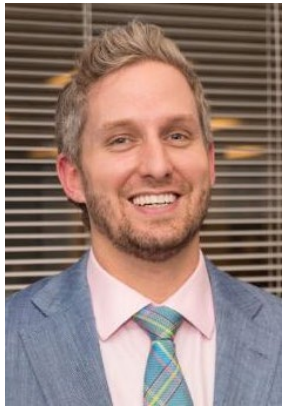
Panel 7: Privacy and Data Security for Law Firms and Legal Support Organizations

The 13th Annual Sedona Conference Institute:
Protecting Privacy, Confidentiality, and Privilege in Civil Litigation
March 7–8, 2019
The Ballantyne Hotel & Lodge, Charlotte, NC

Dialogue Leaders

- Mark S. Hegedus
  - Federal Trade Commission, Washington, DC
- Peter Pepiton
  - Dinsmore & Shohl LLP, Cincinnati, OH
- Geoffrey A . Vance
  - Perkins Coie LLP, Chicago, IL & Shanghai, PRC
- Matthew F. Knouff
  - Greater New York City Area & London, UK



Required and Supplemental Reading

- The Sedona Conference, Commentary on Privacy and Information Security (November 2015)
- The Sedona Conference, Data Privacy Primer (January 2018)
- The Sedona Conference, Incident Response Guide, Public Comment Version (March 2018)
- Perkins Coie, Security Breach Notification Chart (June 2018)
- Geoffrey Vance, When Redactions Don't Redact (January 2019)
- National Security Agency, Redaction of PDF Files Using Adobe Acrobat Professional X
- Kenneth J. Withers, ed., Selected North Carolina Rules of Professional Conduct
- Links to official versions of the General Data Protection Regulation and California Consumer Privacy Act
- American Bar Association, Selected Model Rules of Professional Conduct
- Federal Trade Commission, Data Breach Incident Response: A Guide for Business
- Federal Trade Commission, Protecting Personal Information: A Guide for Business

China-Backed Hackers Targeted US Law Firm: Security Co.

By **Ben Kochman**

Law360 (February 6, 2019, 7:22 PM EST) -- An American law firm specializing in intellectual property was among the businesses targeted by Chinese intelligence-backed hackers in a sustained cyber espionage campaign carried out over nearly a year, security researchers warned Wednesday.

Chinese hackers targeted an American law firm specializing in intellectual property, a cybersecurity company says. Above, Chinese and American flags fly in Beijing. (AP)

The attackers gained access to the firm, which has clients in the pharmaceutical, technology, electronics, biomedical and automotive sectors, as part of a bid to "steal valuable intellectual property or gain commercial advantage" from businesses between November 2017 and September 2018, cybersecurity company Recorded Future wrote in a blog post.

The company did not name the law firm that was attacked, but noted that it has a "dedicated China practice aimed at assisting Chinese companies entering the U.S. market." Attackers used stolen user credentials "possibly gained via a third-party supply chain compromise" to gain access to the firm's network in late 2017, before installing malware that allowed them to obtain user passwords, the researchers said.

Members of the so-called Advanced Persistent Threat 10 group, or APT10, also targeted an international apparel company and Norwegian software company Visma, which provides information technology and cloud computing services, according to the blog post. The hacking group, which the U.S. government has accused of taking orders from the Chinese government, is behind a series of recent intrusions into American businesses, U.S. federal authorities said in a December **indictment**.

In that case, court papers charge two accused hackers with stealing sensitive data from 45 technology companies in the U.S. and globally, as well as several managed service providers. Two months earlier, authorities charged two Chinese intelligence officers and eight others purportedly working under their direction with a **hacking campaign** targeting American and European intellectual property related to aerospace technology.

Ex-federal officials have told Law360 that such "name-and shame" indictments, which may or may not lead to the alleged hackers ever appearing in a U.S. courtroom, will only be successful as part of a **broader strategy** that describes what makes a cyberattack unacceptable and punishes nations that violate established norms.

Whereas the law firm attack is believed to be aimed at stealing intellectual property, the attack into service provider Visma is part of a broader campaign from China's Ministry of State Security to infiltrate such providers, Recorded Future said. Dubbed "Operation Cloud Hopper," the campaign could put "hundreds, if not thousands" of global corporations that store data with managed service providers at risk if it is successful, the researchers say.

The sensitive information that law firms hold has made them prime targets for hackers in recent years. The most recent episode came in January, when a hacking group calling itself "The Dark Overlord" released a cache of **confidential files** it says it stole from a law firm involved in litigation stemming from the 9/11 attacks, and offered more sensitive documents to the highest bidder.

--Additional reporting by Stewart Bishop. Editing by Connor Relyea.

Privacy & Security for Law Firms and LSOs

- Ethical obligations
- External threats
- Internal threats
- Best practices
- Training and guidance

ABA Model Rules

- Rule 1.1: Competence
  - Benefits and risks of relevant technology
- Rule 1.4: Client communication
  - Reasonably consult with client about technology
- Rule 1.6(c): Client confidences
  - Reasonable efforts to prevent inadvertent or unauthorized disclosure or unauthorized access

ABA Model Rules (continued)

- Rule 4.4(b): Inadvertent production
  - Obligation to inform
- Rules 5.1, 5.2 & 5.3: Supervision of subordinates
  - Conduct of lawyers and non-lawyers must be compatible with ethical obligations
- Formal Opinion 483: Post-breach obligations
  - Reasonable efforts to prevent, detect, stop, and notify

Privacy & Security for Law Firms and LSOs

- Ethical obligations
- External threats
- Internal threats
- Best practices
- Training and guidance

External Threats

- Hacking
- Ransomware/Malware
- Socially engineered attacks
- Mobile apps
- Phishing

External Threats

The Legal Intelligencer
POWERED BY LAW.COM

'Spear-Phishing' Is a Growing Cyberthreat to Law Firms—and Expensive Tech Can't Stop It

A three-lawyer shop in suburban Philadelphia and the largest law firm in the world have both fallen victim to it, multimillion-dollar cybersecurity technology can do little to guard against it, and once the damage is done it's all but irreversible. "Spear-phishing" is a growing concern for law firms of all sizes.

By **Zack Needles** | February 25, 2019 at 03:58 PM

Privacy & Security for Law Firms and LSOs

-
-
- Internal threats
-
-

Internal Threats

Infosec: Your password needs to be at least 15 characters, including at least one each of Capital letter, lowercase letter, number, a special character, and a character not found on the keyboard.

And don't write it down.

And change it every 90 days.

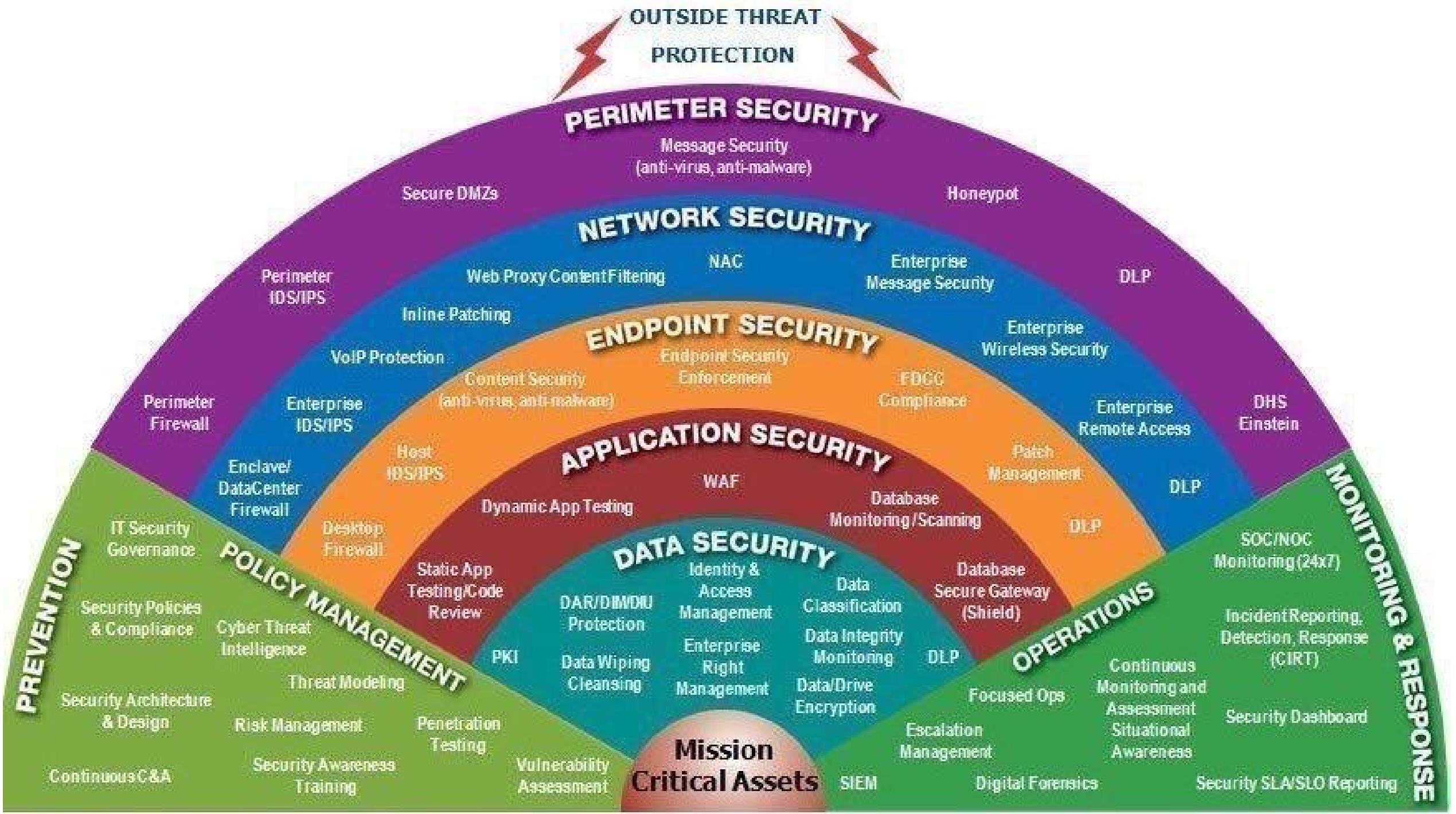
Me:

Internal Threats

Internal Threats

Defense in Depth

aka - Kerplunk


OUTSIDE THREAT
PROTECTION
PERIMETER SECURITY
Message Security
(anti-virus, anti-malware)
Secure DMZs
Honeypot
NETWORK SECURITY
Perimeter
IDS/IPS
Web Proxy Content Filtering
NAC
Enterprise
Message Security
DLP
Inline Patching
ENDPOINT SECURITY
Enterprise
Wireless Security
VoIP Protection
Endpoint Security
Enforcement
Content Security
(anti-virus, anti-malware)
FDCC
Compliance
Perimeter
Firewall
Enterprise
IDS/IPS
Enterprise
Remote Access
DHS
Einstein
Host
IDS/IPS
APPLICATION SECURITY
Patch
Management
Enclave/
DataCenter
Firewall
WAF
DLP
Dynamic App Testing
Database
Monitoring/Scanning
Desktop
Firewall
DLP
DATA SECURITY
Static App
Testing/Code
Review
Identity &
Access
Management
Data
Classification
Database
Secure Gateway
(Shield)
DAR/DIM/DIU
Protection
Data Integrity
Monitoring
PKI
Data Wiping
Cleansing
Enterprise
Right
Management
DLP
Data/Drive
Encryption
PREVENTION
IT Security
Governance
POLICY MANAGEMENT
OPERATIONS
SOC/NOC
Monitoring (24x7)
MONITORING & RESPONSE
Security Policies
& Compliance
Cyber Threat
Intelligence
Incident Reporting,
Detection, Response
(CIRT)
Threat Modeling
Continuous
Monitoring and
Assessment
Situational
Awareness
Security Architecture
& Design
Focused Ops
Security Dashboard
Risk Management
Penetration
Testing
Escalation
Management
Security Awareness
Training
Vulnerability
Assessment
Mission
Critical Assets
Continuous C&A
SIEM
Digital Forensics
Security SLA/SLO Reporting

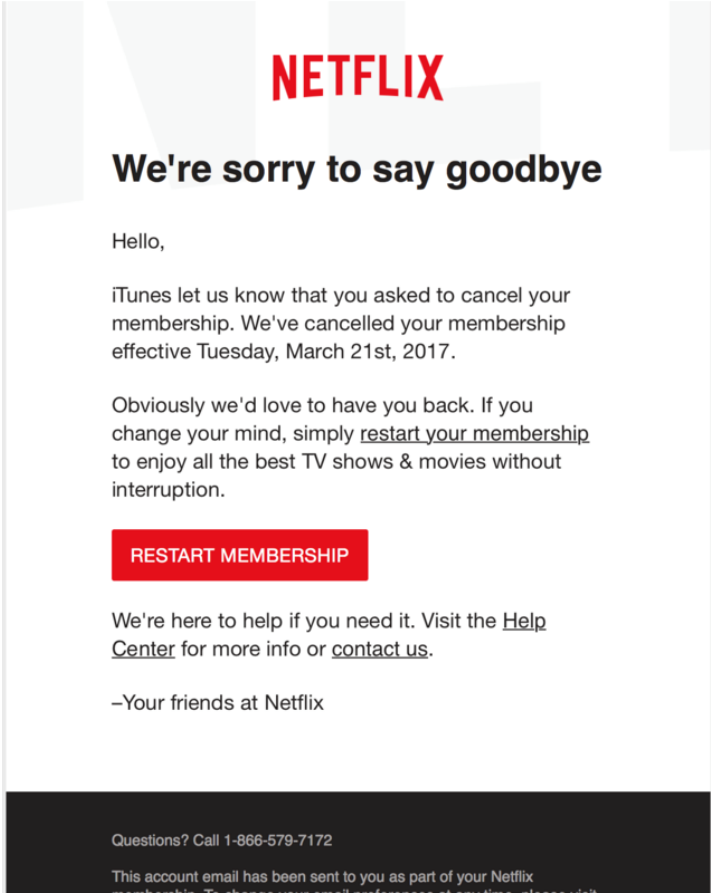
Internal Threats – Defense in Depth

- Perimeter (Firewall, etc)
- Physical Security (access control)
- Network (encryption, for one)
- Access Control (Passwords, for example)
- Monitoring/Incident Response (Logs)
- Security Strategy (Policies, staffing, etc.)
- Data Protection (tools, data classification)
- Risk Management (risk register, vulnerability management)
- Training & Education

More Phishing Examples

- The Urgent Request
- Unexpected Money
- Information-Based Emails

Phishing Redux – The Urgent Request



NETFLIX

We're sorry to say goodbye

Hello,

iTunes let us know that you asked to cancel your membership. We've cancelled your membership effective Tuesday, March 21st, 2017.

Obviously we'd love to have you back. If you change your mind, simply restart your membership to enjoy all the best TV shows & movies without interruption.

RESTART MEMBERSHIP

We're here to help if you need it. Visit the Help Center for more info or contact us.

–Your friends at Netflix

Questions? Call 1-866-579-7172

This account email has been sent to you as part of your Netflix

Subject: Record Update.
From: "Dept. Of Labor" <records@dol.gov>
Date: 1/18/2016 1:57 PM
To: undisclosed-recipients:;

This is an urgent request to update your employment record at the U.S Department of Labor.

Update

Thank you

U.S Dept. of Labor
Frances Perkins Building,
200 Constitution Ave., NW,
Washington, DC 20210

Phishing Redux – The Urgent Request

You forwarded this message on 4/14/2008 8:21 AM.

From: United States District Court [subpoena@uscourts.com]
To: Steve Kirsch
Cc:
Subject: Subpoena in case #28-755-YCH

AO 88(Rev.11/94) Subpoena in a Civil Case

Issued by the
UNITED STATES DISTRICT COURT

Issued to: Steve Kirsch
Propel Software Corporation
408-571-6300

SUBPOENA IN A CIVIL CASE

Case number: 28-755-YCH
United States District Court

YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specifiied below.

Place: United States Courthouse
880 Front Street
San Diego, California 92101

Date and Time: May 7,2008
9:00 a.m. PST

Room: Grand Jury Room

Hi <customer>,

This is a follow-up regarding your package delivery:

- Tracking Number: 0p2uYq5RIho

The package contained in the above-mentioned shipment was not accepted at the destination address. Please contact your local UPS office and provide the printed delivery sticker, included in this email.

Please note that in case of a failure to contact your local UPS office within 21 days the parcel will be returned to sender.

Thanks so much for shipping with UPS.

Get the UPS My Choice app for Facebook

Download the UPS mobile app

Phishing Redux – The Urgent Request

WELLS FARGO

wellsfargo.com

Because of unusual number of invalid login attempts on you account, we had to believe that, their might be some security problem on you account.

So we have decided to put an extra verification process to ensure your identity and your account security.

Please click on continue to the verification process and ensure your account security. It is all about your security.

LOGIN

Confirm that you're the owner of the account, and then follow the instructions.

Confirm all information, and then access your account as normal.

Thank you.

IMPORTANT INFORMATION
(If you cannot click on the link, please move the message into the Inbox).

Terms of use | Security| Privacy

Exclusively for: | VALUED CUSTOMER
Online Banking

Bank of America

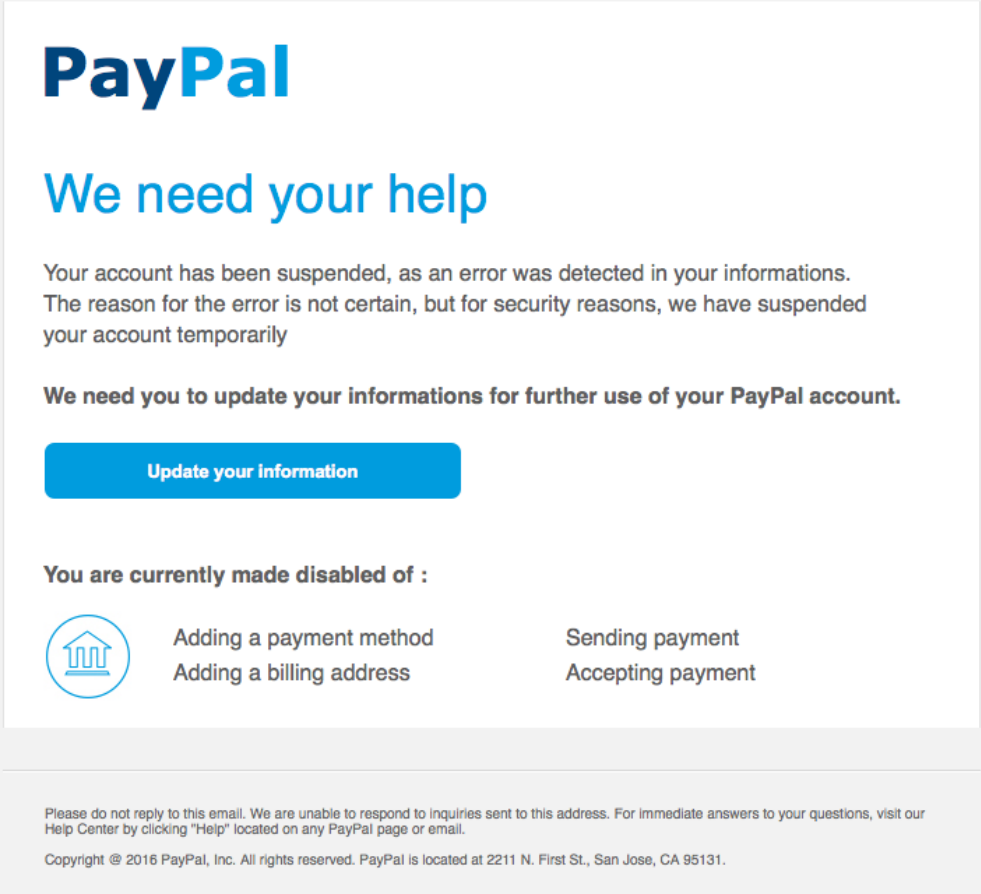
Your Bank of America accounts has been locked!

There are a number of invalid login attempts on your account. We had to believe that, there might be some security problems on your account. So we have decided to put an extra verification process to ensure your identity and your account security.

Please click here to continue the verification process and ensure your account security.

Email Preferences
This is a service email from Bank of America. Please note that you may receive service email in accordance with your

Phishing Redux – The Urgent Request



PayPal

We need your help

Your account has been suspended, as an error was detected in your informations. The reason for the error is not certain, but for security reasons, we have suspended your account temporarily

We need you to update your informations for further use of your PayPal account.

Update your information

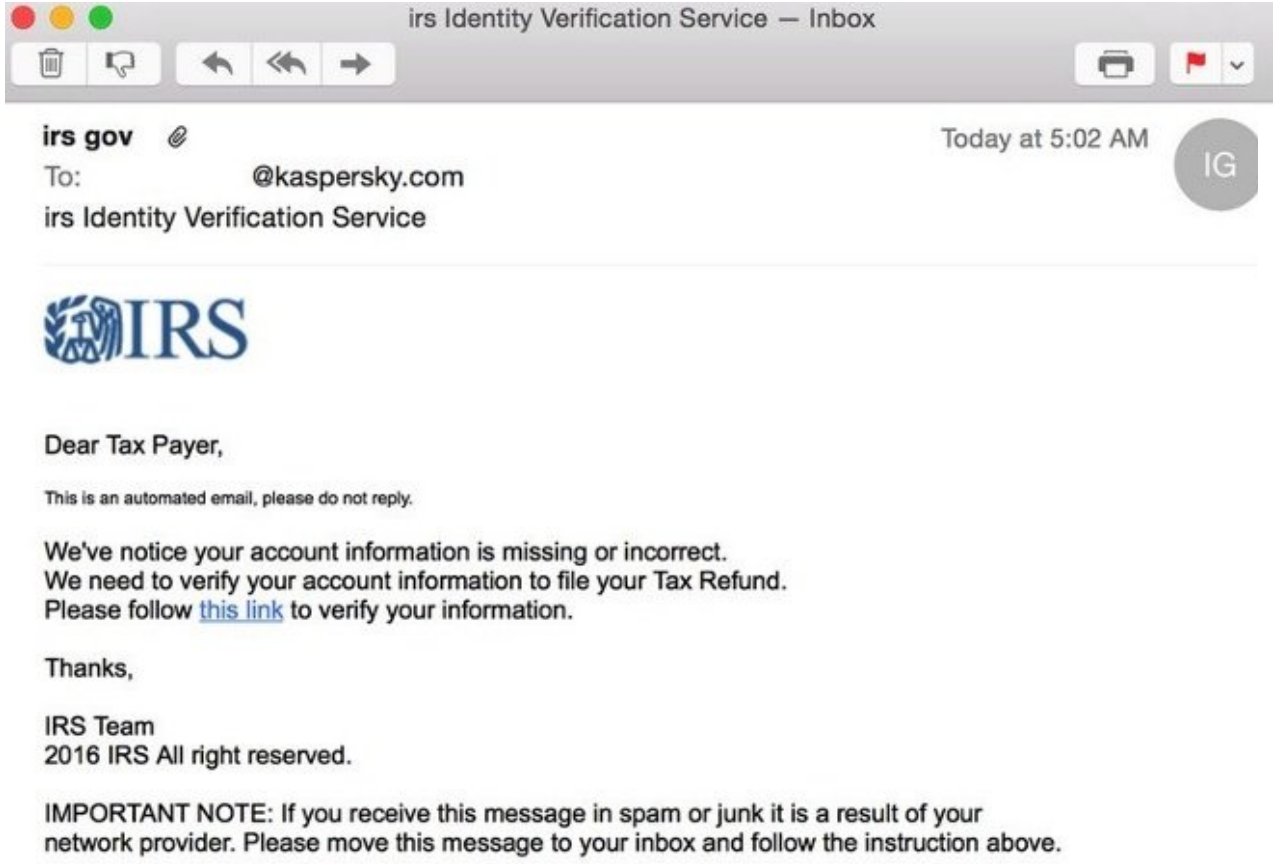
You are currently made disabled of :

Adding a payment method
Adding a billing address
Sending payment
Accepting payment

Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help Center by clicking "Help" located on any PayPal page or email.

Copyright @ 2016 PayPal, Inc. All rights reserved. PayPal is located at 2211 N. First St., San Jose, CA 95131.

Phishing Redux – Unexpected Money



irs Identity Verification Service — Inbox

irs gov
To: @kaspersky.com
irs Identity Verification Service

Today at 5:02 AM

IG

IRS

Dear Tax Payer,

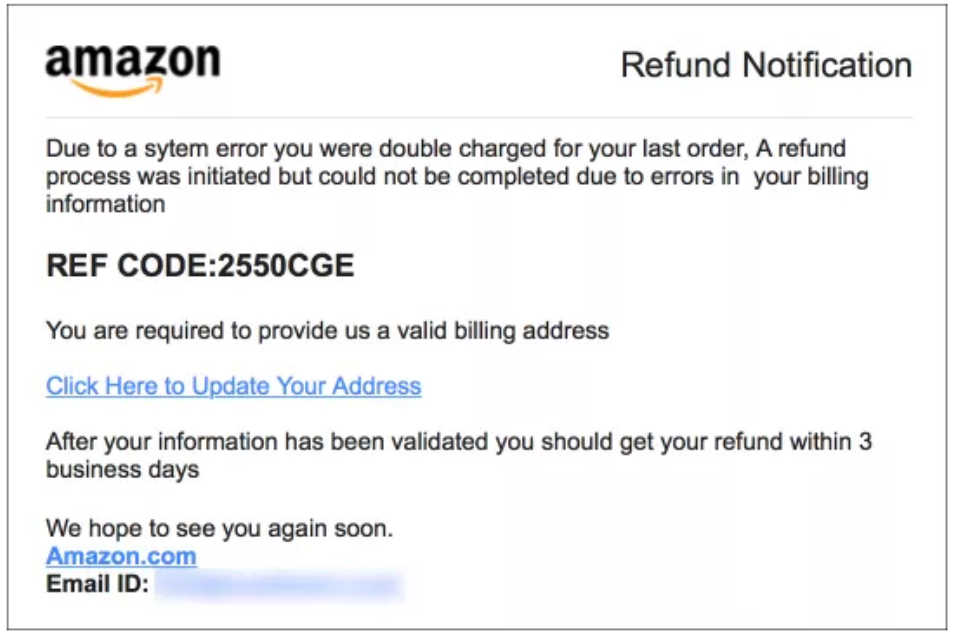
This is an automated email, please do not reply.

We've notice your account information is missing or incorrect.
We need to verify your account information to file your Tax Refund.
Please follow this link to verify your information.

Thanks,

IRS Team
2016 IRS All right reserved.

IMPORTANT NOTE: If you receive this message in spam or junk it is a result of your network provider. Please move this message to your inbox and follow the instruction above.



amazon

Refund Notification

Due to a sytem error you were double charged for your last order, A refund process was initiated but could not be completed due to errors in your billing information

REF CODE:2550CGE

You are required to provide us a valid billing address

Click Here to Update Your Address

After your information has been validated you should get your refund within 3 business days

We hope to see you again soon.
Amazon.com
Email ID:

Phishing Redux – Unexpected Money

Your New Salary Notice
SLU HR [resources_employee_HR@slu.edu]

Sent: Saturday, January 23, 2016 8:03 AM
To:

SAINT LOUIS UNIVERSITY
Higher purpose. Greater good.™

Hello,

After assessing the 2015 SLU salary structure as provided under the terms of employment it was discovered that you are due for a 12.64% salary raise starting January 2016.

Your salary raise documents are enclosed below:

Access the documents here

Ensure all details are entered correctly to avoid cancellation

Human Resources & Benefits

Saint Louis University

Phishing Redux – Information-Based Emails

---------- Forwarded message ----------
From: **Doug Williams** <chrispid@t-online.de>
Date: Wed, Apr 13, 2016 at 11:47 AM
Subject: Invoice for Lehigh University ; Attention: Controller
To: j

This is a private message for the Controller, Lehigh University. If it is not you, please ignore and discard it.

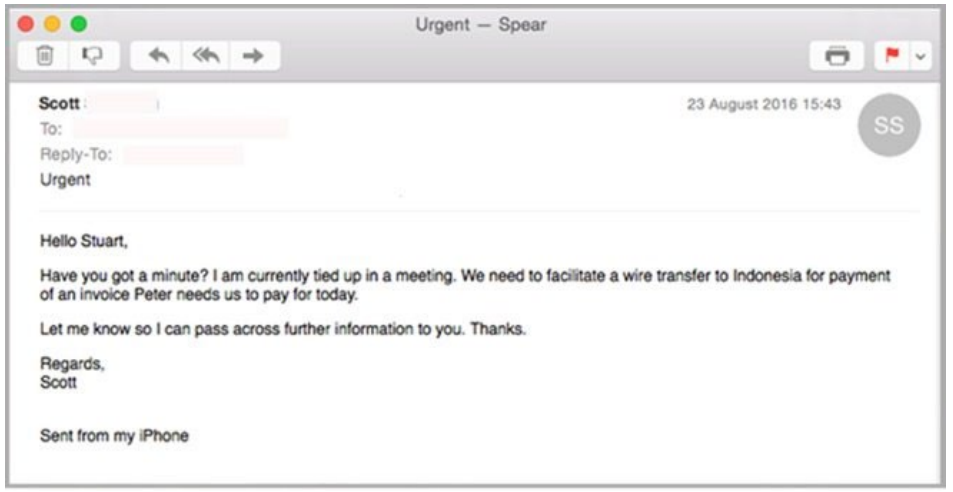
Hi John Gasdaska,

Since we have not received a contract termination letter, I am assuming that you might have unintentionally overlooked our invoice **04/16000331799** (Unpaid). If you intend to bring to an end the account, just let us know. Be informed that early withdrawal penalties will apply.

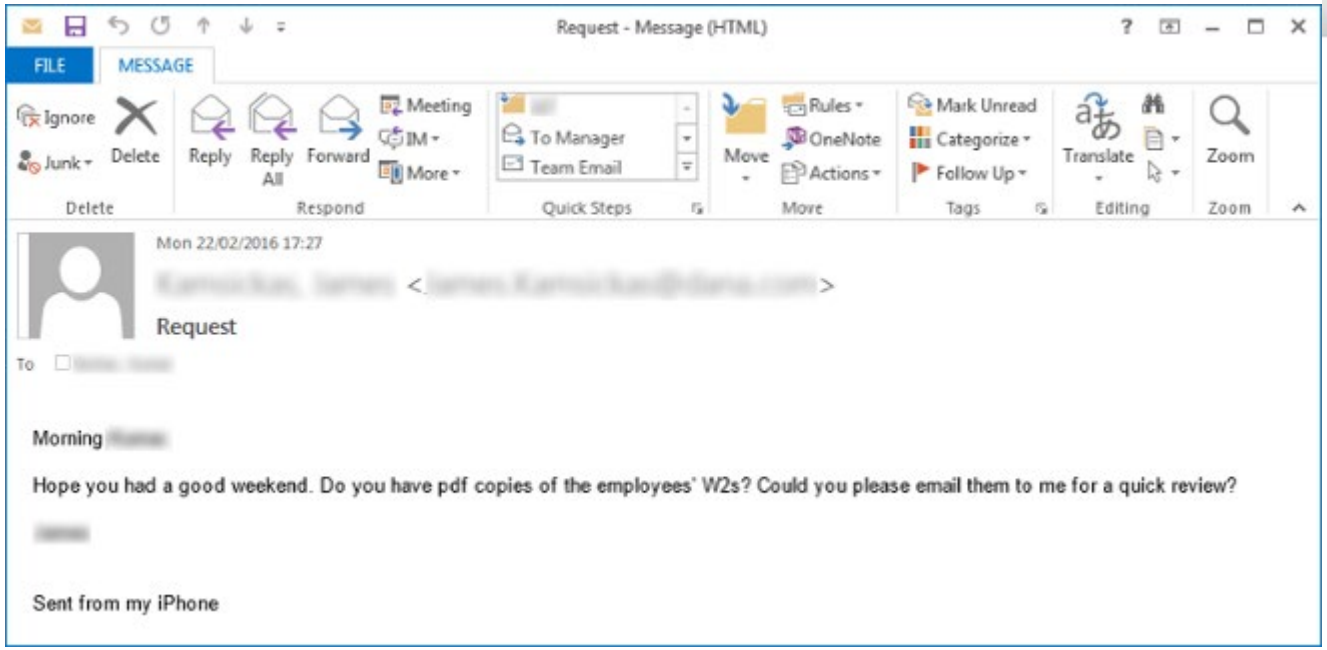
Refer to the attached document for billing information.

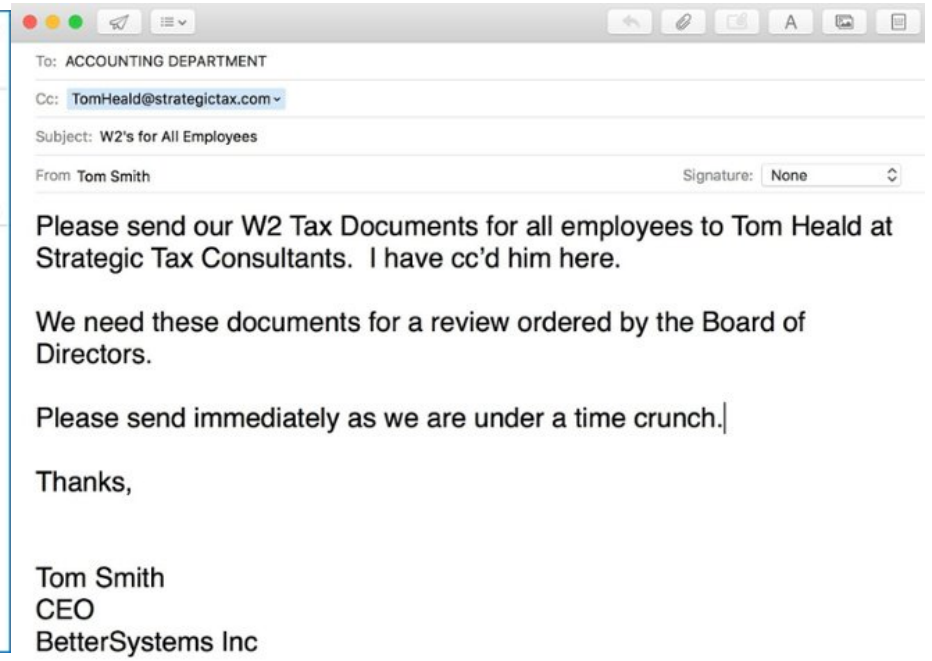
Regards,
Doug.

Doug Williams
Sterling Savings Bank | Accounting and Billing Team
6400 Uptown Blvd Ne,Albuquerque,New Mexico,87110
T: 866-905-9901 | Copyright © 2016



Phishing Redux – Information-Based Emails





Privacy & Security for Law Firms and LSOs

- Ethical obligations
- External threats
- Internal threats
- **Best practices**
- Training and guidance

Best Practices

- Password hygiene:
  - Vaults
  - Two-step verification
- Systems patches
- Content and domain filtering
- Cloud sensitivity

Privacy & Security for Law Firms and LSOs

- Ethical obligations
- External threats
- Internal threats
- Best practices
- Training and guidance

Training and Guidance

- New attorney/employee orientation
- Training emails
- Test phishing emails
- Firmwide webinars
- Retreats and summits
- Promotions
- Computer upgrades

Questions and comments?