

---

# Cybercrimes against the Korean online banking systems

---

2013. 01. 10

Youngjun Chang (zhang95@ahnlab.com)

Senior Advanced Threat Researcher, CISSP

ASEC (AhnLab Security Emergency response Center)

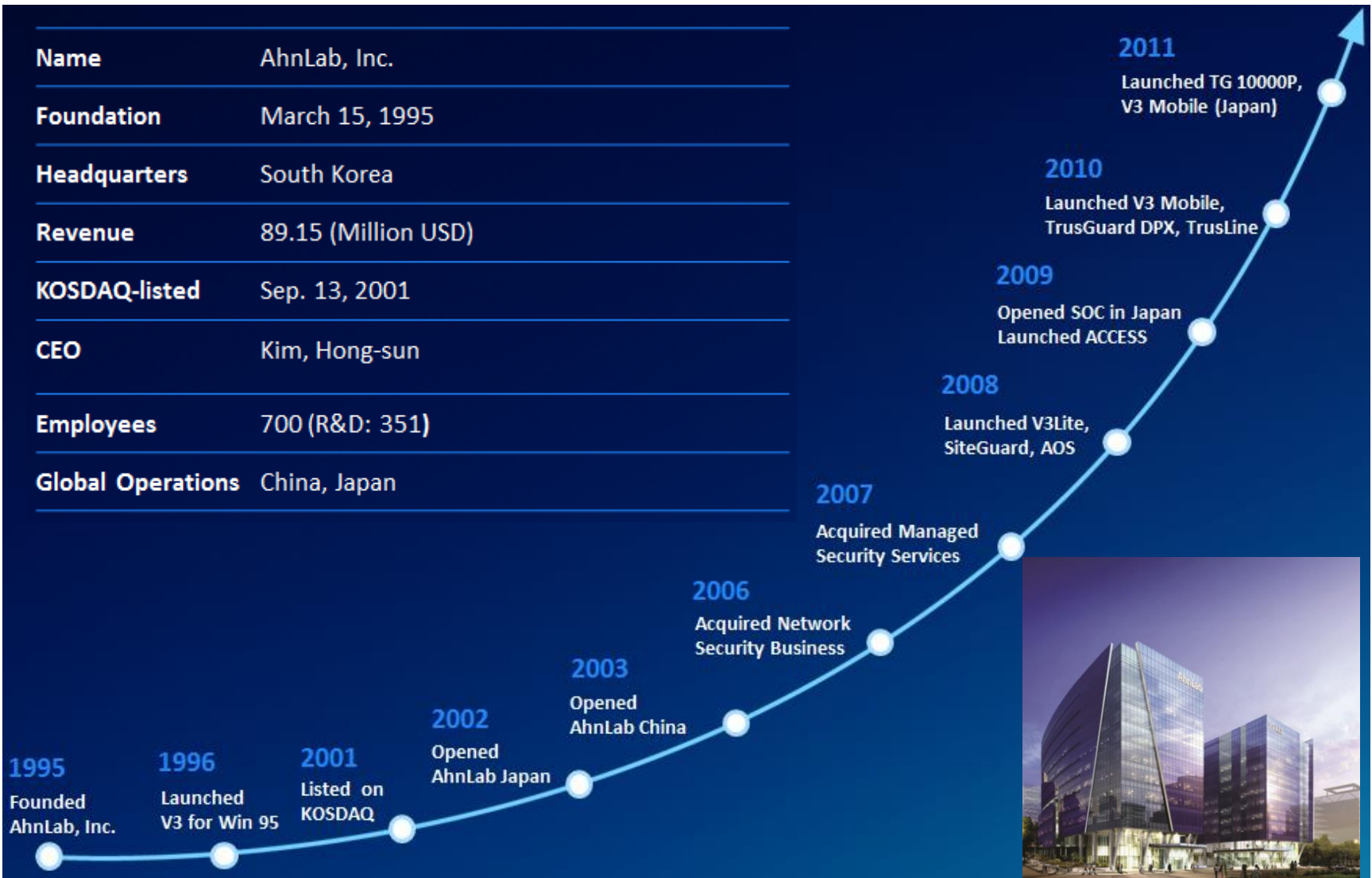
Hayoung Yang (hyyang@ahnlab.com)

Senior Anti-Virus Researcher

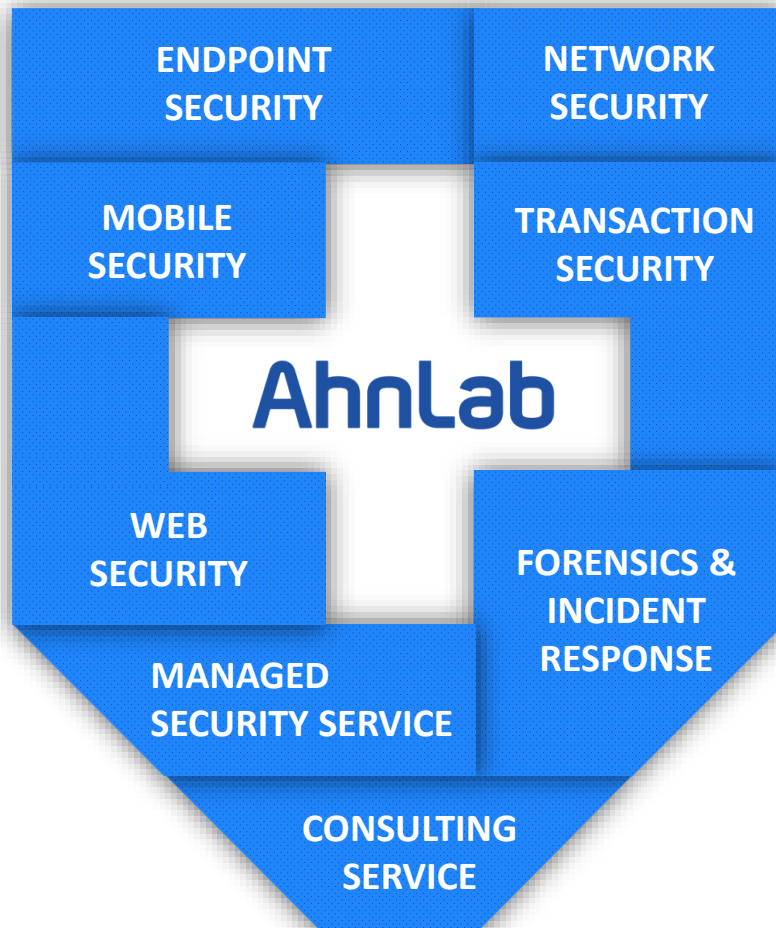
ASEC (AhnLab Security Emergency response Center)

# What is AhnLab ??

<b>Name</b>	AhnLab, Inc.
<b>Foundation</b>	March 15, 1995
<b>Headquarters</b>	South Korea
<b>Revenue</b>	89.15 (Million USD)
<b>KOSDAQ-listed</b>	Sep. 13, 2001
<b>CEO</b>	Kim, Hong-sun
<b>Employees</b>	700 (R&D: 351)
<b>Global Operations</b>	China, Japan



# Business Portfolio of AhnLab



## ◆ ENDPOINT SECURITY

V3 Internet Security  
V3 365 Clinic  
V3 Net for Windows Server  
V3 Net for Unix/Linux Server  
AhnLab TrusLine

## ◆ NETWORK SECURITY

AhnLab TrusGuard  
AhnLab TrusGuard DPX  
AhnLab TrusManager  
AhnLab TrusAnalyzer  
AhnLab TrusZone  
AhnLab TrusWatcher

## ◆ MOBILE SECURITY

AhnLab V3 Mobile  
AhnLab V3 Mobile Enterprise  
AhnLab Mobile Center  
AhnLab V3 Mobile + for Transaction

## ◆ TRANSACTION SECURITY

AhnLab Online Security  
AhnLab HackShield for Online Game

## ◆ MANAGED SECURITY SERVICE

AhnLab Policy Center  
AhnLab Policy Center Appliance  
AhnLab Policy Center Patch Management

---

# Contents

## 01 Financial Cybercrime

- 1) Financial Cybercrime Malware
- 2) Financial Cybercrime Malware is useless in Korea

## 02 Korean Online Banking Systems

- 1) Online Banking and Mobile Banking in Korea
- 2) Policy to install Security Software in Bank website in Korea
- 3) Online Banking process in Korea

---

# Contents

## 03 Financial Cybercrime in Korea

- 1) Financial Cybercrime Status
- 2) Banking Malware in 2007
- 3) Spread ways of Banking Malware in 2012
- 4) Banking Malware in June 2012
- 5) Banking Malware in September 2012

## 04 Summary

- 1) Financial Cybercrime Timeline in Korea
- 2) Banking Malware Features

---

# 01 Financial Cybercrime

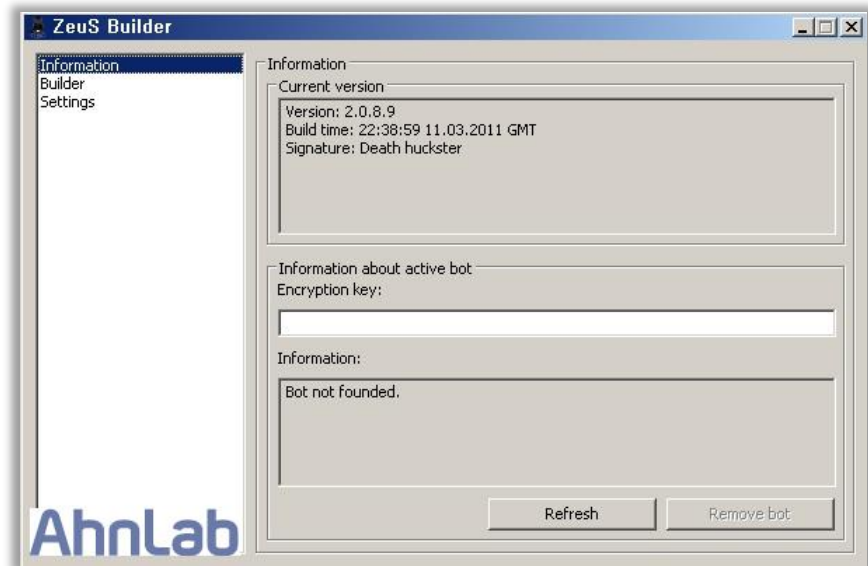
---

# 1) Financial Cybercrime Malware

- ❖ Financial Cybercrime increasing due to the increase in online financial service
- ❖ Zeus, Spyeye and Citadel infections high in Europe and U.S.A
- ❖ Financial Cybercrime Malware widely spread from PC to smartphone



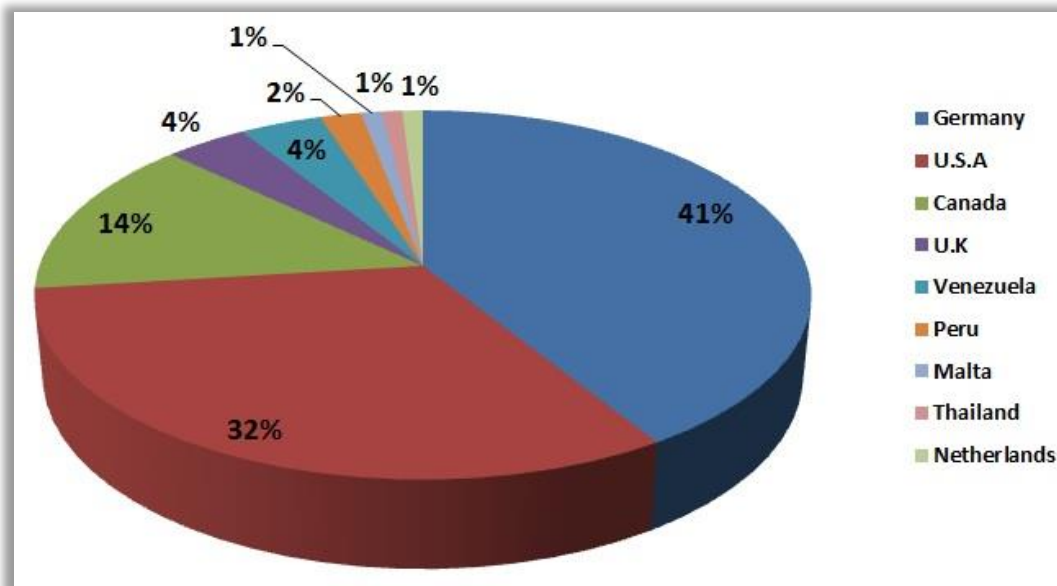
**Spy Eye** v1.2



## 2) Financial Cybercrime Malware is useless in Korea

- ❖ Most Financial Cybercrime Malware is useless in Korea
- ❖ Most Financial Cybercrime Malware's target is bank in Europe and U.S.A
- ❖ Europe, U.S.A and Korea have different online banking systems and process

```
1 https://www.commerzbanking.de ↵
2 https://my.hypovereinsbank.de ↵
3 https://banking.dkb.de ↵
4 https://banking.postbank.de ↵
5 http://www.amazon.de/ ↵
6 https://www.moneybookers.com ↵
7 https://www.paypal.com ↵
8 https://www.entropay.com/ ↵
9 http://www.neteller.com/ ↵
10 https://www.banesconline.com/ ↵
11 http://correoweb.cantv.net/ ↵
12 mail.yahoo.com ↵
13 mail.live.com ↵
14 https://bcpzonasegura.viabcp.com ↵
15 https://www.bankofamerica.com/ ↵
16 https://www.banesconline.com/ ↵
17 http://correoweb.cantv.net/ ↵
```



Websites of Spyeye's target and belong to countries (2012-04)



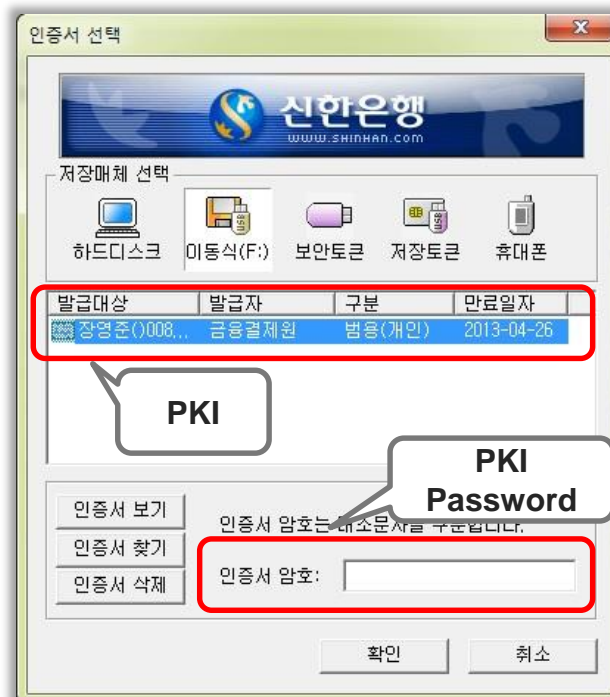
---

# 02 Korean Online Banking Systems

---

# 1) Online Banking and Mobile Banking in Korea

- ❖ Online Banking and Mobile Banking is the usual banking of Korean people
- ❖ Bank can support Mobile Banking in iPhone, Android and Windows Phone
- ❖ Banking user must have bank user ID, PKI and Security Card or OTP in 2 ways



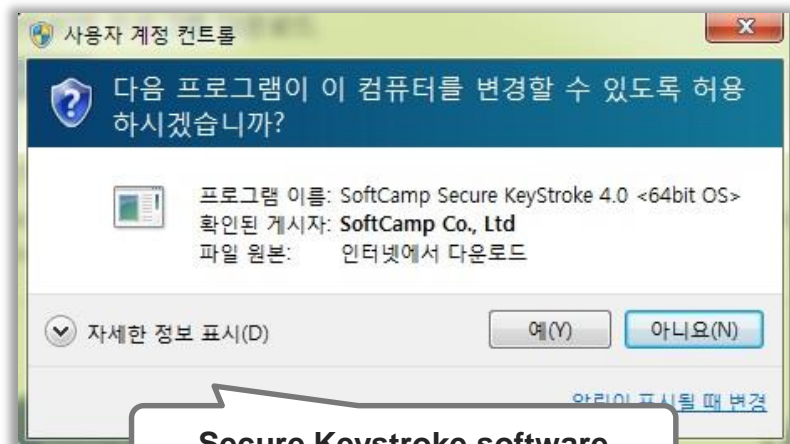
**Mobile Banking App, PKI Manager and Security Card**

## 2) Policy to install Security Software from Bank website in Korea

- ❖ When banking user connect bank website, automate security software installation
- ❖ Korean Government have a policy to automate security software installation in bank website
- ❖ Security software is Anti-Virus, Personal Firewall and Secure Keystroke
- ❖ Some bank can support another security service for their customers



**Anti-Virus and Personal Firewall  
security software**



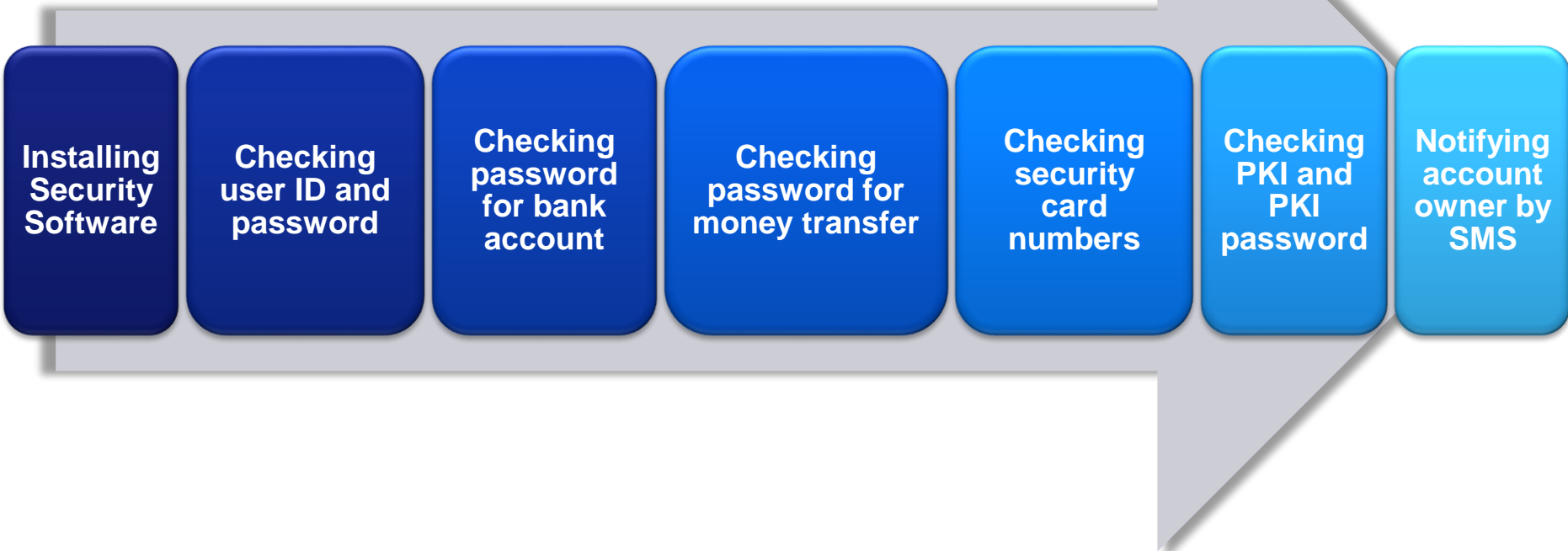
**Secure Keystroke software**

**Automate security software installation from Bank website**

### 3) Online Banking process in Korea

---

- ❖ Korean online banking process have 8 steps
- ❖ If banking user don't have any keyboard and mouse input in 10 mints, automate logout in bank website
- ❖ If banking user have 3 times password error, bank account automate lock



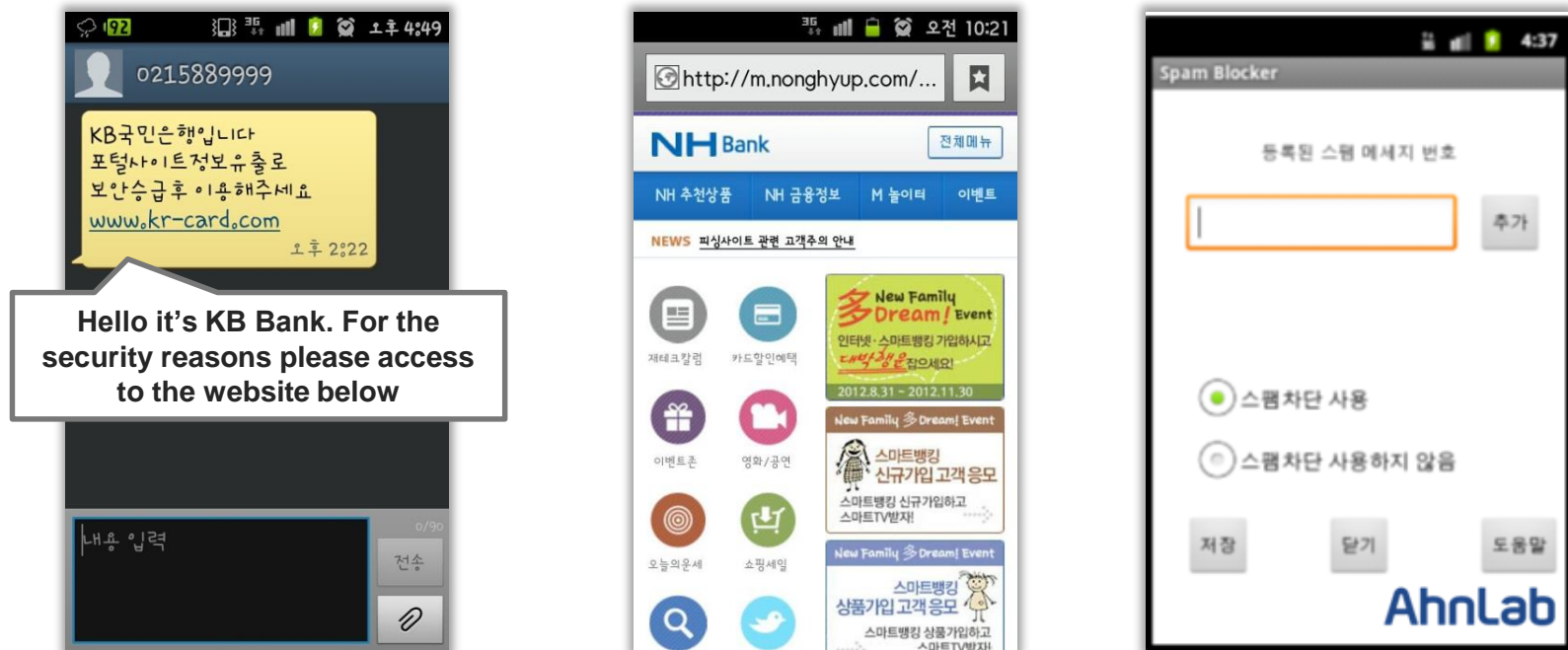
---

# 03 Financial Cybercrime in Korea

---

# 1) Financial Cybercrime Status

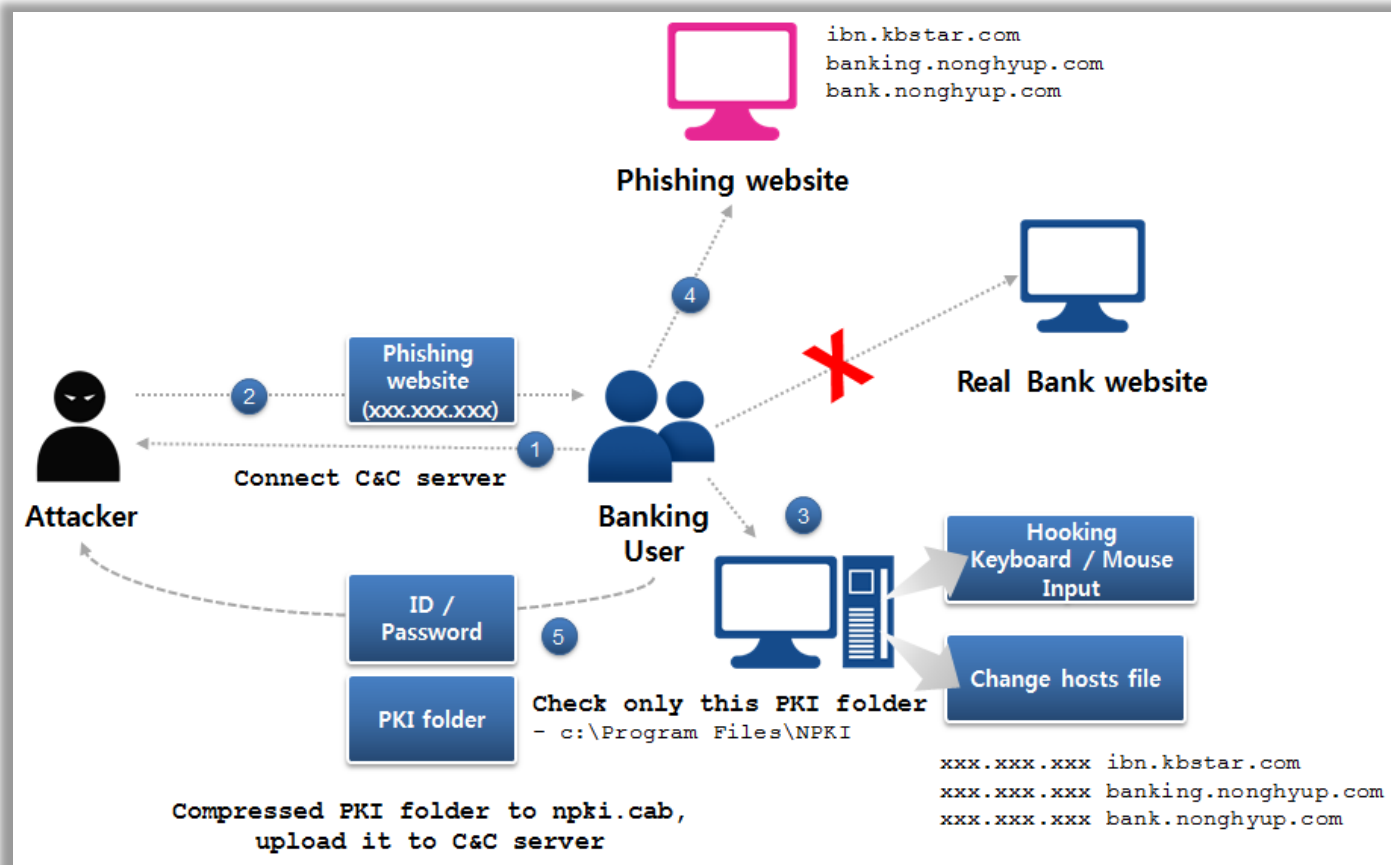
- ❖ Before 2012, Voice Phishing and Messenger Phishing are serious problem
- ❖ In 2011, the amount of damage of Voice Phishing had USD 1.12 million
- ❖ In 2012, PC, Mobile Phishing and Banking Malware are slowly increasing
- ❖ In Oct 2012, the first Android Malware related with Financial Cybercrime



**SMS Mobile Phishing, Mobile Phishing website and Android Malware**

## 2) Banking Malware in 2007

- ❖ In 2007, the first Banking Malware found in Korea
- ❖ It didn't leak PKI password and Security Card Numbers



**In 2007, Banking Malware leak banking information**

### 3) Spread ways of Banking Malware in 2012

---

- ❖ In 2012, the first and Second variant of Banking Malware found in Korea
- ❖ It use various ways to infect PC more than in 2007

#### 1) Application Vulnerability

JAVA - CVE-2011-3544, CVE-2012-0507, CVE-2012-5076

Adobe Flash Player - CVE-2011-2140, CVE-2012-0754

Windows Media Player - MS12-004

Internet Explorer - MS10-018

#### 2) Fake video-sharing website

Disguising video player setup file in fake video-sharing website

#### 3) Change P2P program setup file to Banking Malware

Change uTorrent setup file to Banking Malware

Change Korean P2P program setup file to Banking Malware

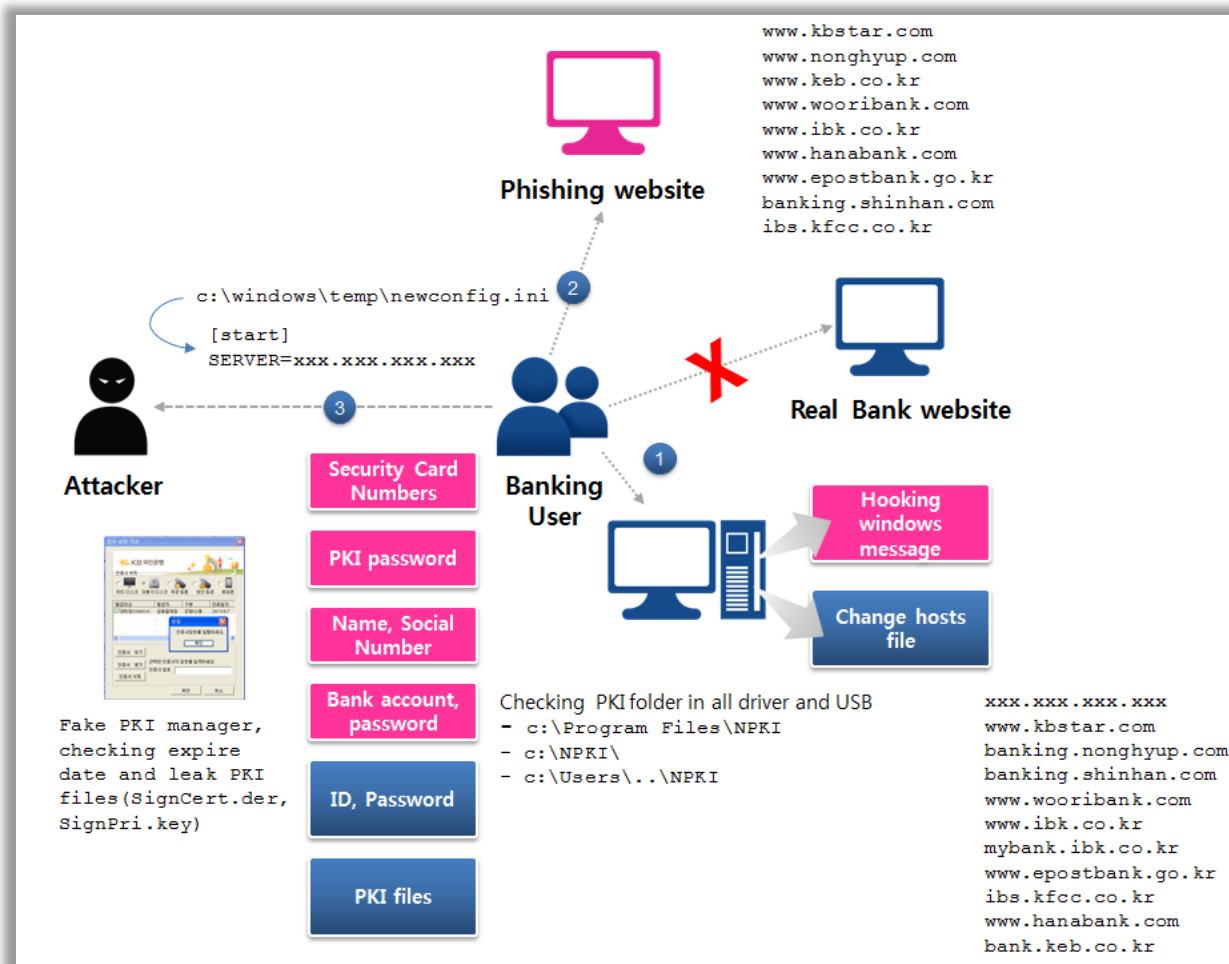
#### 4) Google Code webpage

Banking Malware upload in Google code webpage, redirecting from other website



## 4) Banking Malware In June 2012 (1)

- ❖ Banking Malware leak banking information for transfer money



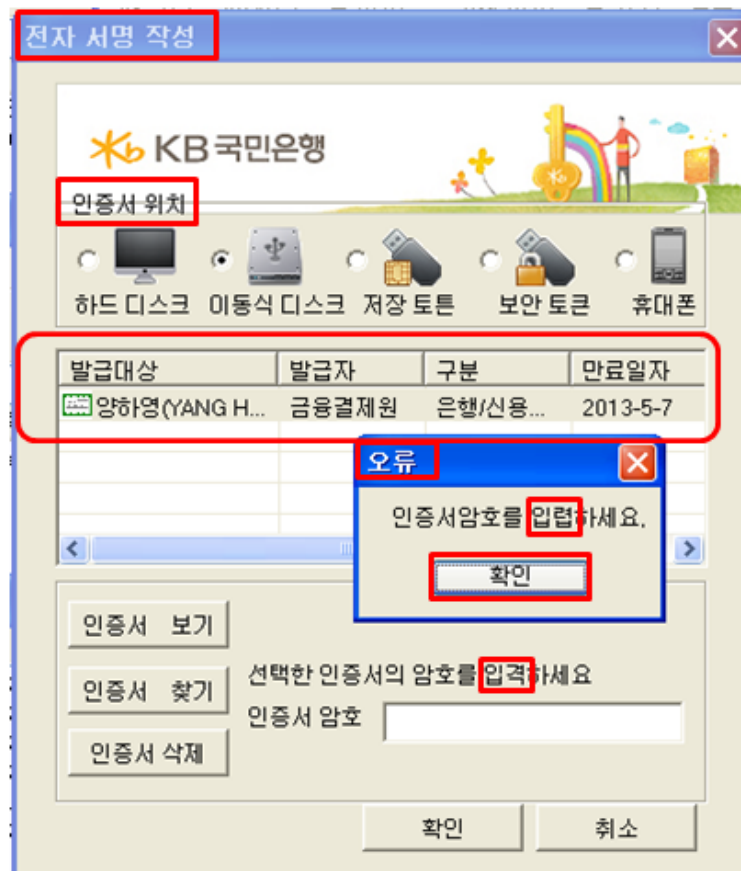
**In June 2012, Banking Malware leak banking information**

## 4) Banking Malware In June 2012 (2)

- ❖ Banking Malware make Fake PKI manager to leak PKI files and PKI password
- ❖ Banking Malware check PKI folder in every driver, including USB



Real PKI Manager



Fake PKI Manager

## 4) Banking Malware In June 2012 (3)

- ❖ When banking user connect bank website, redirect phishing website
- ❖ Phishing website lead banking user input whole banking information

The detailed view shows the following fields and labels:

- Bank account**: 주면등록번호 (343453 - \*\*\*\*\*)
- Bank account password**: 출금계좌번호 (1)
- Password for money transfer**: 출금계좌비밀번호
- Security Card Serial Number**: 이체비밀번호
- Security Card Numbers**: 보안카드 일련번호 (No: )

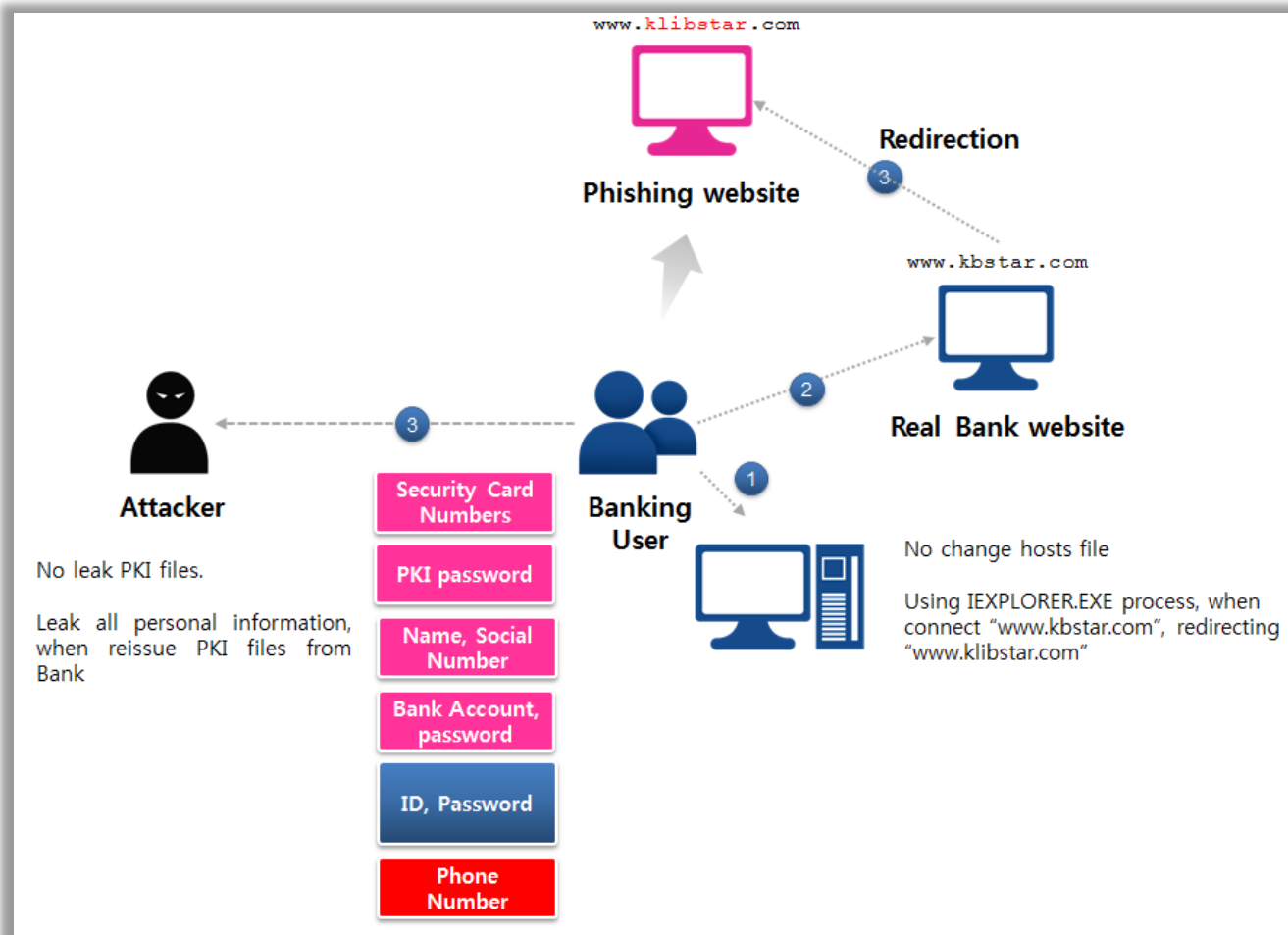
Below the input fields is a grid for the security card numbers:

1		8		15		22		29	
2		9		16		23		30	
3		10		17		24		31	
4		11		18		25		32	
5		12		19		26		33	
6		13		20		27		34	
7		14		21		28		35	

Leak all banking information in Phishing Bank website

## 5) Banking Malware In September 2012 (1)

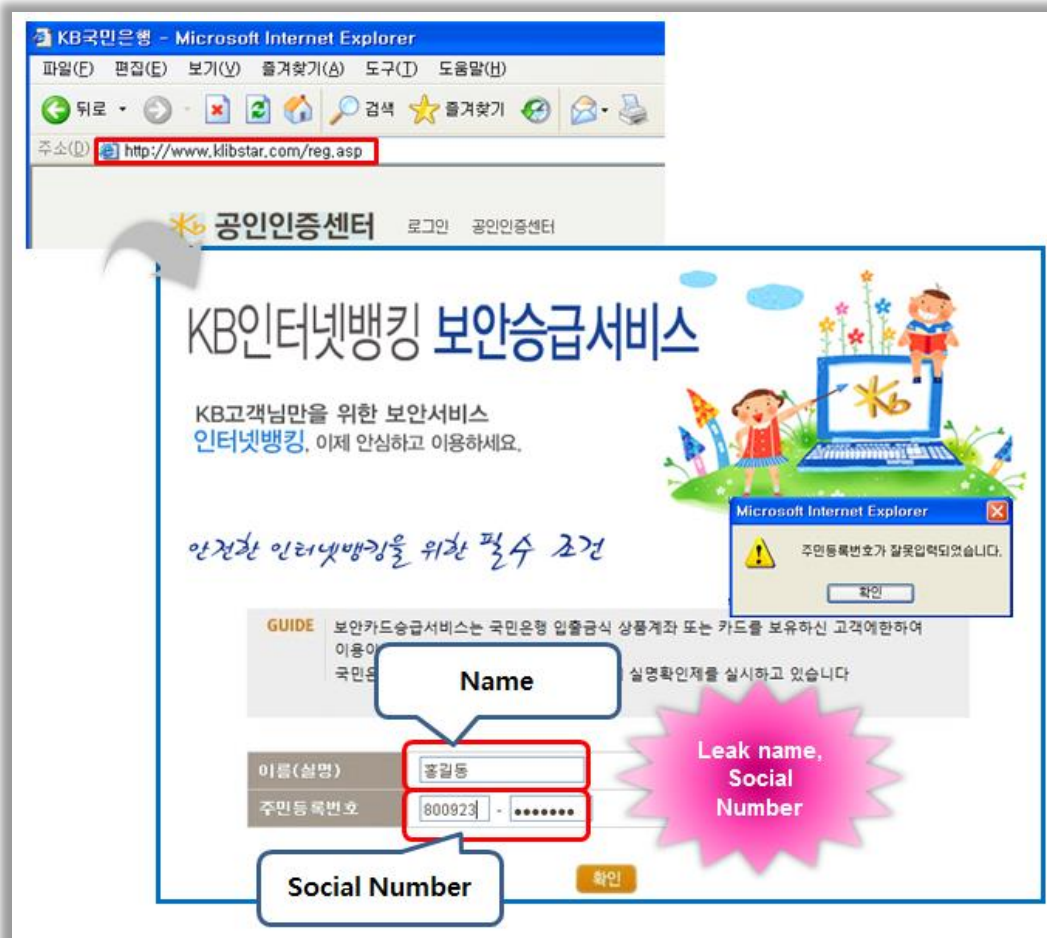
- ❖ Banking Malware leak personal information to reissue PKI files



In September 2012, Banking Malware leak banking information

## 5) Banking Malware In September 2012 (2)

- ❖ First, Phishing Bank website leak name and social number



Leak name and social number in phishing bank website

## 5) Banking Malware In September 2012 (3)

- ❖ Second, Phishing Bank website leak all banking information and phone number

KB국민은행 - Microsoft Internet Explorer

주소(①) <http://www.klibstar.com/regtwo.asp>

로그인 | 동센터

800428-\*\*\*\*\*

Bank user ID

Bank user password

Bank account password

Bank account

Phone number

Security Card Serial Number

Security Card Numbers

**Leak all banking information and phone number**

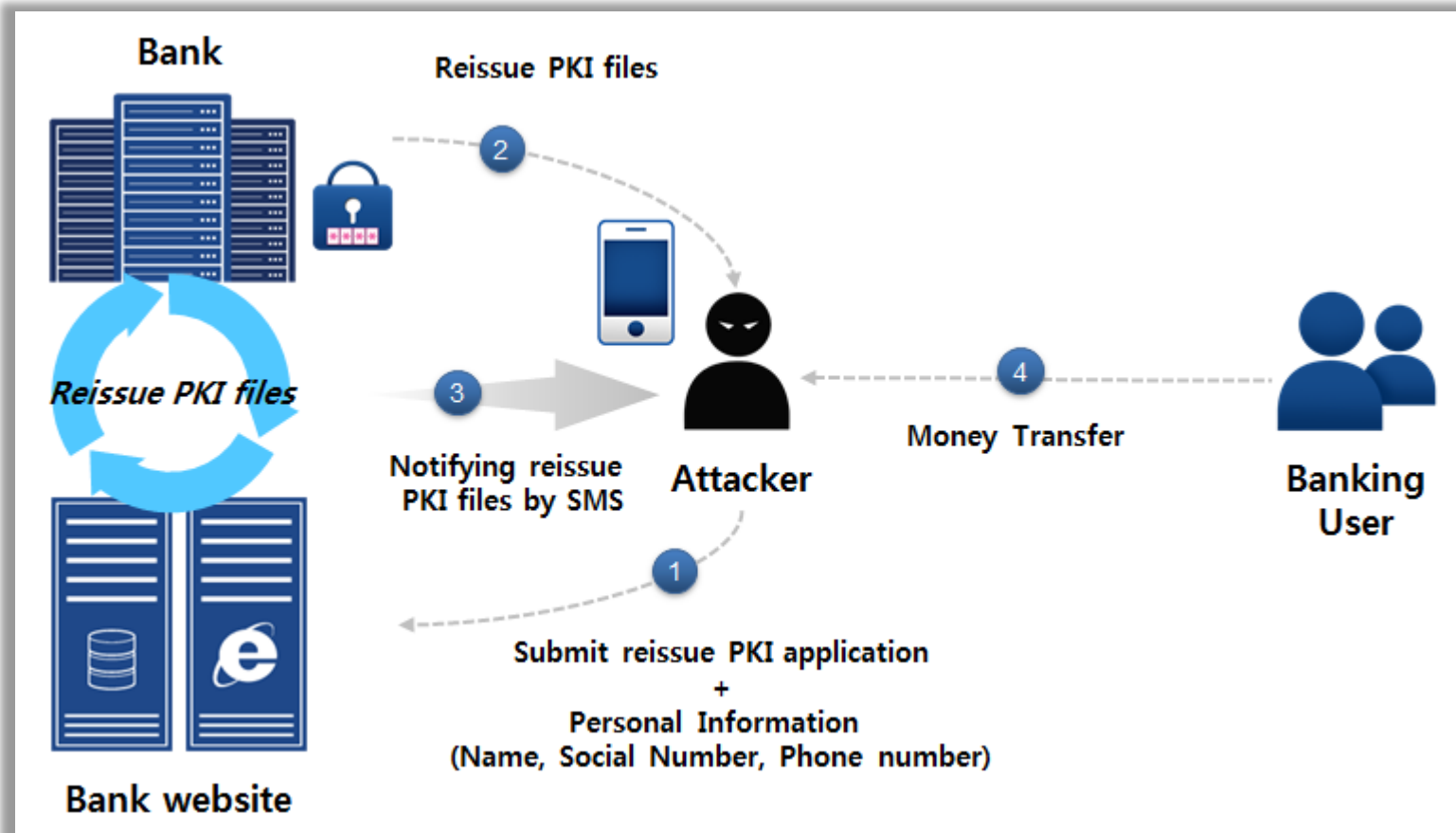
은행에서 제공하며 4자리의 숫자로 구성된 총35개의 도

1-35번까지의 번호를 입력하시고 확인을 누르시면 보안등급이 완료됩니다

**Leak all banking information and phone number in Phishing Bank website**

## 5) Banking Malware In September 2012 (4)

- ❖ It leaked personal information and banking information, to reissue PKI files



**Attacker reissue PKI files, money transfer**

---

# 04 Summary

---



# 1) Financial Cybercrime Timeline In Korea

---

- ❖ In 2007, Banking Malware was a kind of proof of concept in Korea
- ❖ Before 2012, Voice Phishing was serious problem in Korea
- ❖ In 2012, PC, Mobile Phishing and Banking Malware are slowly increasing



**In 2007,  
Banking  
Malware**

**Before 2012,  
Voice  
Phishing is  
serious**

**In April 2012,  
Phishing  
website increase**

**In June 2012,  
Banking Malware  
increase**

**In October 2012,  
Financial Android  
Malware**

## 2) Banking Malware features

- ❖ After the first banking malware found in 2007, it understand Korean banking systems well
- ❖ In June 2012, Banking Malware leak banking information for transfer money
- ❖ In Sept 2012, Banking Malware leak banking and personal information, it could make another kind of Cybercrimes, in the near future
- ❖ Korean Banking Malware relate with Phishing website to leak banking information

Date	Banking Malware type	Change hosts file	Leak Security Card numbers	Leak PKI files	Leak PKI password	Check PKI folder
2007	EXE(1), DLL(1)	O	X	Whole PKI folder and files	X	Static location
2012.06	EXE(2), INI(1)	O	O	Some PKI files	O	Every drivers and USB
2012.09	EXE(1)	X	O	X	O	X

### Korean Banking Malware features

---

**thank you.**

---