Internal Cybersecurity Risks

Peg Bodin, CISA – Local IS Audit Program Manager
Michael Hjermstad – Local IS Audit Assistant Manager
Joseph Clark - Performance Auditor

The risk

The following BEC/EAC statistics were reported in victim complaints to the IC3 from **October 2013 to December 2016:**

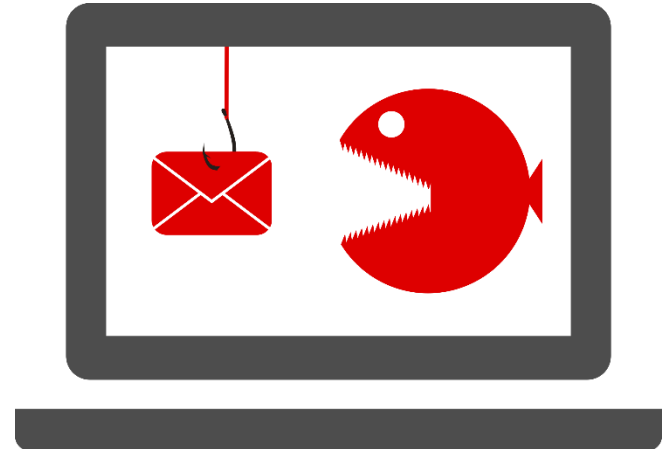|	
Total U.S. victims:	22,292
Total U.S. exposed dollar loss:	$1,594,503,669
Total non-U.S. victims:	2,053
Total non-U.S. exposed dollar loss:	$626,915,475

BEC = Business Email Compromise

EAC = Email Account Compromise

Source: IC3 (Internet Crime Complaint Center)

Phishing emails

- Your W-2 is available online, click here (sent in mid- to late January)

- Win Seahawks tickets!

Phishing Campaign:
Open: 1 minute, 40 seconds
Click: 3 minutes, 45 seconds

Source: Verizon 2016 DBIR

Business email and email account compromise scams

- I'm your boss, please respond to me, via return email, an employee report (with SSNs)

- I'm your boss, I need you to transfer $$$ to this bank account

- I'm your vendor, pay this invoice and send the $$$ to this bank account

Phishing really works — well

- *"most successful variety [of social engineering] is phishing"*
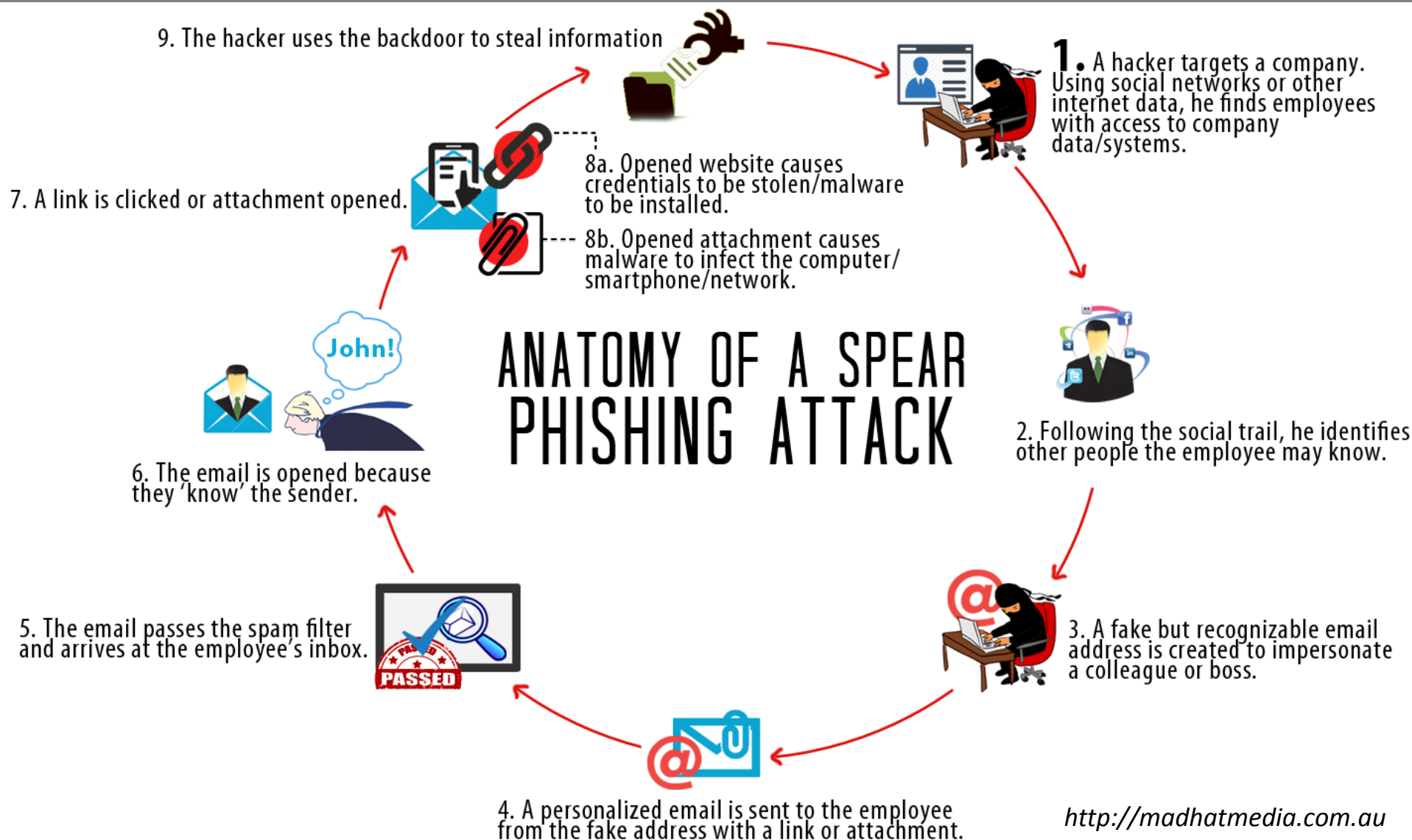- *"30% of phishing messages were opened"*

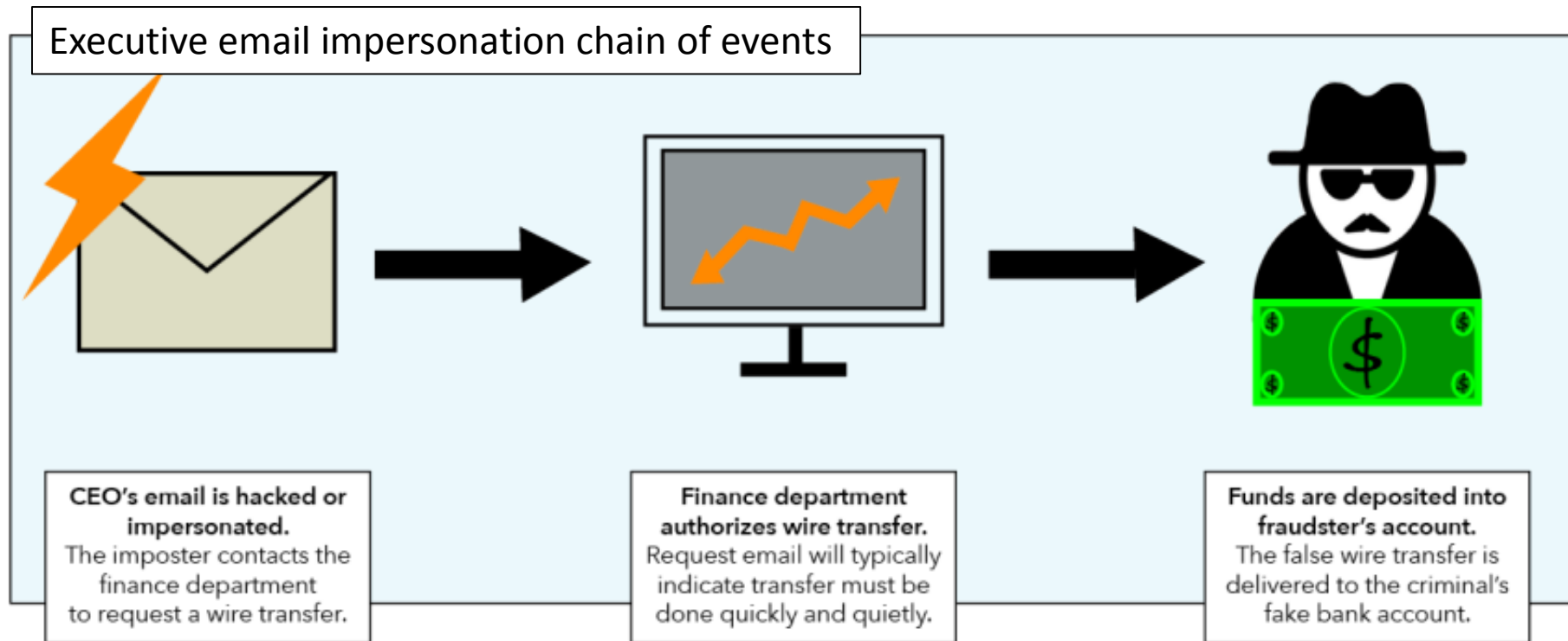- *Reliance on employees for advanced phishing detection*

- *Phishing as a service is twice as profitable as traditional phishing*

9. The hacker uses the backdoor to steal information

1. A hacker targets a company. Using social networks or other internet data, he finds employees with access to company data/systems.

8a. Opened website causes credentials to be stolen/malware to be installed.

7. A link is clicked or attachment opened.

8b. Opened attachment causes malware to infect the computer/smartphone/network.

ANATOMY OF A SPEAR PHISHING ATTACK

John!

6. The email is opened because they 'know' the sender.

2. Following the social trail, he identifies other people the employee may know.

5. The email passes the spam filter and arrives at the employee's inbox.

PASSED

3. A fake but recognizable email address is created to impersonate a colleague or boss.

4. A personalized email is sent to the employee from the fake address with a link or attachment.

http://madhatmedia.com.au

Executive email scam

Executive email impersonation chain of events

CEO's email is hacked or impersonated.
The imposter contacts the finance department to request a wire transfer.

Finance department authorizes wire transfer.
Request email will typically indicate transfer must be done quickly and quietly.

Funds are deposited into fraudster's account.
The false wire transfer is delivered to the criminal's fake bank account.

Executive email scam example

From: John Doe <John_Doe@example.com>
Sent: Thursday, April 17, 2014 11:46 AM
To: Smith, Jim

Subject: Fwd: Wiring instructions ·········· 🗎 ANGTAI WIRING INSTRUCTION.pdf (88 KB)

Process a wire for $260,536.17 to the attached instructions, code this to admin expenses. Send me the wire confirmation once completed.

John

------------ Forwarded message ------------
From: **Joe Jones** <Joe_Jones@example.com>
Date: Apr 18, 2014
Subject: Wiring instructions
To: John_Doe@example.com
John,

Per our conversation, attached is the wiring instructions. Forward wire confirmation when you have it.

Joe

Sanitized sample of an email used in this campaign to trick targets into wiring funds to the attacker's account

The attached PDF contains instructions for the wire transfer, including the destination account

WIRING INSTRUCTION

BANK NAME: ·········· SHANGHAI PUDONG DEVELOPMENT BANK, OFFSHORE BANKING UNIT.

BANK ADDRESS: ·········· NO 12 ZHONGSHAN DONG YI LU, SHANGHAI

ACCOUNT NAME: ·········· ANGTAI INTERNATIONAL CO LIMITED.

ACCOUNT NUMBER: ·········· ████████ 2009

SWIFT CODE: ·········· █████ HOSA

Mitigations to consider

- Have a system for reporting phishing

- Provide training that emphasizes:

  - Know who to contact; quicker is better

  - Pick up a phone before acting on the email

  - Be wary of suspicious phone calls

  - Do not use a website connected to the email

- Set up an internal phishing program

- Use email system rules

- Scrutinize all e-mail requests for fund transfers to determine if the requests are out of the ordinary
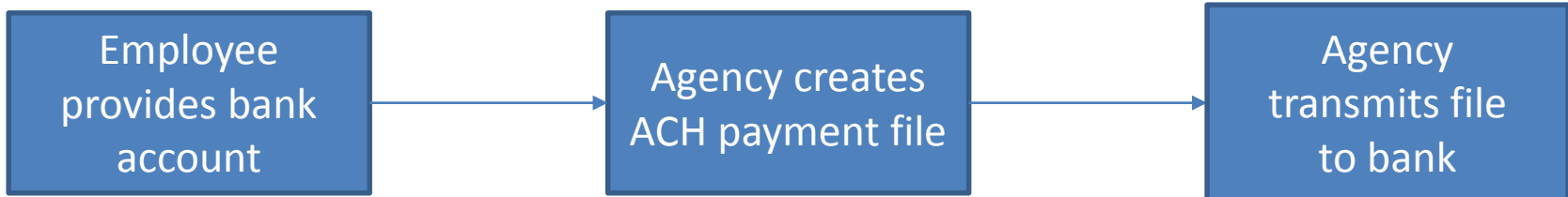
- Patch systems for critical vulnerabilities

I'm from your IT department, I need you to confirm your password by going to this site

Business credentials compromise

- Computerworld: Hacker steals teacher's direct deposit paycheck

- KrebsOnSecurity: Crooks hijack retirement funds via SSA portal

Employee provides bank account	→	Agency creates ACH payment file	→	Agency transmits file to bank

Phishing for credentials?

When you "mouse over" the hidden link

A compromised website with a fake Washington HRMS web link
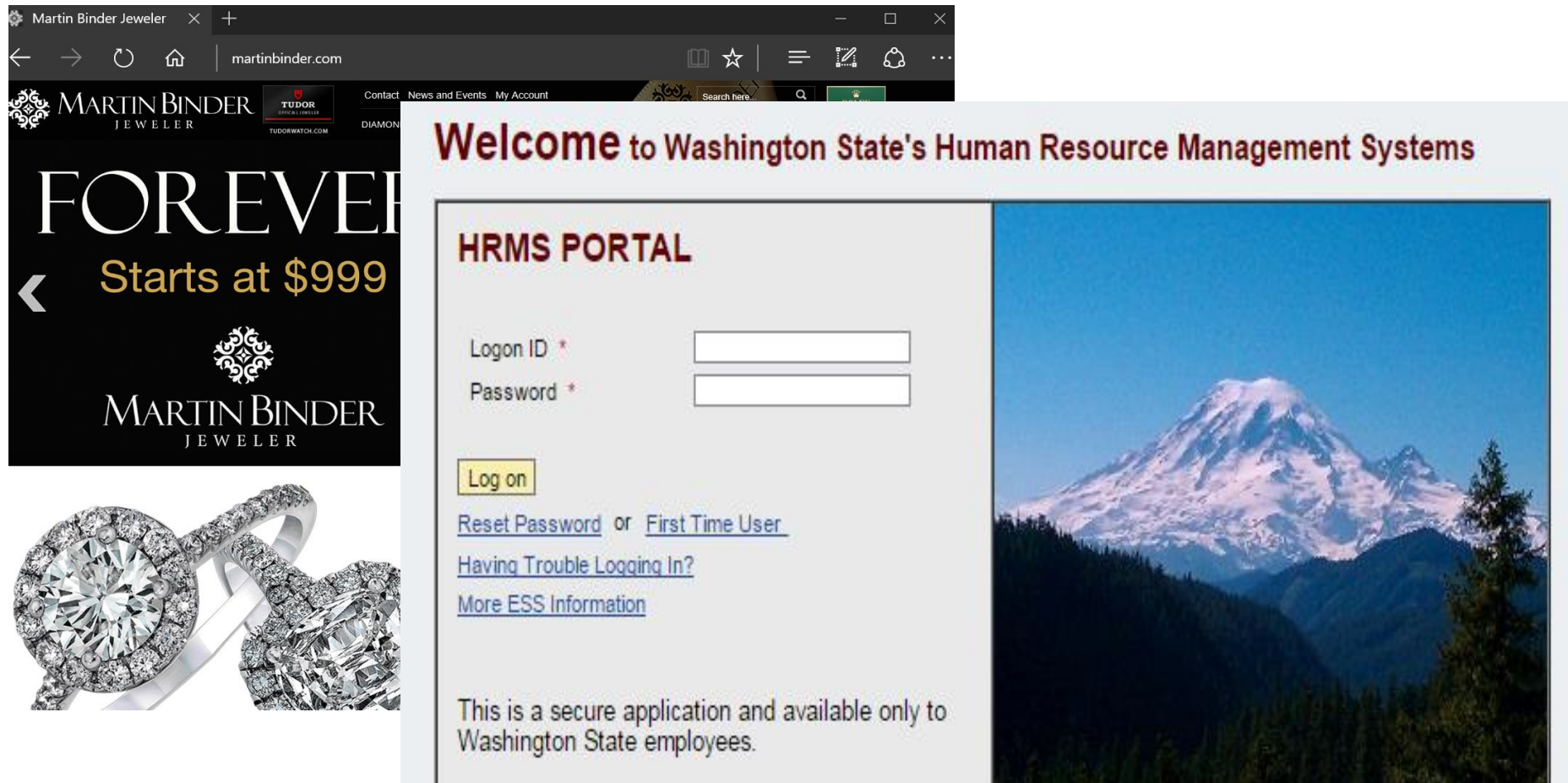
Convincing web page to make victim think everything is OK
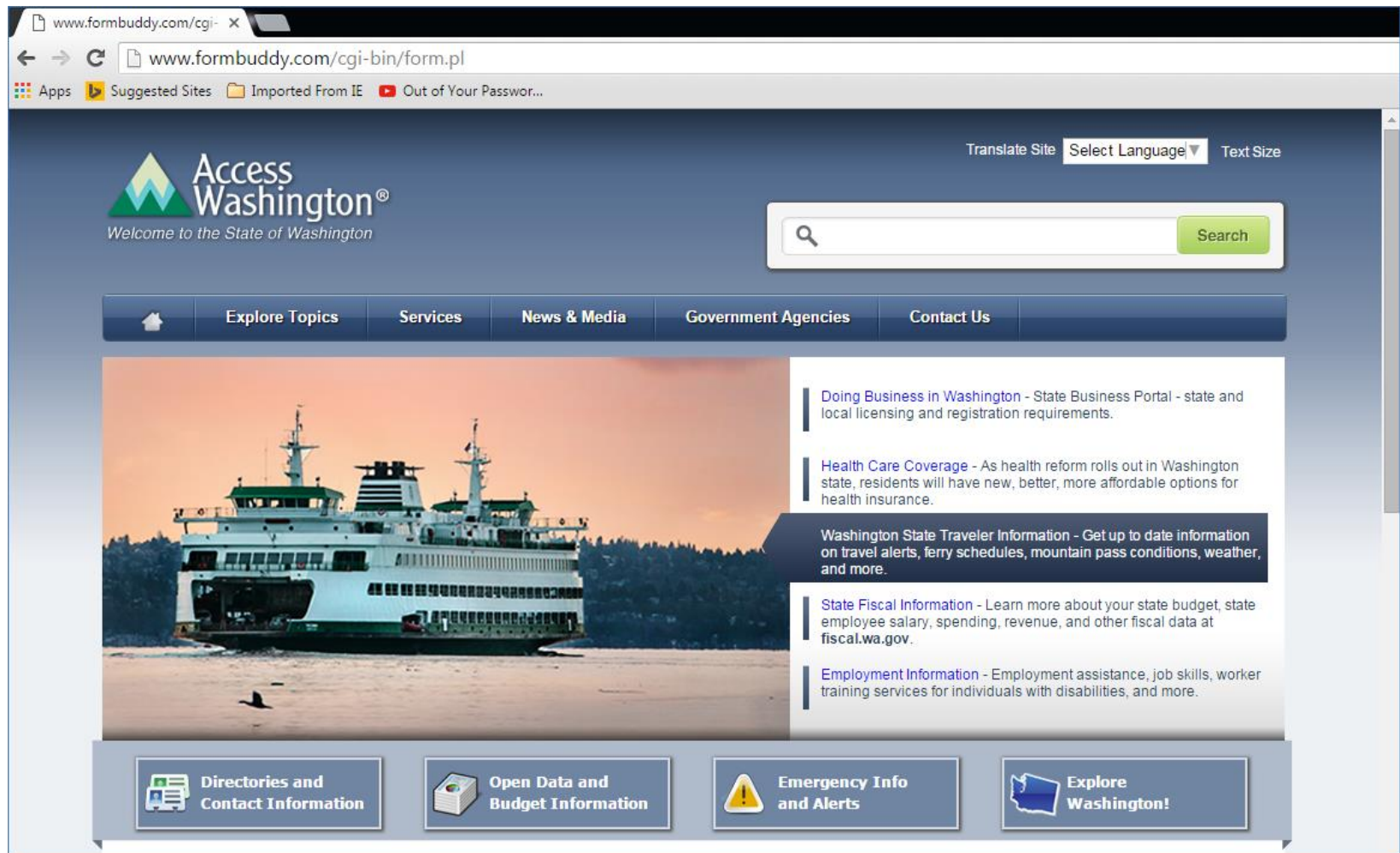
Spear-phishing email used in DNC attacks

Text of spear-phishing email sent to John Podesta, the chairman of the 2016 Clinton presidential campaign.

From: Google <no-reply@accounts.googlemail.com>

Date: March 19, 2016 at 4:34:30 AM EDT

To: ████████ @gmail.com

Subject: *Someone has your password*

Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account
████████ @gmail.com.

Details:

Saturday, 19 March, 8:34:30 UTC

IP Address: 134.249.139.239

Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD <https://bit.ly/1PibSU0>
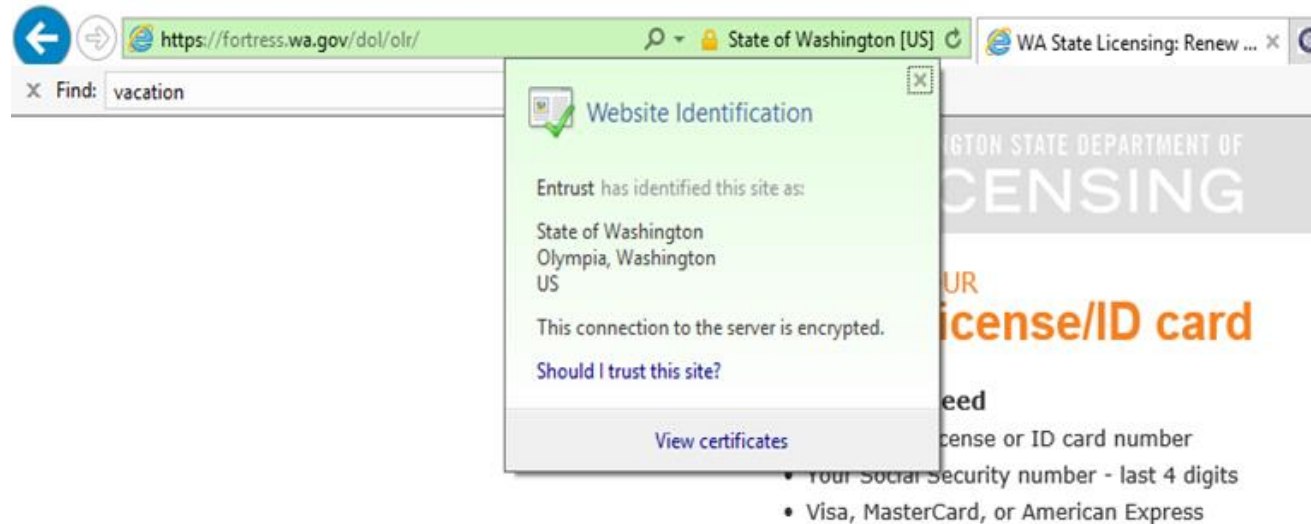
Best,

The Gmail Team

You received this mandatory email service announcement to update you about important changes to your Google product or account.

Source: Symantec Internet Security Threat Report

- Only conduct financial or secure transactions on a secure webpage with encryption

- Verify by hovering

Mitigations to consider

- Reputable organizations do not ask for personal information via email

- Spam email filters reduce phishing email

- Dual-factor authentication

- No password multi-use

- Risk assessment

- Incident response

Mission critical systems

- Emergency communications

- Air traffic control

- Electrical systems

- Heating/cooling systems

- Water/sewer systems

- What else?

Serious impacts

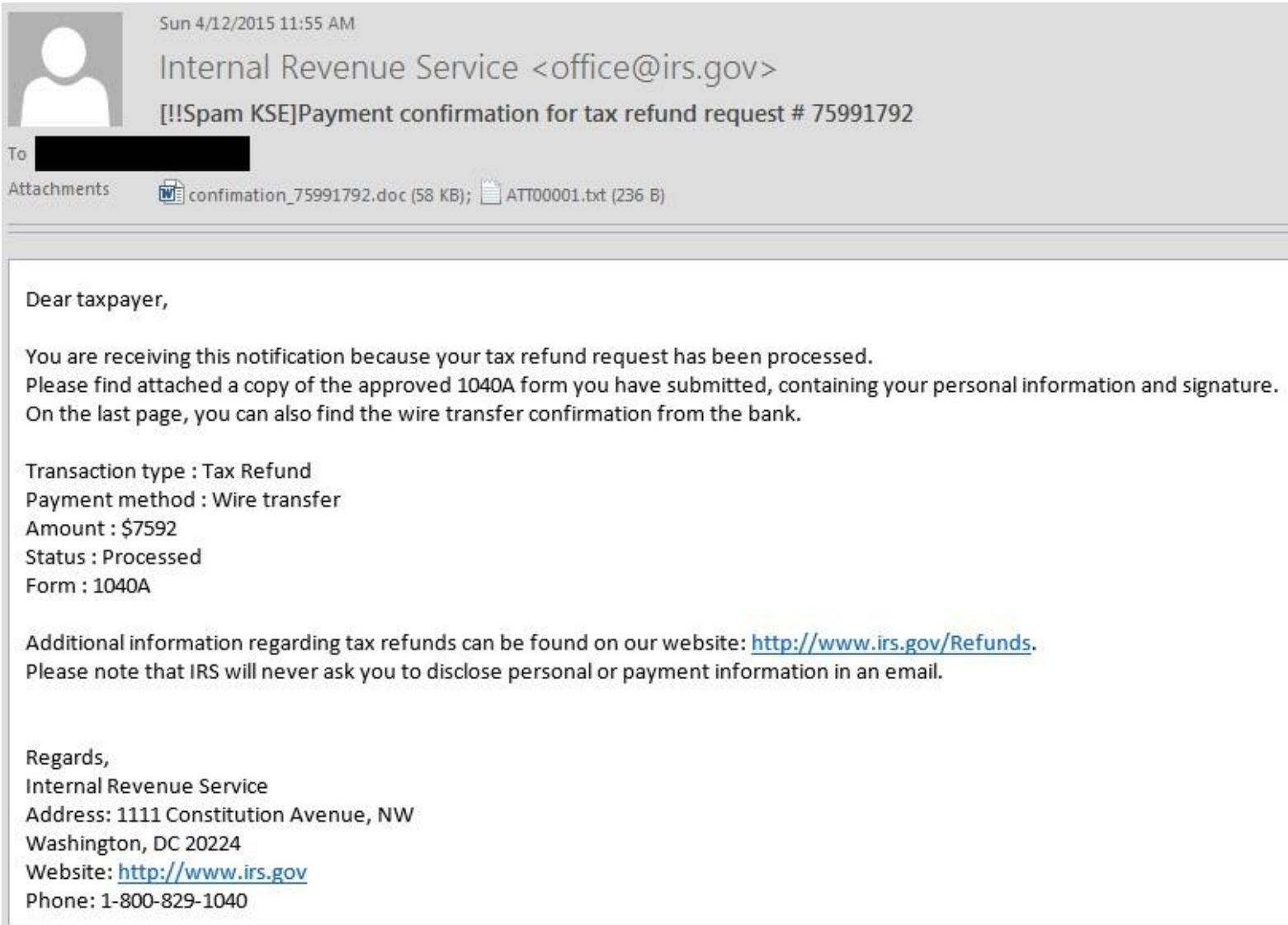Major events

- Ransomware

- Exfiltrated confidential information

Costs

- Loss of trust

- Breach notifications (multi-state)

- Lawyers

- Security experts

- Lost revenue

Ransomware

Have bitcoin?

CryptoLocker

Your Personal files are encrypted!

Your personal files **encryption** produced on this computer: photos, videos, documents, etc. Encryption was produced using a **unique** public key RSA-2048 generated for this computer.

To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **1.00 bitcoin** (~291 USD).

You can easily delete this software, but know that without it, you will never be able to get your original files back.

Disable your antivirus to prevent the removal of this software.

For more information on how to buy and send bitcoins, click "Pay with Bitcoin" To open a list of encoded files, click "Show files"
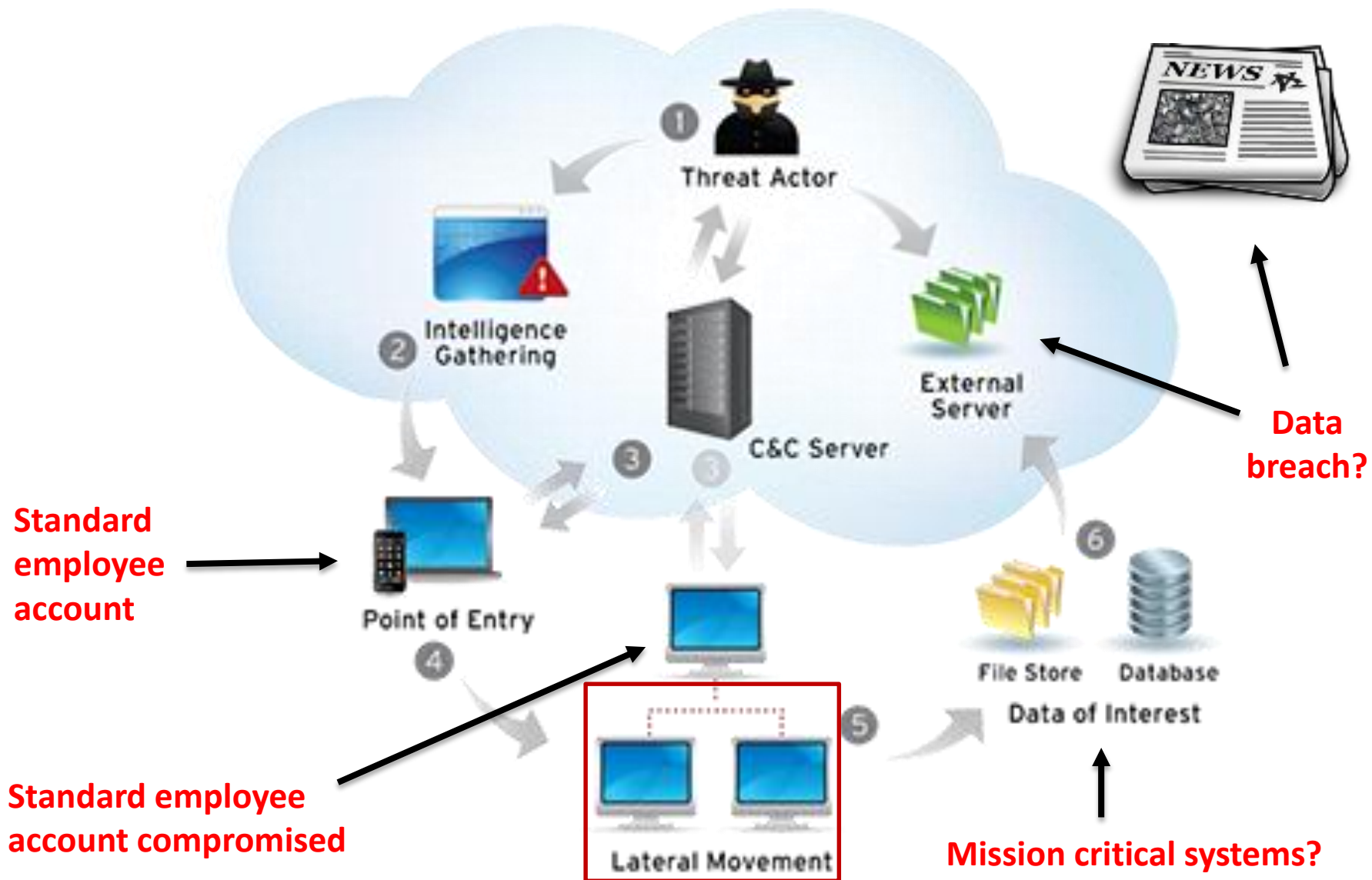
Do not delete this list, it will be used for decryption. And do not move your files.

Private key will be destroyed on

1/6/2015 1:11:47 PM

Time left

71:52:21

Checking wallet..

Received: 0.00 BTC

Show files   Pay with Bitcoin

Data breach?

Standard employee account

Standard employee account compromised

Mission critical systems?

Mitigations and other considerations

- Back up your critical information (air gapped)

- Limit user access to only what employees need

  - Least-privilege rule or role-based security

- Segment the network – not all systems have access to all other systems

- Devise a continuity-of-operations plan; identify key systems

- Complete and test an IT data recovery plan

Reporting incidents

- For government agencies, report fraud or theft to our Office:
  http://portal.sao.wa.gov/saoportal/public.aspx/LossReport

- Data breach notification:
  http://www.atg.wa.gov/data-breach-notifications

- File a complaint with FBI Internet Crime Complaint Center:
  www.ic3.gov (regardless of loss size)
  BEC.IC3.gov (business email compromises)

- Consumers can report identity theft to Federal Trade Commission:
  IdentityTheft.gov

Audits

- **Performance audits**

- **Financial statement audits**

- **Accountability audits**

  - Backups

  - User access

  - IT vendor management/contracts

  - Current policies and procedures

- **Federal financial assistance audits**

Questions?

Pat McCarthy
State Auditor
(360) 902-0360
Pat.McCarthy@sao.wa.gov

Peg Bodin, CISA
Local IS Audit Program Manager
(360) 464-0114
Peggy.Bodin@sao.wa.gov

Mike Hjermstad
Assistant Audit Manager
(253) 372-6250
Michael.Hjermstad@sao.wa.gov

Joseph Clark
Performance Auditor
(360) 725-5572
Joseph.Clark@sao.wa.gov

Websites: www.sao.wa.gov https://auditconnectionwa.org/
Facebook: https://www.facebook.com/WAStateAuditorsOffice
Twitter: www.twitter.com/WAStateAuditor