HONG KONG

PISA

"Stay Smart, Keep Cyber Scam Away" Seminar
Build a Secure Cyberspace 2018

Phishing Awareness

2018-05-25
16:00 – 16:30
Lecture Theatre, Hong Kong Central Library

Connect | Educate | Inspire | Secure

Frankie Leung

CISA Certified Information Systems Auditor
CISM Certified Information Security Manager
CRISC Certified in Risk and Information Systems Control
CISSP Certified Information Systems Security Professional

Program Director, PISA (2015-2018)
Email: frankie.leung@pisa.org.hk
Website: http://www.pisa.org

Today's Agenda

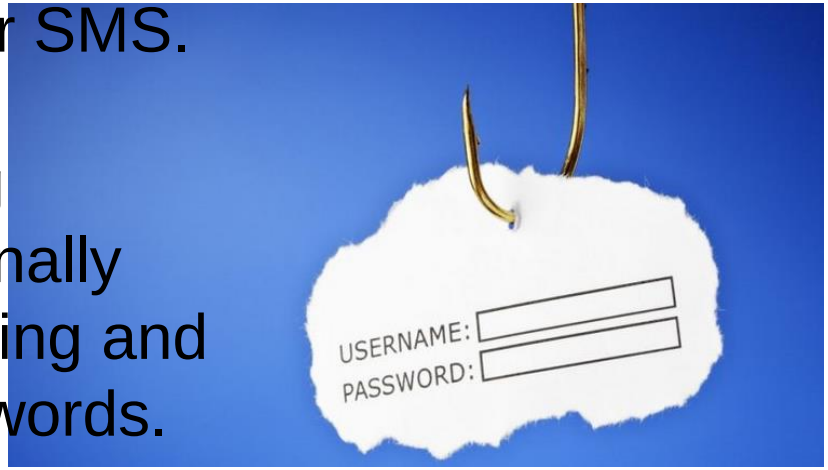
1. What is Phishing?
2. First Phishing Lawsuit
3. How to distinguish Phishing?
4. How is the dangerous of Phishing?
5. 10 Ways To Avoid Phishing Scams
6. What I can do if I am phished?
7. Who can help?
8. Free Resources

OFFICIAL (ISC)² CHAPTER | HONG KONG

PISA

What is Phishing?

- is a cybercrime
- a target or targets are contacted by email, Phone, Mobile Apps or SMS.
- lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.



- can result in identity theft and financial loss, reputational loss, intellectual property loss.

First Phishing Lawsuit

- A Californian teenager created the imitation of the website “America Online” to gain sensitive information from users and access the credit card details to withdraw money from their accounts in 2004 .

- ‘vishing' (voice phishing)
- 'smishing' (SMS Phishing

How to distinguish Phishing?

- Spam is unsolicited e-mail, usually from someone trying to sell something.
- Phishing email always have wrong spelling, wrong grammar (wrong)
- The Email Filter can screen out the Spam mail but not Phishing mail.

How to distinguish Phishing?

- Too Good To Be True
- Sense of Urgency
- Generic salutation
- Don’t Trust Your Eyes or URLs
- Attachments
- Unusual Sender

MESSAGE FROM BANK OF AMERICA

1 message

BANK OF AMERICA <info1@hyper.ocn.ne.jp> Wed, May 2, 2018 at 12:48 AM
Reply-To: jeffanderson955@gmail.com

Bank of America
115 W 42nd St, New York, NY 10036, USA
From Desktop of Mr. Jeff Anderson
Our Ref: BOF-0XX2/987/20
E-mail:jeffanderson955@gmail.com

It is my modest obligation to write you this letter as regards the Authorization of your owed payment through our most respected financial institution (Bank of America). I am Mr. Jeff Anderson, TRANSFER INSPECTION OFFICER, foreign operations Department Bank of America, the British Government in Conjunction with us government, World Bank, united Nations Organization on foreign Payment matters has empowered my bank after much consultation and consideration to handle all foreign payments and release them to their appropriate beneficiaries with the help of a Representative from Federal Reserve Bank of New York.

As the newly Appointed/Accredited International Paying Bank, We have been instructed by the world governing body together with the committee on international debt reconciliation department to release your overdue funds with immediate effect; with this exclusive vide transaction no.: wha/eur/202,password: 339331, pin code: 78569, having received these vital payment numbers, you are instantly qualified to receive and confirm your payment with us within the next 96hrs.

Be informed that we have verified your payment file as directed to us and your name is next on the list of our outstanding fund beneficiaries to receive their payment. Be advised that because of too many funds beneficiaries, you are entitled to receive the sum of $14.5M,(Fourteen Million Five Hundred Thousand Dollars only), as to enable us pay other eligible beneficiaries.

To facilitate with the process of this transaction, please kindly re-confirm the following information below:

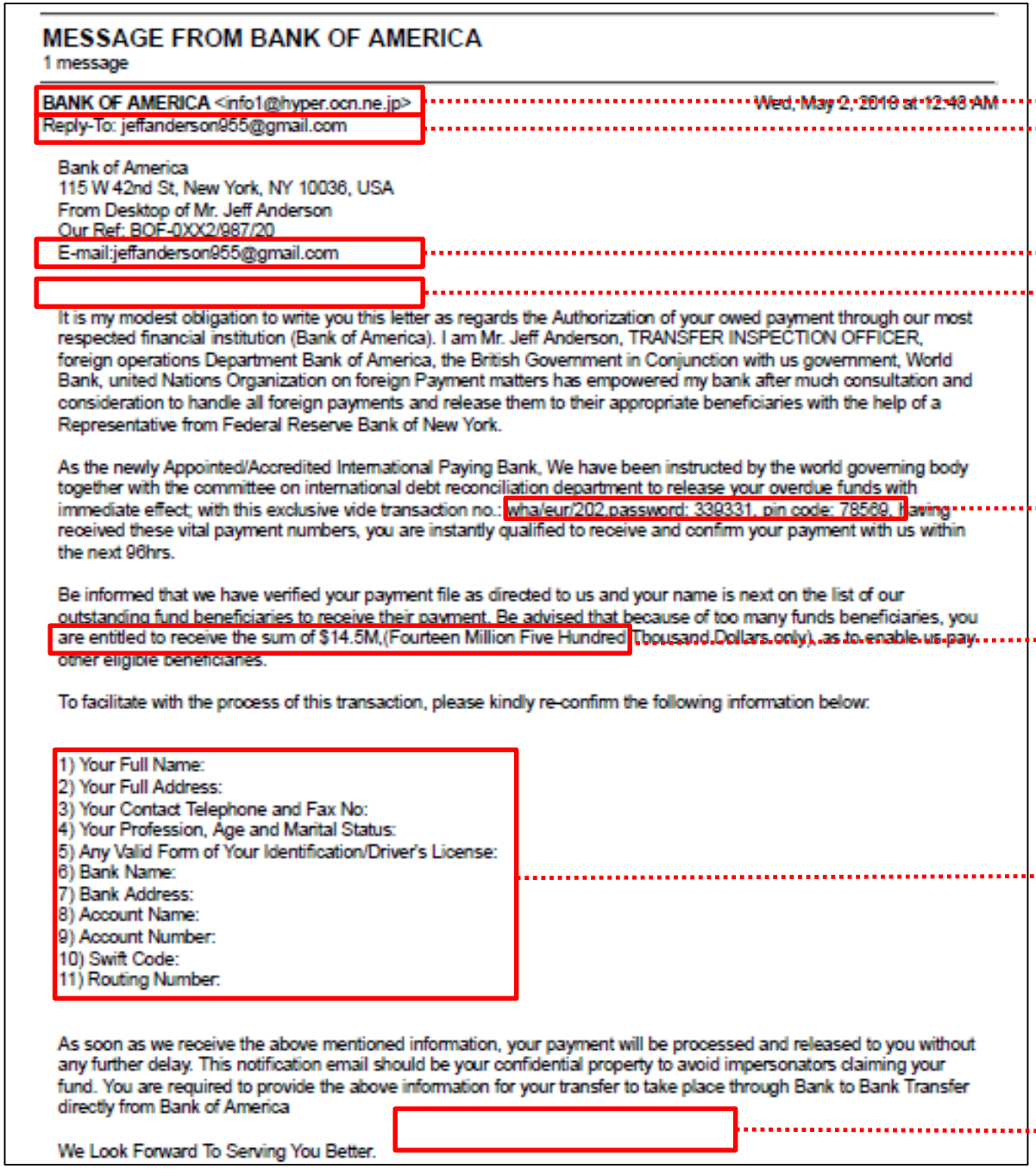
1) Your Full Name:
2) Your Full Address:
3) Your Contact Telephone and Fax No:
4) Your Profession, Age and Marital Status:
5) Any Valid Form of Your Identification/Driver's License:
6) Bank Name:
7) Bank Address:
8) Account Name:
9) Account Number:
10) Swift Code:
11) Routing Number:

As soon as we receive the above mentioned information, your payment will be processed and released to you without any further delay. This notification email should be your confidential property to avoid impersonators claiming your fund. You are required to provide the above information for your transfer to take place through Bank to Bank Transfer directly from Bank of America

We Look Forward To Serving You Better.

Typical Phishing Mail

PISA



MESSAGE FROM BANK OF AMERICA

1 message

BANK OF AMERICA <info1@hyper.ocn.ne.jp> Wed, May 2, 2018 at 12:48 AM

Reply-To: jeffanderson955@gmail.com

Bank of America
115 W 42nd St, New York, NY 10036, USA
From Desktop of Mr. Jeff Anderson
Our Ref: BOF-0XX2/987/20

E-mail:jeffanderson955@gmail.com

It is my modest obligation to write you this letter as regards the Authorization of your owed payment through our most respected financial institution (Bank of America). I am Mr. Jeff Anderson, TRANSFER INSPECTION OFFICER, foreign operations Department Bank of America, the British Government in Conjunction with us government, World Bank, united Nations Organization on foreign Payment matters has empowered my bank after much consultation and consideration to handle all foreign payments and release them to their appropriate beneficiaries with the help of a Representative from Federal Reserve Bank of New York.

As the newly Appointed/Accredited International Paying Bank, We have been instructed by the world governing body together with the committee on international debt reconciliation department to release your overdue funds with immediate effect; with this exclusive vide transaction no.: wha/eur/202,password: 339331, pin code: 78569. Having received these vital payment numbers, you are instantly qualified to receive and confirm your payment with us within the next 96hrs.

Be informed that we have verified your payment file as directed to us and your name is next on the list of our outstanding fund beneficiaries to receive their payment. Be advised that because of too many funds beneficiaries, you are entitled to receive the sum of $14.5M,(Fourteen Million Five Hundred Thousand Dollars only), as to enable us pay other eligible beneficiaries.

To facilitate with the process of this transaction, please kindly re-confirm the following information below:

1) Your Full Name:
2) Your Full Address:
3) Your Contact Telephone and Fax No:
4) Your Profession, Age and Marital Status:
5) Any Valid Form of Your Identification/Driver's License:
6) Bank Name:
7) Bank Address:
8) Account Name:
9) Account Number:
10) Swift Code:
11) Routing Number:

As soon as we receive the above mentioned information, your payment will be processed and released to you without any further delay. This notification email should be your confidential property to avoid impersonators claiming your fund. You are required to provide the above information for your transfer to take place through Bank to Bank Transfer directly from Bank of America

We Look Forward To Serving You Better.

Not from Bank of America Email Domain

Not from Bank of America Email Domain

They do not know who you are and not specify to who. Sometimes, they may use dear Sir/Madam

No Bank or Financial Institute released the Password in Plaint Test in Email.

Too Good to be True! Are you so lucky?

No Bank or Financial Institute ask for personal information over the email. They want to get your personal information to steal your identification.

No Telephone Number for you to call back. In fact, it is a phone number from any No Bank or Financial Institute, please call their general inquiry hot line instead of any number.

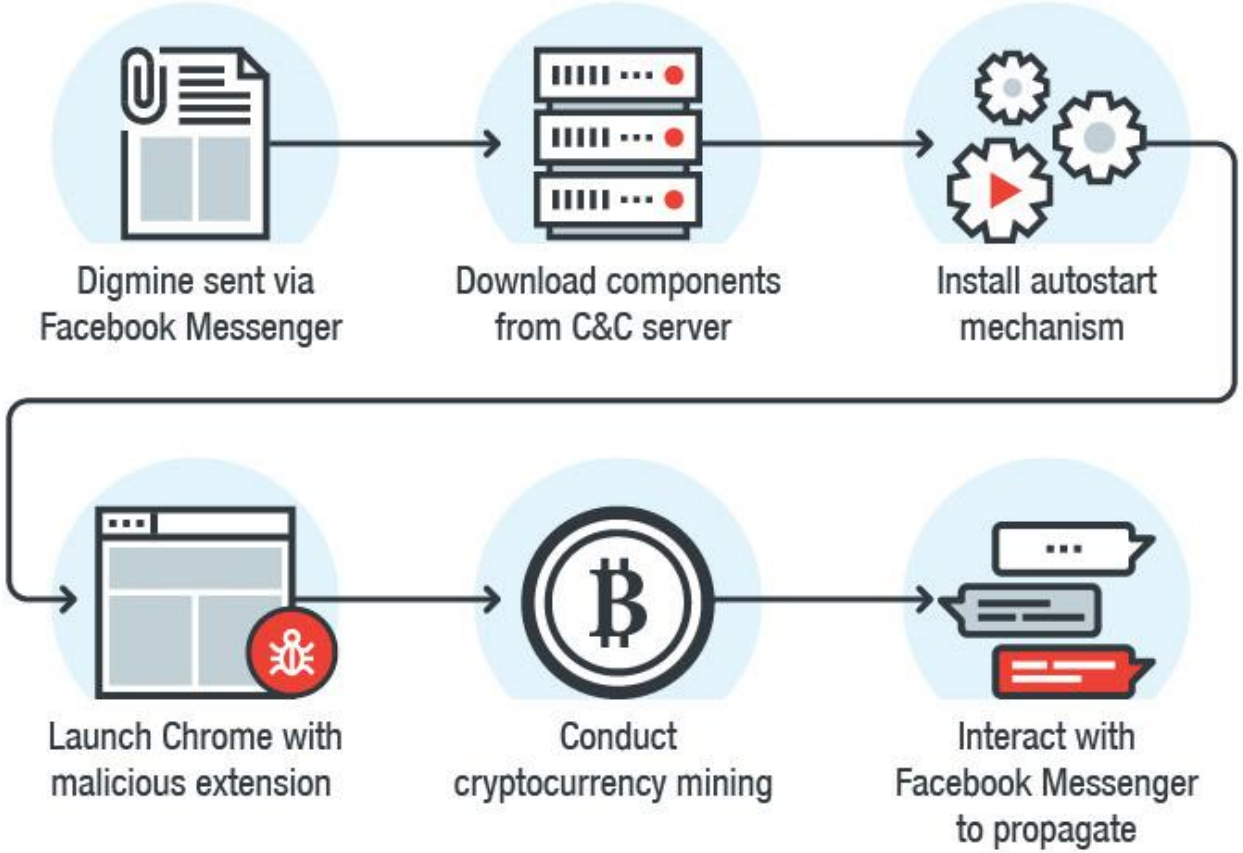
How is the dangerous of Phishing?

Source: https://www.esecurityplanet.com/network-security/over-97-percent-of-all-phishing-emails-deliver-ransomware.html

New trend for Crypto-miner on Mobile

https://arstechnica.com/information-technology/2017/12/currency-mining-android-malware-is-so-aggressive-it-can-physically-harm-phones/

New trend for Crypto-miner on Mobile



Over 500,000 Windows Machines infected with Monero Mining Software

https://www.infosecurity-magazine.com/news/over-500000-machines-infected/

OFFICIAL (ISC)² CHAPTER | HONG KONG

PISA

10 Ways To Avoid Phishing Scams

- Think Before You Click!
- Pick Up the Phone to Verify
- Install an Anti-Phishing Toolbar
- Verify a Site's Security
- Effective Anti-Phishing Policies
- Be Wary of Pop-Ups
- Never Give Out Personal Information
- Keep Your Browser, OS and Apps Up to Date
- Use legal Antivirus Software
- Conduct security awareness training or phishing simulations

OFFICIAL (ISC)² CHAPTER | HONG KONG

PISA

What I can do if I am phished?

- ✓ If you have provided login credentials in suspicious website, please reset password and review the security settings in the related online service accounts.
- ✓ If you have provided financial information, such as credit card number, and incur financial loss, please contact your bank immediately.
- ✓ You should report to nearby police station if any financial loss is incurred.
- ✓ If someone spoofs your identity to send email to your family, friends and business partners, you should alert them by other trusted communication channels.

OFFICIAL (ISC)² CHAPTER | HONG KONG

PISA

Who can help?

- Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT)
- Hong Kong Government OGCIO
  - www.infosec.gov.hk
  - www.cybersecurity.hk
- Hong Kong Police Cyber Security and Technology Crime Bureau (CSTCB)
- PISA and (ISC)2 Hong Kong Chapter

OFFICIAL (ISC)² CHAPTER | HONG KONG

PISA

Free Resources

Anti-Spam

- Mail washer
  http://www.mailwasher.net/
- Spam Fighter
  http://www.spamfighter.com/SPAMfighter/Product_Info.asp

Web Filtering

- K9 Web Filtering
  http://www1.k9webprotection.com/
- Handy Filter
  http://www.handyfilter.com/

Reference

- OGCIO
  - Information Security www.infosec.gov.hk
  - Cyber Security www.cybersecurity.hk
- HK Cert
  - https://www.hkcert.org/my_url/en/guideline/18040602
- Professional Information Security Association
  - www.pisa.org.hk
- Microsoft Safety Scanner
  - www.microsoft.com/security/scanner
- MailWasher
  - http://www.mailwasher.net/
- Spam Fighter
  - http://www.spamfighter.com/SPAMfighter/Anti_spam_software.asp

Reference

- www.phishing.org/what-is-phishing
- http://www.dummies.com/computers/pcs/how-to-recognize-a-phishing-scam/
- https://cdn2.hubspot.net/hubfs/241394/Knowbe4-May2015-PDF/SocialEngineeringRedFlags.pdf?t=1524675334093
- https://www.knowbe4.com/what-is-social-engineering/?hsLang=en&__hstc=59035826.b926b416dc8150c71e54919cb294bee3.1524677217276.1524677217276.1524677217276.1&__hssc=59035826.5.1524677217278&__hsfp=2143943458
- Best Practices for Dealing With Phishing and Ransomware - An Osterman Research White Paper, Published September 2016

End of Presentation
Thank You.