FORUM 2017: Creating Connections Together

Cyber Security in the Social Media Age

Special Agent Robert J Brown
Virginia State Police

Virginia State Police High Technology Crimes Division

High Tech Crimes Section

- 15 Special Agents
  - Forensic Examinations
  - Network Security Investigations
  - Computer Facilitated Crimes

What you will learn

- Current trends of cyber attacks
- Discuss an actual compromise
- Best practices to protect yourself

Current Threats

Current Threats

- Malware
- Business Email Compromise

How do compromises start

- Phishing Attacks
  - Spear Phishing
    - Customized messages to individual person
    - Link to fraudulent website
    - Link that downloads malware

How do compromises start

- Phishing Attacks
  - Deceptive Phishing
    - Mass messages using legitimate companies
    - Tricked to entering log-on credentials

Malware

- Trojan
- Spyware
- Backdoor
- Keyloggers
- Ransomware

Ransomware

- Encrypts or Locks personal files
- Encryption Key required to unlock
- Request payment by Bitcoin

WannaCry – May 2017

Technology

NHS 'could have prevented' WannaCry ransomware attack

2 hours ago | Technology

Share

BadRabbit – Oct 2017

Business Email Compromise

Email appears to be sent from a trusted source

Actually a “spoofed” message

Business Email Compromise

Compromises

Email Accounts

Calendars

BEC Case

- Small but International company
  - About 10 employees
- Owner/Chairman resides in Europe
- CEO & CFO based in US
- Regularly conduct business via Wire Transfer
  - 4-10 per week

BEC Case

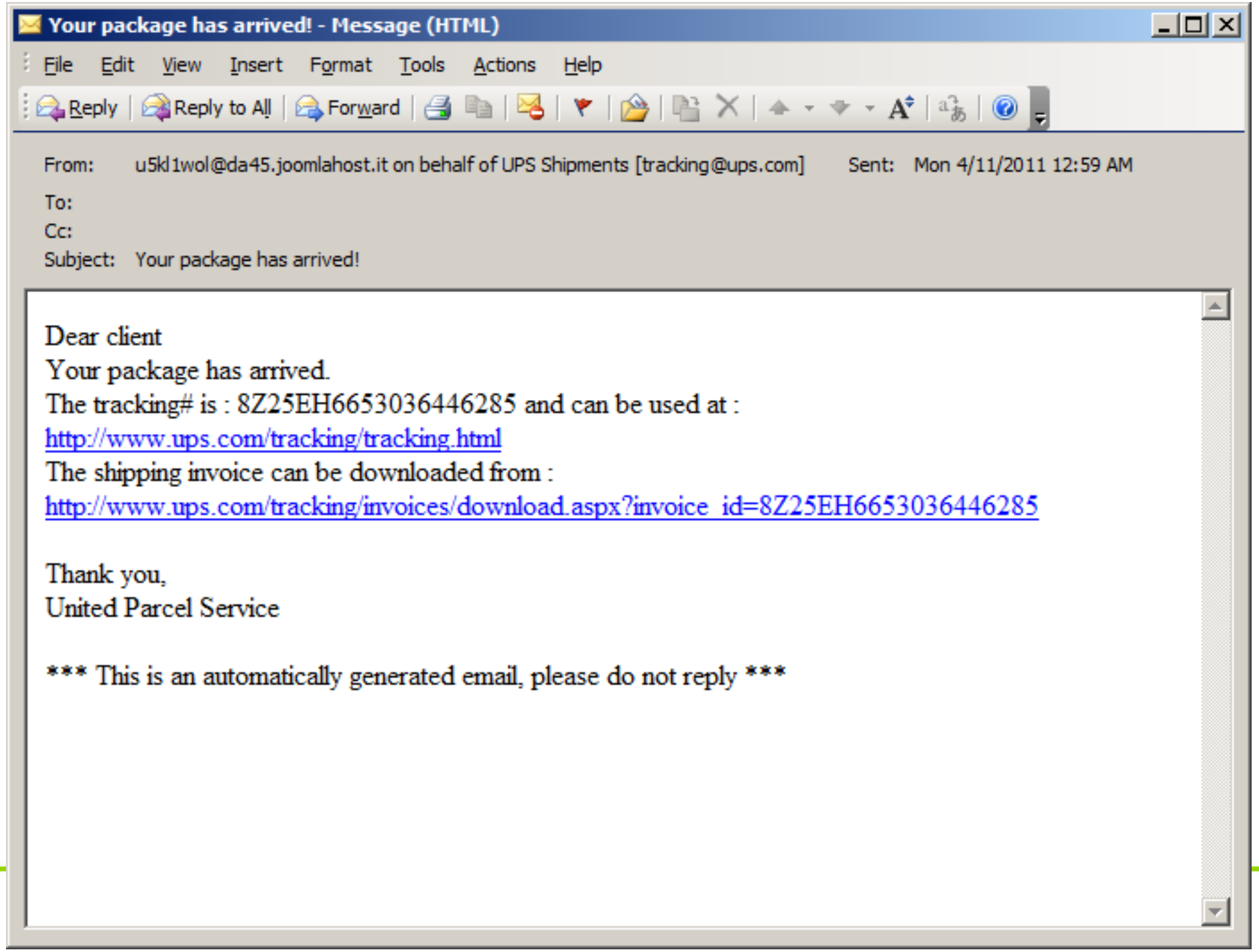
- CEO or Chairman communicate prior to transfer of funds via Email
- CEO, CFO and Chairman must all agree before funds are transferred

BEC Case

- CFO has LinkedIn, Facebook accounts
- Website, Email accounts through Google

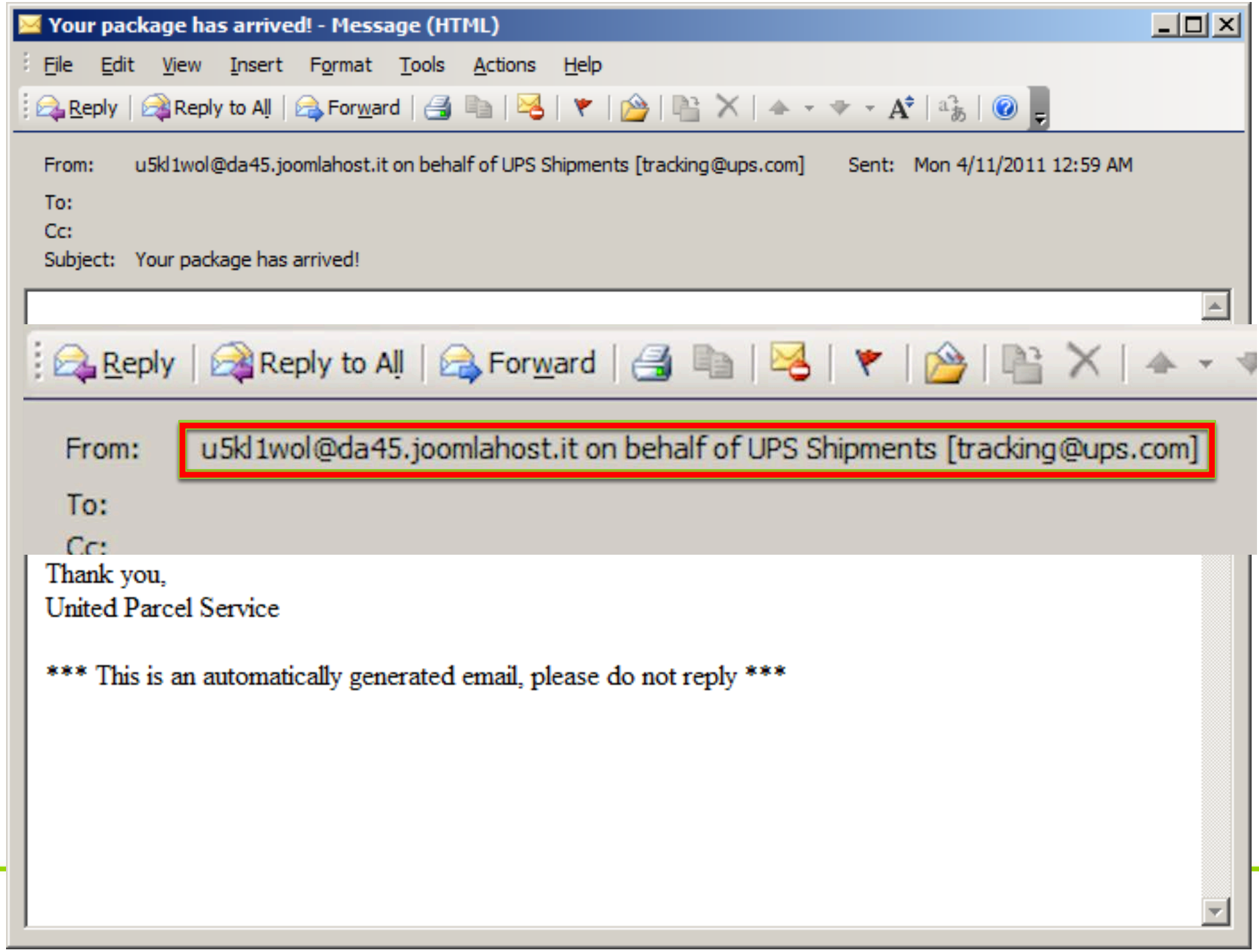
BEC Case

- March 2017 CFO receives Email he believes is from UPS sending him link to track a package


Your package has arrived! - Message (HTML)
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward
From: u5kl1wol@da45.joomlahost.it on behalf of UPS Shipments [tracking@ups.com] Sent: Mon 4/11/2011 12:59 AM
To:
Cc:
Subject: Your package has arrived!
Dear client
Your package has arrived.
The tracking# is : 8Z25EH6653036446285 and can be used at :
http://www.ups.com/tracking/tracking.html
The shipping invoice can be downloaded from :
http://www.ups.com/tracking/invoices/download.aspx?invoice_id=8Z25EH6653036446285
Thank you,
United Parcel Service
*** This is an automatically generated email, please do not reply ***

BEC Case

- Email seems legit
- Same format as previous messages
- CFO clicks on link, nothing happens


Your package has arrived! - Message (HTML)
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward
From: u5kl1wol@da45.joomlahost.it on behalf of UPS Shipments [tracking@ups.com] Sent: Mon 4/11/2011 12:59 AM
To:
Cc:
Subject: Your package has arrived!
Reply Reply to All Forward
From: u5kl1wol@da45.joomlahost.it on behalf of UPS Shipments [tracking@ups.com]
To:
Cc:
Thank you,
United Parcel Service
*** This is an automatically generated email, please do not reply ***

BEC Case

- Link has downloaded Malware
  - Keylogger
- Criminal gained access
  - Social Media
  - Business Email account

BEC Case

- Previous transactions
- Communication protocols
- Monitored current business contracts

Re: Hangseng Bank, Hongkong & Cimb Bank. Malaysia

NS

[redacted]n>
Thursday, May 11, 2017 at 2:44 PM
To: accounts
Cc [redacted]m

Pl go ahead

Sent from my iPad

On Fri, May 12, 2017 at 2:42 AM, [redacted].com> wrote:

> Dakshaybhai,
> Kindly arrange to pay 520,287 usd Hong Kong from SOR LLC and 250,231 usd to Malaysia to:
>
> **Beneficiary Name:** HAWTAI TECHNOLOGY CO., LIMITED
> **Beneficiary full Address:** 83 DES VOEUX ROAD
> CENTRAL HONG KONG
> **Beneficiary A/C NO:** 788-282663-883
> **Beneficiary Bank Name:** HANG SENG BANK
> **Beneficiary Bank full Address:** HONGKONG
> **Beneficiary Bank Swift Code:** HASEHKHH
>
> **Beneficiary Name:** EZEE B RESOURCES
> **Beneficiary full Address:** 227 JALAN BANDAR 13, TAMAN MELAWATI,
> 53100 KUALA LUMPUR,
> MALAYSIA
> **Beneficiary A/C NO:** 8007988652
> **Beneficiary Bank Name:** CIMB BANK BERHARD
> **Beneficiary Bank full Address:** MALAYSIA
> **Beneficiary Bank Swift Code:** CIBBMYKL
>
> Regards
>
> manish

BEC Case

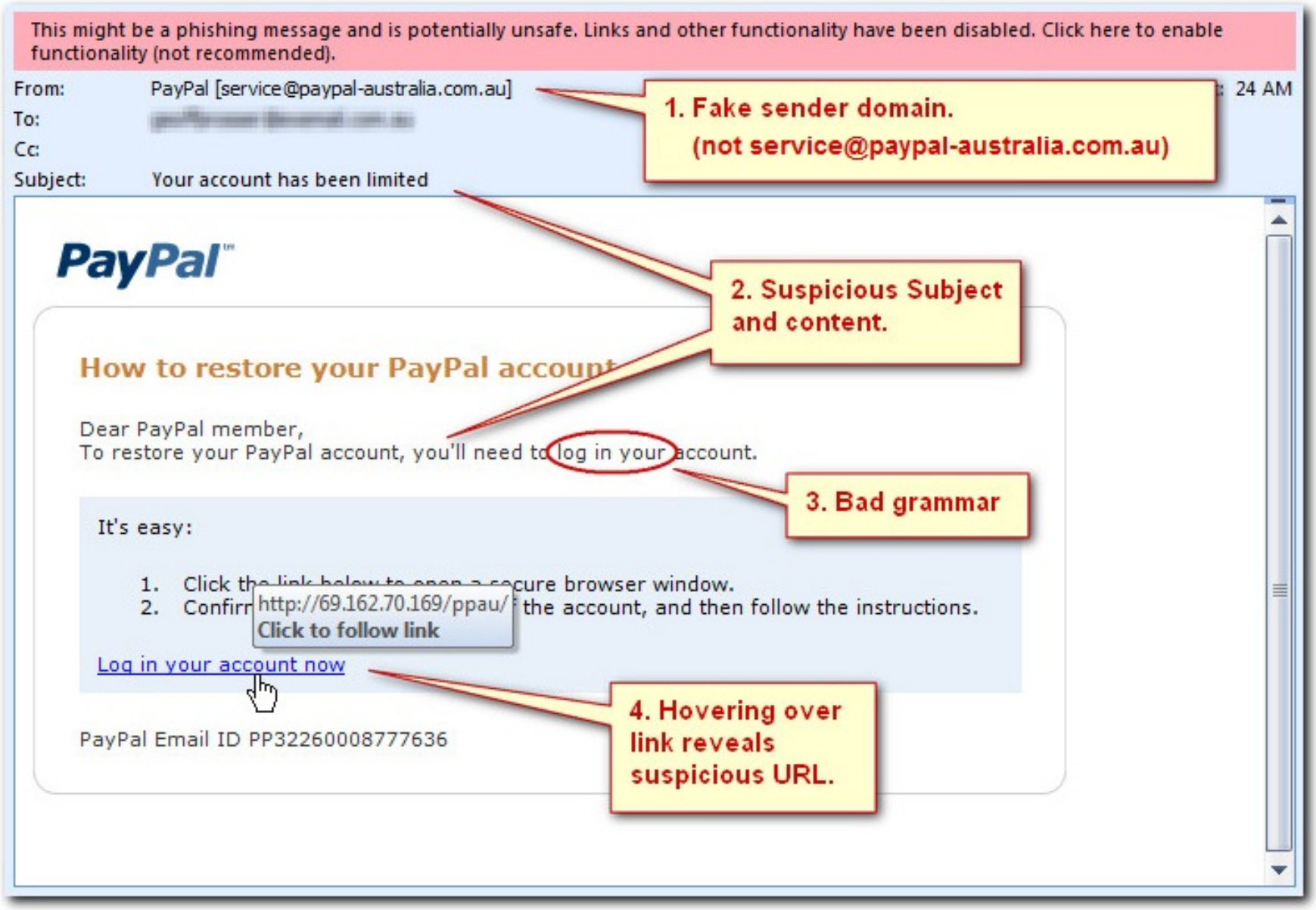
- 8 days in May 2017
  - 11 fraudulent wire transfers
  - $ 3,765,800.00 lost

Protecting Yourself

Phishing Attacks

- Scrutinize Email messages
  - Look at the senders informatio
  - Hover over links
  - Check the URL of the website
  - Don’t respond to unsolicited messages with personal information


From:
on behalf of
Amazon <management@mazoncanada.ca>
not an Amazon email address
(note the missing A in Amazon)
To:
@sheridanc.on.ca
Cc:
Subject: Suspension
amazon.com
Dear Client,
Generic non-personalized greeting
We have sent you this e-mail, because we have strong reason to belive, your account has been used by someone else.In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.
To confirm your identity with us click the link bellow:
https://www.amazon.com/exec/obidos/sign-in.html
Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"
Sincerely,
The Amazon Associates Team
© 1996-2013, Amazon.com, Inc. or its affiliates


This might be a phishing message and is potentially unsafe. Links and other functionality have been disabled. Click here to enable functionality (not recommended).
From: PayPal [service@paypal-australia.com.au]
To:
Cc:
Subject: Your account has been limited
24 AM
1. Fake sender domain.
(not service@paypal-australia.com.au)
PayPal
2. Suspicious Subject and content.
How to restore your PayPal account
Dear PayPal member,
To restore your PayPal account, you'll need to log in your account.
3. Bad grammar
It's easy:
1. Click the link below to open a secure browser window.
2. Confirm the account, and then follow the instructions.
http://69.162.70.169/ppau/
Click to follow link
Log in your account now
4. Hovering over link reveals suspicious URL.
PayPal Email ID PP32260008777636

Protecting Yourself

Social Media

- Customize your Privacy Settings
- Limit the amount of personal information you post

Protecting Yourself

Social Media

- Don’t accept friend requests from strangers
- Use strong passwords
- Remember the Internet is a public resource

Protecting Yourself

Update Software

Backup Data regularly

- Use external storage
- Flash Drives & Hard Driv

Protecting Yourself

WiFi Security

- Change the default passwords
- Ensure WPA2/AES is enab
- Update firmware
- Turn off when not in use

Protecting Yourself

Lock your Computer

Create strong passwords

Be Skeptical


VIRGINIA
SIC SEMPER TYRANNIS
TROOPER
VIRGINIA
STATE POLICE