶ <http://mybank.com/ebanking?URL=http://evilsite.com/phishing/fakepage.htm>

### 다) Bad 도메인 Name

[사례] 유사 URL을 이용하여 사용자가 혼동하도록 하는 방법

정상적인 <http://www.mybank.com/> 대신에 <http://www.mybank.com.ch> 처럼 유사형태의 도메인을 악용하는 방법을 사용하기도 한다.

### 라) Friendly Login URL's

[사례] 일반적인 피싱기법으로 인증한 정보처럼 위장하여 URL 을 조작하는 방법

▶ <http://mybank.com:ebanking@evilsite.com/phishing/fakepage.htm>

### 마) Host Name Obfuscation

Phishing Crimer 가 URL 의 도메인 네임대신 IP 주소를 사용하여 도메인 이름을 혼란스럽게 하여 콘텐츠 필터링을 피하거나 목적지를 속이기 위한 방식으로 IP 주소를 Hex, Oct, 십진수 등 다양하게 나타낼 수 있다.

[사례-1] 도메인 이름대신 IP주소로 표현을 다음과 같이 바꿔서 표현한다.

▶ <http://mybank.com:ebanking@evilsite.com/phishing/fakepage.htm>

→ <http://mybank.com:ebanking@210.134.161.35/login.htm>

[사례-2] 십진수 IP 주소를 다양하게 표현 사용하는 방식

- 십진수 IP 주소 : <http://210.134.161.35/>
- Dword IP 주소로 표현 : <http://3532038435/>
- 8진수 IP 주소 표현 : <http://0322.0206.0241.0043/>
- HEX 주소 표현 : <http://0xD2.0x86.0xA1.0x23/> 또는 <http://0xD286A123/>

- 특별한 경우에는 포맷 혼합도 가능(e.g. <http://0322.0x86.161.0043/>).

### 2.2 Sooping E-mail Phishing

위장된 메일 주소를 이용한 Phishing 기법으로 실제 도메인과 IP 주소가 다르게 되어 있다.



[그림] Citibank 의 E-Mail Spoofing 사례

### 2.3 DNS 관련 공격(Multiple Scams & One Domain, DNS Posioning)

다수의 Phishing Scam 공격시 단일 도메인이 사용된다. 아래의 예는 “mujweb.cz”라는 단일 도메인이 사용된 Phishing Scam 사례이다.

[사례-1] 단일 도메인에 Multiple Phishing Scam

- Domain : mujweb.cz



- Phishing Targets : eBay, PayPal, Wachovia

[사례-2] Phishing Site 는 Free Web Hosting 사이트에서 많이 만들어진다

Phishing sites 는 공짜로 제공되는 웹 호스팅 서비스(Geocities)에 주로 만들어 진다.

- Domain: 81.113.212.146
- Phishing Targets : eBay, Barclays Bank, Citi Bank

[사례-3] 로컬 PC 의 LMHOST 및 host 파일의 변조를 통한 위조된 Phishing 사이트 유도  
백도어 웜바이러스에 의한 로컬 PC의 host 변조를 통한 피싱

## 2.4 IDN spoofing

IDN(Internationalized Domain Names)이란 영문자 대신 각 지역 언어의 문자를 그대로 사용하는 다국어 도메인 이름이다. IDN Spoofing은 거의 유사한 문자(예를 들면, 라틴어 또는 로마자와 비슷한 러시아 문자인 키릴문자를 사용)를 사용하는 방식이다.

아래 예는 paypal.com의 경우로 라틴문자 "a"를 키릴문자로 대체한 것이다. 거의 모양이 흡사하여 혼동하기 쉽다.

[사례] #1072는 십진수로 표시이며 'a'를 나타낸다.

- ▶ <http://www.p#1072ypal.com> (Original <http://www.paypla.com>)
- ▶ <http://www.paypal.com>

[사례-2] Red로 표시된 문자는 알파벳 'o'가 아니라 키릴문자 'o'이다.

- ▶ <http://www.theshmo#1086group.com/>(<http://www.theshmoogroup.com>)
- <http://www.theshmoogroup.com/>

ASCII코드 및 Unicode 문자열을 DNS에서 문자셋을 다른 문자(키릴문자)로 맵핑되지 않도록 제한해야 한다.(Punycode 사용)



### 2.5 Hidden Attacks

Hidden Attack 에 가장 일반적으로 사용되는 공격은 다음과 같다.

- Hidden Frames
- Overriding Page Content
- Graphical Substitution

#### 가) Hidden Frames

프레임(Frame)은 숨김(Hidding) 공격에 가장 많이 사용되는 방법이다.

다음 예는 두개의 프레임이 정의되어 있는 것을 보여준다. 첫번째 프레임은 정상적인 URL 정보가 포함되어 있고, 두번째 프레임은 숨겨진 프레임은 Phishing 페이지를 참조하도록 하고 있다. 숨겨진 프레임내에는 Phishing 콘텐츠로 링크되어 있다. 이러한 공격(AJAX 를 이용한 스크립 캡처, 키로깅)을 통해 세션 ID 또는 민감한 정보가 노출될 수 있다.

```
<frameset rows="100%,*" framespacing="0">
<frame name="real" src="http://mybank.com/" scrolling="auto">
<frame name="hiddenContent" src=http://evilsite.com/bad.htm
scrolling="auto">
</frameset>
```

Hidden 프레임이 사용되는 목적은 다음과 같다.

- Aattacker 서버의 주소를 숨기기 위한 목적
- Master URL 만 frameset document 가 브라우저에서 보인다. 단, 속성을 "\_top"으로 설정하지 않은 경우에 해당됨
- Hiding HTML code from the 사용자의 HTML 코드를 숨기기. 소스보기 즉, "View Source" 기능을 사용하여 숨겨진 페이지 코드를 볼 수 없게 된다.
- 악의적인 어플리케이션(Malicious application)에 의해 백그라운드 형태로 HTML 콘텐츠 및 Image 를 로딩한다.
- Client-side scripting languages 와 같이 결합되어지면, 브라우저 툴바 기능을 복제하는 것이 가능하다.(URL 정보와 페이지 헤더정보를 포함)

### 나) Overriding Page Content

Overriding Page Content 방법은 가장 많이 사용되는 fake content 삽입 방식으로 실제 웹 페이지 화면에 숨겨진 웹 페이지를 삽입시키는 방법이다.

DHTML 함수(DIV)를 사용하여 페이지에 위장된 페이지를 삽입하는 공격이 가장 많이 사용된다.

DIV 함수는 STYLE 메소드를 통해서 위치와 크기를 조정하여 “virtual container”안의 콘텐츠의 위치(Position)를 숨기거나 또는 대체(Replace)시킬 수 있다.

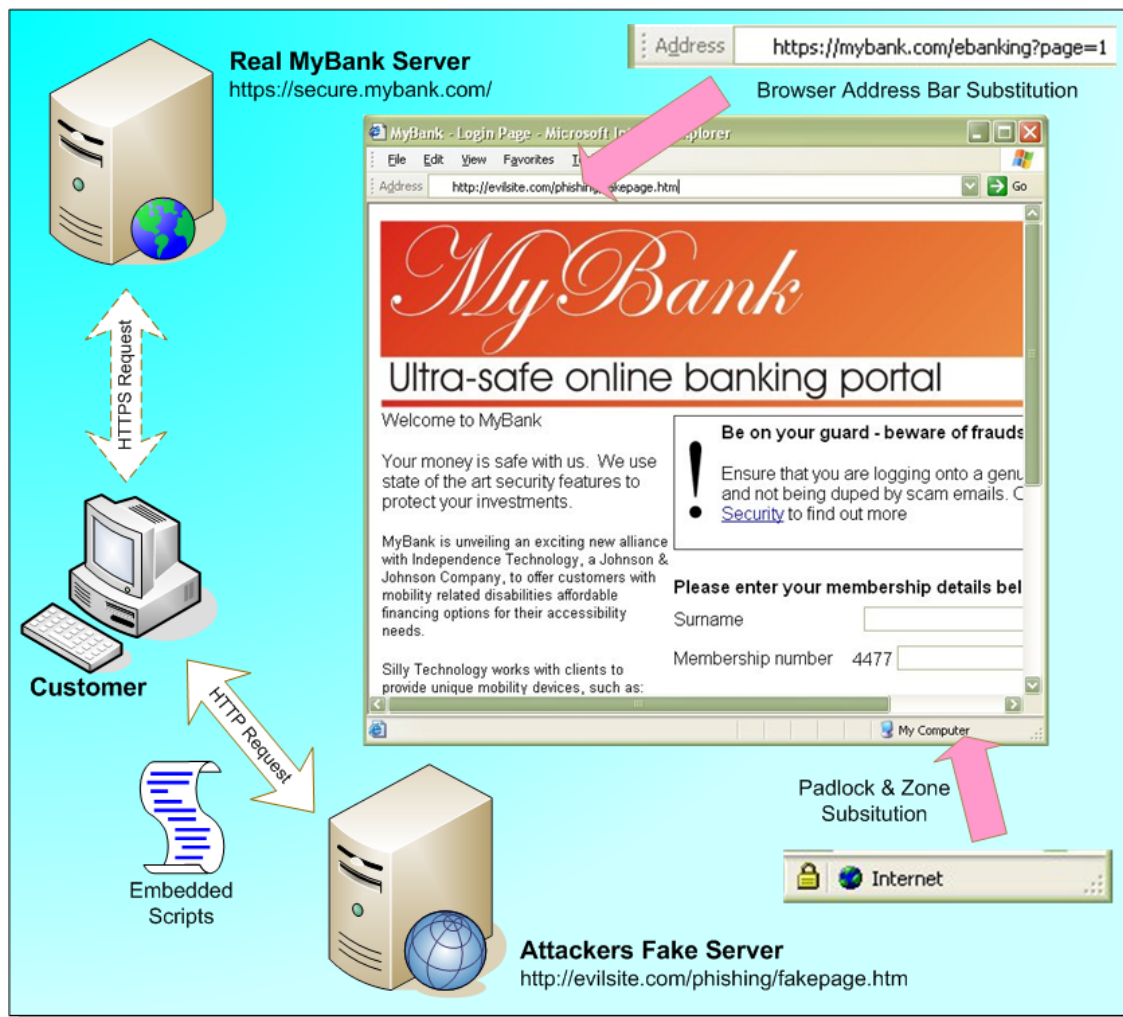
다음 예는 fake.js 자바 스크립트의 처음 3줄의 코드에 의해서 페이지 내용이 덮어쓰여 질 수 있음을 나타내고 있다.

```
var d = document;
d.write('<DIV id="fake" style="position:absolute; left:200; top:200;
z-index:2">
<TABLE width=500 height=1000 cellpadding=14><TR>');
d.write('<TD colspan=2 bgcolor=#FFFFFF valign=top height=125>');
.....
```

이 방법은 공격자 실제 웹 페이지 상단 위에 하나의 완전한 페이지(이미지와 스크립트 코드를 포함)를 생성하도록 할 수 있다. 그리고 간단한 HTML embedded commands를 사용하면, 공격자가 사용자의 세션을 하이잭킹 할 수 있다.

다음은 window.createPopup()과 popup.show() commands를 사용한 예이다.

```
op=window.createPopup();
op.document.body.innerHTML="...html...";
op.show(0,0,screen.width,screen.height,document.body);
```



[그림] Hidden Frame Attak 의 구성

### 3. 대응 방안

Phishing 공격에 대한 최선의 방안은 클라이언트 단에서는 Phishing 공격을 차단하기 위한 다양한 보안 솔루션에 필요하다.

- 사용자 PC 보안(안티바이러스, 스파이웨어 차단, 그레이웨어 차단)
- 사용자 어플리케이션 레벨의 모니터링 솔루션 설치
- 이메일에 대한 디지털 서명(Digital signing and validation of email)
- 피싱 탐지 및 차단 솔루션

#### 가) Desktop Protection Agents

사용자는 백신, PC 방화벽 같은 기본 PC 보안 솔루션을 설치해야 한다.

- Anti-Virus protection
- Personal Firewall
- Personal IDS 및 Anti-Spam
- Spyware Detection
- 로컬 PC의 host 변조여부 차단

특히, Trojan horses, key-loggers, screen-grabbers과 backdoor 설치를 탐지해야 한다.  
(이메일의 첨부파일, 파일 다운로드, 동적 HTML과 스크립트를 통한)

#### 나) Browser Capabilities

가장 일반적으로 Phishing 공격은 웹 브라우저를 통해서 차단할 수 있다. 웹브라우저의 차단은 주기적인 IE 패치를 통해서 Phishing Attack에 악용될 수 있는 취약점을 제거하는 것이 좋다. (평균적으로 거의 1일 단위로 새로운 MS 취약점이 발견되고 있고 그중에서 IE를 이용한 해킹공격의 빈도가 가장 높음)

- 신뢰할 만한 사이트를 제외하고 모든 윈도우 팝업창 기능은 Disable
- Disable Java runtime support
- 신뢰할 만한 사이트 이외의 ActiveX Disable
- 모든 멀티미디어의 자동 플레이 및 실행을 Disable
- 안전하지 않은 쿠키 저장을 방지

### 다) Anti-Phishing 솔루션

단순한 Phishing Black List 기반으로 탐지하는 것은 한계가 있으며, 기본적으로 Phishing에 악용될 수 있는 모든 해킹기법을 차단할 수 있어야 한다.

- URL Spoofing Attack
- URL Obfuscation(유사 도메인 탐지, URL IP 주소 Obfuscation, IDN Obfuscation)
- URL Redirection
- DNS Pharming

### 라) DNS 파밍 차단

로컬 PC에 DNS에 대한 유효성에 대한 필터링(Proxy 서버 설정여부 탐지)

- 국내 ISP의 DNS 서버가 아닌 국외 DNS 서버여부 점검(Proxy 서버)
- 로컬 PC의 host 파일 변조 여부 차단
- DNS 서버의 유효성 검증

## 4. 결론

Phishing은 기존의 해킹보다 범죄적 성격이 강해 웹과 인터넷을 비즈니스 인프라로 사용하는 기업에게는 경영상 중대 위협요인이 되고 있다. 따라서 피싱에 대해서는 적극적인 대응이 필요하다. 또한 과거의 보안의 트렌드가 주로 기업의 서버 및 인프라 네트워크가 대상이었다면 향후의 핵심적인 보안 트렌드는 클라이언트를 대상으로 하는 것이 될 것이다.

## [별첨] Phishing Scam 통계 자료

### 1. Networks That Host Phish

(2007 년 2 월 기준 PhishingBank 자료 참조)

Top 10 Networks		Valid Phishes
1	Hanaro Telecom Inc.	469
2	National Internet Backbone	333
3	TELESC Telecomunicacoes de Santa Catarina SA	224
4	EMCATEL	211
5	Instituto Costarricense de Electricidad y Telecom.	190
6	CQNET Chongqing Broadband Networks	163
7	Futures Cable Television, Inc.	143
8	SAVVIS Savvi	101
9	CANTV Servicios C.A.	93
10	MobiFon S.A.	89

## 2. Popular Targets

(2007 년 2 월 기준)

Top 10 Identified Targets		Valid Phishes
1	PayPal	2,693
2	Barclays Bank PLC	1,972
3	eBay, Inc.	1,423
4	Fifth Third Bank	1,302
5	Bank of America Corporation	1,048
6	JPMorgan Chase and Co.	643
7	Volksbanken Raiffeisenbanken	379
8	Wells Fargo	233
9	HSBC Group	149
10	Citibank	120

### **[참고 사이트]**

#### **[1] The Phishing Guide – Part2**

*<http://www.technicalinfo.net/papers/Phishing2.html>*

#### **[2] NGSSoftware**

*<http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf>*

#### **[3] Anti-Phishing Working Group**

*<http://www.antiphishing.org>*