# *Light & Shadow about Net-Banking $ecurity @ Japan*

*@2013 HITCON*
*愛奴 & 愛花 Punpun*
*maru*


## *Profile*

- Started lecturing and writing as a freelancer since 2000
- AVTOKYO Speaker (2010, 2011, 2012)
- Wrote "Introduction of Information Security " for the textbook of universities
- Regular writer for "Hacker Japan Magazine "
- Serious day job around Financial Industry

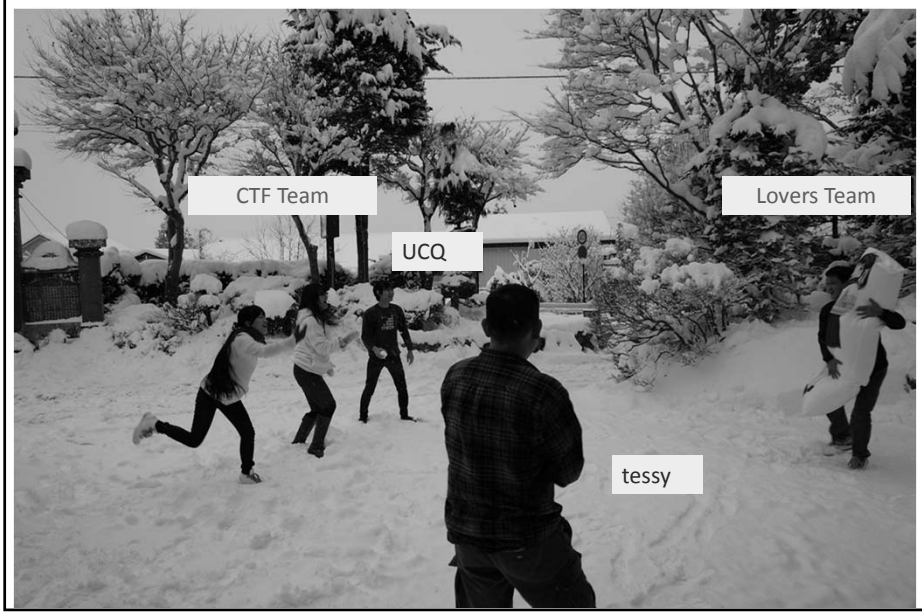
AV TOKYO www.avtokyo.org


## *Profile （愛奴＆愛花 Aido & Manaka）*

- I successfully took her out from the virtual game world.
- I am presenting about how beautiful life with Girlfriend
- Please see Every day of love


## *京都 伏見稲荷大社 Fushimi Inari Taisha*

## *Snowball fight against Japan CTF team*




## *Famous Castle in Japan*

Kumamoto Castle

Himeji Castle
World Heritage

# *Agenda*

- Background
- History
- Data and Statics
- "Light and Shadow" of net-banking security practices
  - *Screen Keyboard*
  - *Eliminating Popup Windows*
  - *S/MIME mail*
  - *Password Reminder*
  - *One Time Password (Bingo Card)*
  - *One Time Password (send by e-mail)*
  - *Secure Browser*
  - *Password Number(PIN)*
  - *Telephone Banking*
- Cost and work amount
- Business Strategy
- Power balance against Systems Integrators
- The result of a Power Balance
- Studies and Solutions

# *Background*

- In order to prevent drawing money by fraud, phishing or spyware, many banks performed original various measures in Japan.
- It's unfortunate but they failed to protect their customers from a crime.
- I will explain the light and the shadow of those measures.

# *History*

- 1997/01 The first net-banking services was launched by Sumitomo Bank.
- 2000/01 The first bank provides all services via the internet, was established.
- 2005 Phishing fraud mail posing Mega-Bank (Bank of Tokyo-Mitsubishi UFJ) was found.
- 2006 The first damege by phishing fraud was found at E-bank (Rakuten Bank, today).
- 2007 Phishing fraud site have users enter all numbers on Bingo Card was found at Shinsei Bank (First Case).
- 2011 Simultaneous multiple phishing fraud (use spyware) posing regional banks occurred in later half of the year.
- 2012 Phishing fraud site have users enter all numbers on Bing Card was found at famous 3 Mega-Banks.
- 2013 As of Apr. end, defrauded amount exceeds 100 million JPY (30 million NTD) .



# *Data and Statics*

| | |
|---|---|
| The number of Banks witch give Internet Banking | 411 |
| The number of accounts | 60,258,506 |

at 31/03/2012 Researched by FISC

- Half of peoples have accounts of net-Banking in Japan!!

# *Data and Statics*

| | | 2010 | 2011 | 2012 (Apr-Dec) |
|---|---|---|---|---|
| Internet Banking | The number of Damage | 78 | 162 | 91 |
| | Amount of damage(JPY) | 88million | 402million | 68million |
| Use Fake Cash Card | The number of Damage | 272 | 477 | 670 |
| | Amount of damage(JPY) | 248million | 320million | 583million |
| Cash Card Theft | The number of Damage | 6,589 | 5,289 | 2,853 |
| | Amount of damage(JPY) | 3,888 million | 2,856 million | 1,227 million |

http://www.fsa.go.jp/news/24/ginkou/20130524-1.html

- Comparing with the Cash card theft, amount of damage is **about 1/20**.



# *Light & Shadow*

## *of net-Banking $ecurity practices*

# *Screen Keyboard*

*Light*

- Most popular in Japan
- “Trump” against software key loggers


*Shadow*

- Have ever been breached many times
- Weak against RAT(Remote Access Trojan horses)
- Inconvenient to use
- Security tends to come with inconvenience, but inconvenience do not mean secured



# *example : Ultimate Screen Keyboard*

- If mouse cursor was out of window, Key pattern appeared
- If mouse cursor was inside window, Key pattern disappeared
- You must memorize random Key pattern!!



*Mitsui sumitomo Banking*

## *Eliminating popup windows*

### *Light*

- Prevents XSS, transfer to fraud site
- Countermeasure for insert Malicious Frame window , Man in the Browser Attack

### *Shadow*

- One of major bank in Japan has ″preference″ to adopt popup windows; they even provides caution for malfunctioning popup windows by popup window
- ″standards ″ does not make sense, unless everybody adopts



## *Bad case about popup windows*


caution for malfunctioning popup windows

Oh!! It hided URL Bar


And so, popup window appeared!!

## *S/MIME mail*

*Light*

- Assures the validity and non-compromised
- Easy to adopt; just adding onto mail servers
- Inexpensive, tens of millions JPY

*Shadow*

- Most consumers do not know what is S/MIME
- They even misunderstand the signature to be malware!
- "Cheap", tens of millions adoption cost brings nearly ZERO benefit.
- Does not work with Gmail
- As the result, it is only "way to excuse" for banks



## *Password Reminder*

*Light*

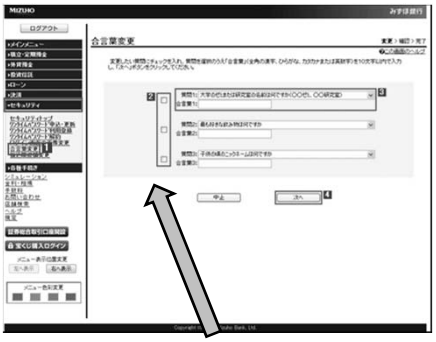
Identify users by "secret" question; asking what only oneself knows.

i.e. mother's maiden name, name of pet

*Shadow*

- By checking Facebook/Blog, easy to know one's personal information including mother's maiden name and name of pet
- A junior high school student cracked by checking information on SNS.

*A Bad example*



The question pattern are fixed.

Easy to predict.

*A comparatively good example*

The question are made by customer.


Example questions are not so good.



*One Time Password (Bingo Card)*

*Light*

- Specify different two cells in Bingo card at random
- Eavesdropping password does not make sense

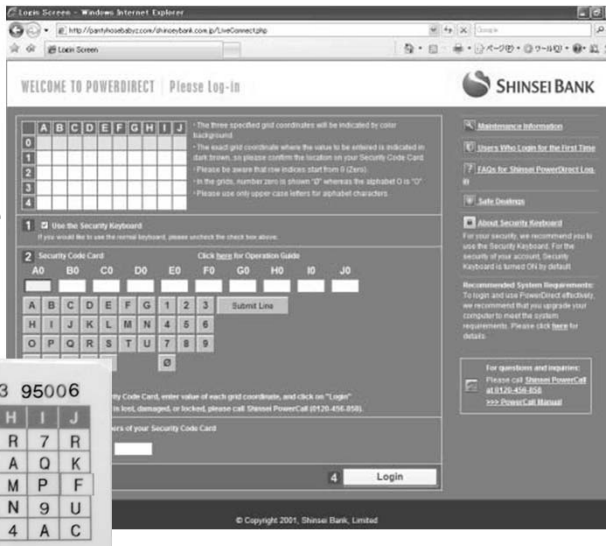
*Shadow*

- Some banks do not limit reloading times; keep reloading until the eavesdropped pattern appears
- If the Bing Card does not have many enough numbers, the card could be reproduced by eavesdropping for several times.
- Successfully phished by entering all the numbers in Bingo Card.
- If the Bing Card adopts 8–10 random numbers (not number matrix), even easier to phish.

*Phishing Site : entering all the numbers*

Shinsei Bank

**Phishing Site**




**Bingo Card**




*Phishing Site : entering all the numbers*

The Bank of Tokyo-Mitsubisi UFJ

**Phishing Site**


**Bingo Card**

## *One Time Password (send by e-mail)*

### *Light*

- Virtual 2 factor authentication by e-mail address in addition of ID/password.
- Expires in certain minutes against repeat use (Replay Attack)
- Rather lower cost to adopt, as it does not require tokens to be delivered.

### *Shadow*

- Eavesdropping by spyware and use before expiration works; it allows repeat use.
- Several cases are already there by spyware. (Bank of Tokyo-Mitsubishi UFJ)



## *Secure Browser*

### *Light*

- Eavesdropping by spyware and use before expiration works; it allows repeat use.
- Several cases are already there

**If All Banks keep pace and progress, it becomes a trump card.**
**(Restrict custom-designed )**

### *Shadow*

- Difficult to prove validity of itself.
- Hard to install for non-technical consumers
- Can be faked easily
- Fake browser is more user friendly and validity appearing; assurance phrase can also be faked on the fake, like "100% secure"!

## *Password Number(PIN 4digits)*

*Light*

- Called attention of not to use easy-to-guess numbers like date of birth or call number
- Can be changed on ATM, do not have to talk to representatives.

*Shadow*

- Cannot force change
- Some of customers have difficulty to use ATM
- Some other of customers(senior, patients) even cannot go up to ATM booth.
- Date of birth is "popular" information on Facebook



## *Telephone Banking*

*Light*

Avoid fraud withdraw by limiting functions like follows

1. Checking balance only
2. Transfer only to registered accounts
3. Operators are always in the process of withdraw/transfer

Frankly speaking, this is one of critical point!!

*Shadow*

- Gain authentication information, not withdraw money
- No.1 and No.2 above are useful to guess PIN; there are cases
- Some banks do not limit PIN enter times
- Even if there are limit, it still useful to check if the date of birth is PIN

## *Cost and work amount*

- Bingo Card must be sent to all individual customers.
- Many inactive accounts
- Some customers do not report address change (amount 10%)
- Bank of Mitsubishi Tokyo UFJ have 13 million customers
- How much the cost would be, delivering IC cards to 13 million customers?
- Still, how much the cost would be delivering Bing Cards?
- As the result, adopting OTP sent by e-mail; it is only solution to make the cost "realistic level"
- Only 1 of 20 damage, of emergency scam
- "reasonable" level from the standpoint of risk and cost



## *Business Strategy 1*

- Due to the quota number, net banking services were applied anyone who open accounts.
- Most of the people, do not use net banking services.
- The quota was set based on the myth of "eternal growth".

## *Business Strategy 2*

- Japan banks prefer to do what others are doing. ″Must do, because they are doing!!″
- Intends differentiation, but do what others do.
- Care do same as or more than others, than what to prioritize for benefit
- Ironically, customer expect bank to do so.
- Customer said “Don ‘t you have the service, while *** Bank have?″
- As the result of the above, ″adopt Bingo Card, because *** Bank did″.



## *Power balance against Systems Integrators*

- Banking System is one of the best business for Systems Integrators.
- That means, banks become the customer of ″self-consequence″
- Systems Integrators become ″ ingratiating″

## *The result of a Power Balance*

- The structure above means banks do not have to know about information systems/information security, and they actually do not know. Consequently, Systems Integrators provides "easy-to-understand security solutions" to bank.
- Visible; for example, Screen Keyboard
- Bank do not think by themselves.
- Systems integrators provides solutions of delighting banks
- It means no one analyze risk.



## *Studies and Solutions*

- Once services are deployed based on convenience, Security is hard to implement.
- Design should be scandalized and applied without any exceptions.
- Should not allow differentiation, as it confuse customers and complicate specification enough to have vulnerabilities.
- Internet banking services should not be applied for those who do not use; ATM is good enough.
  (Simple services, such as a check of the balance )
- Wire transfer can be switched to Credit Card Payment, as it makes maximum damage within card credit limit. Everybody checks credit card bills more frequently than rarely used bank account statement.
- To suppress the part of way out, just lower wire transfer limit.

# *Thank you for listening*

In Taiwan, internet banking services are provided only those who really needs the services, as it require IC cards and card readers.

This is very good practice.

As shown in my presentation, with chasing the number of service users, providing such services to those who do not need, become risk.
In addition, banks must consider how to deal with their security risk without completely relying on to Systems Integrators.
I hope Taiwanese to establish good security practice based on the Japanese case studies mentioned in my presentation.

e-mail : aido@hkg.odn.ne.jp
Facebook : Hiroshi.Aido 相戸 浩志
Twitter ID : @aido_hpf