

Identity Theft: Phishing Email Scams Fake Websites

ISACA Hong Kong Chapter
Professional Development Seminar
4 November 2004

EMA Project Team
K.C. Lau, Calvin Tam
Jeff Ho, W.W. Fung



Copyright © 2004 EMA Project. All rights reserved. May not be reproduced or distributed without written permission of the EMA Project team.

Disclaimer

Any mention of commercial products within this presentation is for information only; it does not imply recommendation or endorsement by the EMA project team of any company or solutions proposed and does not imply a preference over any one solution or a combination of solutions proposed.

Any products and company names are the trademarks or registered trademarks of their respective owners. It is not intended that the use of a term in this presentation affects the validity of any trademarks, registered trademarks or copyrights.

The opinions expressed in this presentation do not necessarily represent the views or opinions of any company. Your comments are encouraged and can be sent to anti.phishing@gmail.com

2

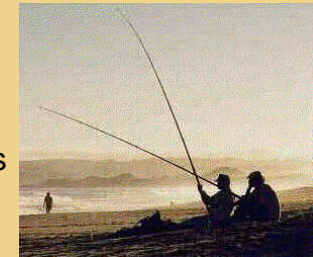
EMA Project

- Design principle: Enforced Mutual Authentication
- Project established October 2003
 - Rise in phishing attempts targeting local Financial Institutions
- Objectives
 - Design and develop practical solutions to combat identity theft
- Approach
 - Inter-disciplinary approach with input from Financial Institutions
 - HKMA guidelines on e-Banking Security

3

Agenda

- Introduction
- Phishing
- Anti-Phishing Solutions
- Summary



4

Introduction



- Physical World
 - Theft: Shop theft
 - Fraud: Employment fraud
 - Deception: Superstition deception
- Cyber World
 - Theft: Identity theft
 - Fraud: e-banking fraud
 - Deception: Deception by scam e-mail

Just a New Way to Commit Old Crimes

Phishing



What is Phishing?

- Aim
 - Identity theft
- How?
 - Technical deceit
 - Social engineering practices
- Consequence
 - Loss and misuse of personal confidential information

We recently noticed one or more attempts to log in to your Citibank account from a foreign IP address and we have reasons to believe that there was attempts to compromise it with brute forcing your PIN number. No successful login was detected and you have full protection by now. If you recently accessed your account while travelling, the unusual login attempts may have been initiated by you.

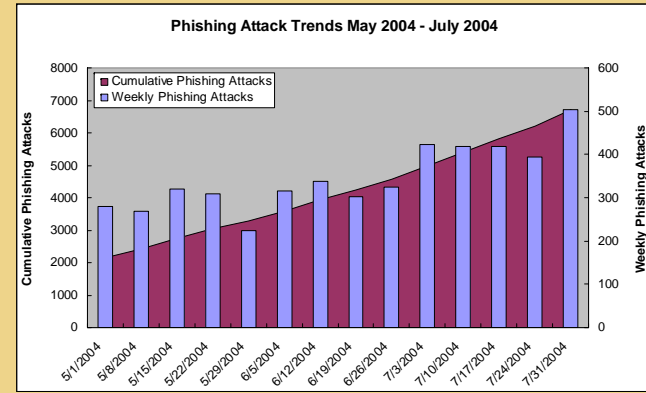
Enter Your Registration Information

User ID

Password

- User IDs and Passwords are case-sensitive
- Do not use your browser's "Back" button to return to this page. Doing so may cause your transaction to be voided.

Phishing Trends



Source: Anti-Phishing Working Group (July '04)

Phishing Trends

- 95% of phishing exploits reported originate from forged addresses
- 5 new phishing exploits are reported every month
- 5% of all recipients actually respond to phishing exploits

9

Source: Anti-Phishing Working Group (July '04)

The Phishing Process



Phishing Preparation



11

Propagation



- Online
 - Scam emails
 - Newsgroups
- Offline
 - Phone calls
 - Scam letters

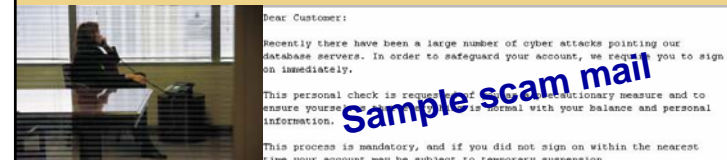
Scam Emails and Newsgroups

- Propagation
 - Scam email, bogus news posting, lucky draw
- Preventive control (User):
 - Education and awareness training
- Detective control (User):
 - Scam text scanning
 - Spam trap, signatures, patterns

13

Scam Letters and Phone calls

- Determined fraudsters may resort to phone calls, send letters or even physical visits
- Preventive control (User):
 - Education and awareness training to combat social engineering



Information Misuse

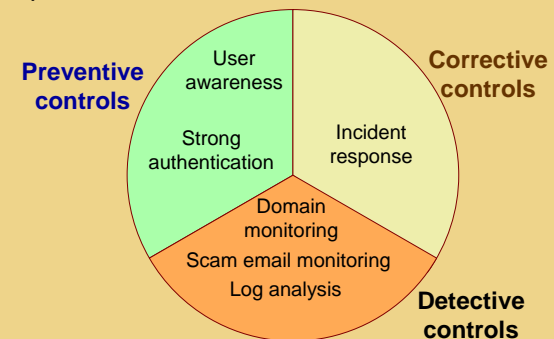
- Open bank accounts
- Apply for loans
- Apply for credit cards
- Direct funds transfer uncommon -- traceable



15

Defence Strategies

- Defence strategies must be implemented at the corporate and user level



16

Risks of Not Addressing Phishing

- To the Banks
 - Loss due to fraud
 - Loss of reputation
 - Decreased profitability
- To the User
 - Monetary loss
 - Higher borrowing costs



17

Anti-Phishing Solutions



Sender Policy Framework (SPF)



How SPF Works

- Advantages
 - Prevents sender forgery
 - Reduces inbound spam
- Disadvantages
 - No anonymity

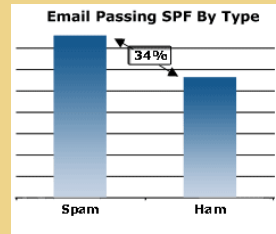


20

source: spf.pobox.com

SPF Considerations

- Will SPF stop spam?
 - Not yet
 - It will stop address forgery
 - It cannot stop the legitimate spammer address
- Spammers already bypassing SPF
 - 34 percent more spam is passing SPF checks than legitimate e-mail



Source: CipherTrust Spam Statistics

21

SPF Developments

- Microsoft – Digital stamp
 - Objection from Open-source advocates
 - Patent and monopoly issues
- America Online (AOL) Sender ID
 - AOL withdraws support for Sender ID (mid Sep 2004)
- Internet Engineering Task Force (IETF)
 - IETF rejects Sender ID (mid Sep 2004)
- Microsoft resubmits modified SPF scheme (late Oct 2004)

22

Public Key Infrastructure



PKI Features

- Entity authentication
- Data confidentiality
- Data integrity
- Non-repudiation



24

PKI Considerations

- Implementation costs of public key infrastructure (PKI)
 - Who do we trust (Bank or Local CA)?
 - CA cross certification issues
 - CRL maintenance
- Difficult to implement on user side
 - Card reader security
 - User workstation security
 - Secure hardware mobility

25

Digital Cert Considerations

- How do you protect your certs?
 - More passwords to lose and forget
- How secure is the user computer?
 - Professional advice: Anti-virus, personal firewall, frequent system updates and patching, system hardening
 - Too technical for end-users?
- End-user usability?

26

HKMA Circular on e-Banking Security – 23 June 2004

Two-factor authentication should be implemented for high-risk transactions by June 2005



3rd Party Account Registration

- Controlling third-party transfers is not enough
 - Other unauthorised transactions
 - e.g. Selling of entire portfolio
 - Privacy and confidentiality of customer information
 - e.g. Residential address, account balance

28

Per Transaction Control

- Eliminates unauthorised transactions
- Considerations
 - Does not prevent loss of personal and confidential customer information

29

e-banking Logon Control

- Main two-factor authentication control point
- No unauthorised access to e-banking services
 - No disclosure of personal and confidential customer information
 - No unauthorised transactions

30

Control Point Comparison

Control point	Third-party account registration	Per Transaction Control	e-banking Logon Control
Considerations			
Disclosure of customer confidential information	Cannot prevent	Cannot prevent	Prevented
Unauthorised transactions	Cannot prevent (Only prevents transfers to unregistered 3 rd -party accounts)	Prevented	Prevented

31

HKMA Suggested Solutions

- Digital Certificates
 - Smart HKID
- One-Time Password
 - RSA SecurID
 - Mobile Short Messaging Service (SMS)



32

Digital Certificates (Smart HKID)

- Hong Kong Post Certification Authority
- Gradual replacement of old plastic HKID
 - Expected: All cards replaced by **2007**
- Free personal digital certificates for the first year
- Certificate renewal costs

33

Usage of Digital Certificates in e-Banking Services

- The Bank of East Asia
 - Corporate Cyberbanking Service
- CITIC Ka Wah Bank
 - Banking Online Service
- Dah Sing Bank
 - Dah Sing e-banking Service
- DBS Hong Kong
 - ec-business
- Belgian Bank
 - E-Banking
- Shanghai Commercial Bank Ltd
 - Corporate Internet Banking Service

Digital Certificates Anyone?

34

One-Time Password Token



35

One-Time Password Solutions

- One-Time Passwords (OTP) protect against external passive attacks against the authentication subsystem.
- An OTP system guarantees a new password on every connection.
- Commercially available solutions:
 - SecurID (RSA)
 - CryptoCard (CryptoCard)
 - Defender (Axent)
 - ActivCard (ActivCard)
 - SafeWord (Secure Computing Corporation)

36

RSA SecurID Token

- RSA SecurID two-factor authentication
- Advantages
 - Dynamic passwords
- Disadvantages
 - Infrastructure investment
 - Multiple tokens needed for different systems



37

Mobile One-Time Password Short Messaging Service



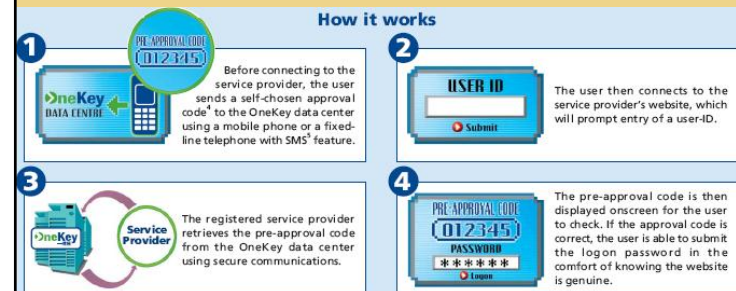
Mobile OTP SMS Solution

- One-time-password distribution via SMS.
- Usage of SMS in e-Banking Services:
 - HSBC in Singapore
 - NAB in Australia
- Advantages
 - Uses existing infrastructure
- Disadvantages
 - Telco / SMS provider security
 - Availability
 - Compatibility
 - Reliability
 - What about 3G? SMS will no longer be 'Out-of-band'
 - SMS infrastructure is out of the bank's control



39

OneKey Solution



40

OneKey Solution Considerations

- User inconvenience
 - Similar problems to SMS
 - User sends pre-approval code to OneKey data centre
 - Out going SMS charges
- Availability
 - Congested telephone networks
 - Typhoon signal 8, Black rain storm warning, Christmas eve, New Year's eve
- Infrastructure is out of the bank's control
 - Security issues
 - Downtime

41

From Another Perspective

"Ask not what your user can answer to you, ask what you can answer to your user."

Enforced
Mutual Authentication



42

Solution Design Philosophy

- Easy to use
 - User convenience, minimum learning curve
- Short development and implementation time
 - Easy integration with existing applications and infrastructure
- Low costs
 - Administration, operations, logistics, infrastructure maintenance
- Good availability
 - Useable everywhere
- Strong security
 - Enforced mutual authentication
 - Prevents unauthorised access even when username, password and second factor passcode are captured by the fraudsters

43

EMA Solution

This page has been intentionally left blank

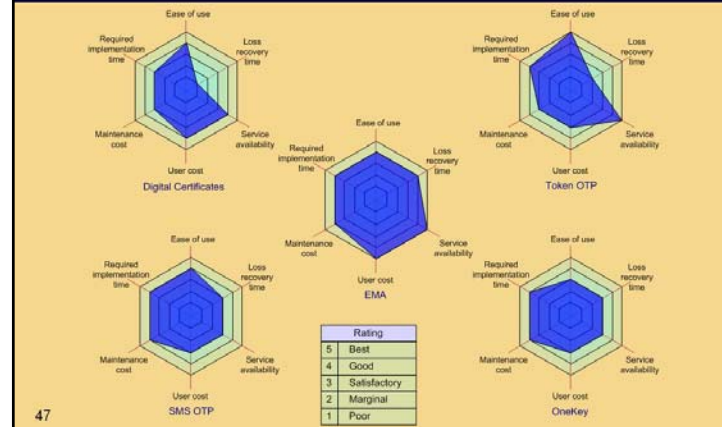
44

Evaluation Criteria

- Ease of use
 - User convenience, learning curve
- User cost
 - Token, Certs, card reader, SMS charges
- Implementation time
 - Application development time
 - Integration complexity
- Maintenance cost
 - Administration, operations, logistics
 - Infrastructure maintenance
- Service availability
 - Geographic mobility, card reader availability, telephone network congestion
- Loss recovery time
 - Time required to resume service after loss of token, SIM card, Certs

45

Solutions Comparison



47

Summary

- Identity theft and phishing are growing problems
- **Phishing is about stealing personal and confidential information**
- Defence strategies should adopt a multi-layer approach
- Anti-phishing solutions should rely less on user knowledge and awareness
- **Enforced mutual authentication at logon**

47

Thank You

email contact :
anti.phishing@gmail.com

EMA Project Team
K.C. Lau, Calvin Tam
Jeff Ho, W.W. Fung