

Think Before You Click!

Cybersecurity Awareness for Lawyers and Law Firms

Bankruptcy & Commercial Law Section
Dallas Bar Association
April 5, 2017

Presented by Steve Thomas



STEVE
MARTIN

MICHAEL
CAINE

DIRTY ROTTEN SCOUNDRELS



“Con Artist”

One who tries to swindle the victim
by first gaining his confidence.

The goal is
VOLUNTARY ACTION
by the victim.

A FRANK OZ FILM STEVE MARTIN MICHAEL CAINE

“DIRTY ROTTEN SCOUNDRELS”

Starring GLENNE HEADLY with ANTON RODGERS and BARBARA HARRIS. Music by MILES GOODMAN

Edited by STEPHEN A. ROTTER and WILLIAM SCHARF. Production Designed by ROY WALKER. Director of Photography MICHAEL BALLHAUS, A.S.C.

Executive Producers DALE LAUNER and CHARLES HIRSCHHORN. Written by DALE LAUNER and STANLEY SHAPIRO & PAUL HENNING

Produced by BERNARD WILLIAMS. Directed by FRANK OZ

PG PARENTAL GUIDANCE SUGGESTED. Some material may not be suitable for children. © 1988 Orion Pictures Corporation. All Rights Reserved. An ORION PICTURES Release

“Phishing”

ELECTRONIC CON GAME

Criminals use

SOCIAL ENGINEERING

To gain your trust and convince you to

ACT before you THINK

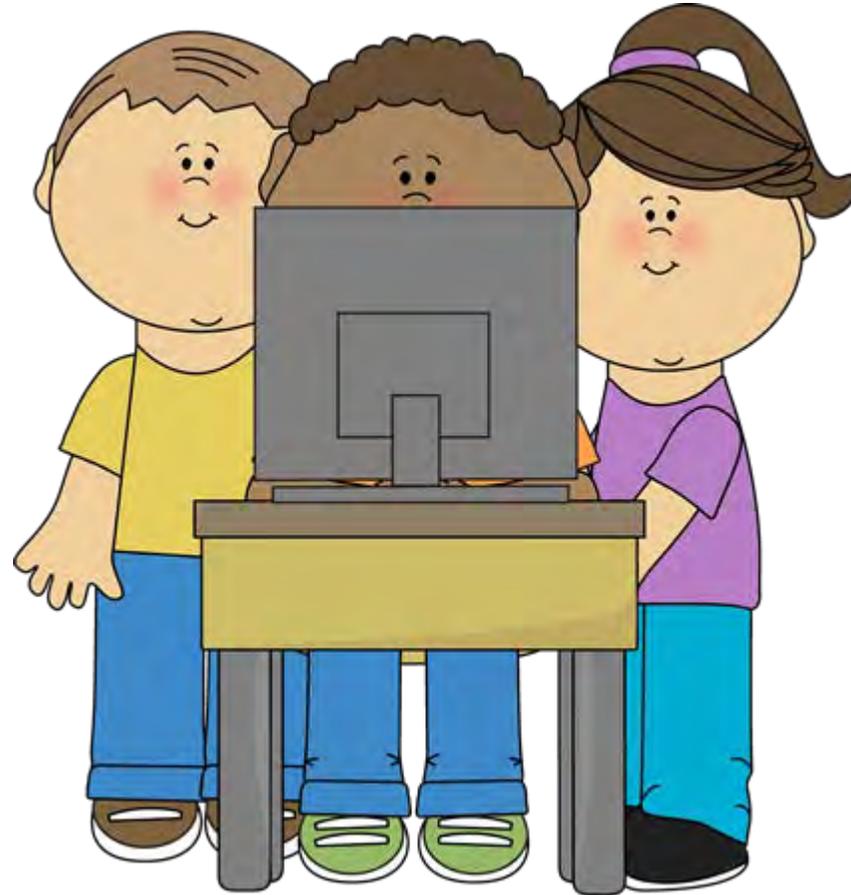
Training helps you

SPOT the con before you ACT



But why
would a
criminal
want access
to my
computer?

There's nothing on it
worth anything.



Ransomware

Access to corporate network

Information about your contacts

Credit card or log in information

Client information

Banking information

Use your computer as a bot

To cybercriminals,
any working computer
located in the United States
that is connected to the internet
possibly has value.

Tactics, techniques and procedures of financial attacks attributed to the Lazarus group

Lazarus is widely considered to be the group behind multiple, devastating cyberattacks including the \$81 million heist of Central Bank of Bangladesh, at the beginning of 2016, and several other attacks against banks worldwide. While conducting their operations, hackers follow a set of tactics, techniques and procedures which allow them to quietly penetrate targeted systems and gain access to critical ones.



Step 1

Compromise of a webserver



1. The compromised server is used as an entry point to the company

OR



1. A government website is hacked through a known vulnerability

2. The exploit is placed on the hacked website with a whitelist of targets to serve the exploit to
3. The target visits a government website and becomes infected

Step 2



2. The attacker migrates system into the company and gains access



3. Additional lateral movement tools are installed – some for privilege escalation purposes

Less than
10 Percent
Of all attacks are
Targeted!

Step 4

Identify including:



1. Custom malware is deployed, that disables internal security checks of the SWIFT software



2. SWIFT message filtering malware is integrated to hide rogue messages created by the attackers



IT administrators' systems

backup servers

3. Money theft starts



While investigating Lazarus' financial attacks, Kaspersky Lab researchers were able to identify 150+ different malware samples related to recent group's activity.

Kaspersky Lab products successfully detect and block all known malware used by the Lazarus group.



What is Phishing?

The attempt to acquire sensitive information or control over valuable resources by masquerading as a trustworthy person or entity in an electronic communication.

What is Phishing?

Let's break that down:

The attempt to acquire sensitive information

Credit card information

Bank account information

User names and passwords for online accounts

Contact information

What is Phishing?

Let's break that down:

or control over valuable resources

A computer connected to the internet

Network servers or other components

Infrastructure systems such as power grids

Your data

What is Phishing?

Let's break that down:

by masquerading as a trustworthy person or entity

A company you know

A friend, client, colleague, or co-worker

The government

A website you trust (spoofs or exploit kits)

What is Phishing?

Let's break that down:

in an electronic communication

Email

Text Messages

Visiting a website (exploit kits)



How does Phishing work?

You have to take an action:

Click on a link in an email or text message

Open an attachment to an email or a text message

Click on a component of a webpage (picture, link, graphic, etc.)

Reply to an email

Make a phone call

But if it looked dangerous or risky, you wouldn't act. That's why the criminals use . . .

SOCIAL ENGINEERING

Deceptive tactics designed to make it look safe to act



Email comes from someone you know or trust

The attachment appears innocuous (Word, Excel, PDF)

The website is a well-known one.

What happens when I click?

An executable program or script runs on your computer.
The program might:

Lock down your computer (Ransomware)

Capture information (e.g., Man In The Browser – Girl with the Dragon Tattoo)

Provide access (e.g., Nymaim)

Redirection Attacks (e.g., Gozi)

Anything software can do, malware can do, because malware is just software designed for malicious purposes.



EXAMPLES

And what to look for



From: Stephanie D. Curtis [<mailto:scurtis@curtislaw.net>]

Sent: Wednesday, March 01, 2017 1:41 PM

Subject: Please Review & Act on These Documents.

Hi,

YOU HAVE A DOCUSIGN REQUEST. KINDLY [CLICK HERE](#) TO VIEW IT.

THANKS

Stephanie D. Curtis

Curtis | Castillo PC

901 Main Street, Suite 6515,

Dallas, TX 75202

T: 214.752.2222 | F: 214.752.0709

C: 214.460.2461

E: scurtis@curtislaw.net

W: www.curtislaw.net

From: Stephanie D. Curtis [<mailto:scurtis@curtislaw.net>]

Sent: Wednesday, March 01, 2017 1:41 PM

Subject: Please Review & Act on These Documents.

Hi,

<http://woodmaster.com.np/config/font>

Click or tap to follow link.

YOU HAVE A DOCUSIGN REQUEST. KINDLY [CLICK HERE](#) TO VIEW IT.

THANKS

Stephanie D. Curtis

Curtis | Castillo PC

901 Main Street, Suite 6515,

Dallas, TX 75202

T: 214.752.2222 | F: 214.752.0709

C: 214.460.2461

E: scurtis@curtislaw.net

W: www.curtislaw.net

Country Code Top Level
Domain (ccTLD) for NEPAL

From: Debbi Graham [<mailto:orders@quarrytitle.com>]
Sent: Tuesday, January 31, 2017 1:47 PM
To: Cullen Aderhold
Subject: Debbi Graham Title Commitment S1235948

Sharefile Attachments

Expires February 15, 2017

[S1235948 Title Commitment sw.pdf](#)

440.6 KB

Download Attachments

Debbie Graham uses ShareFile to share documents securely. [Learn More.](#)

Debbi Graham

Closing Assistant

Quarry Title & Closing, LLC

Company State License No. 40118391

****Please forward new title/closing orders to orders@quarrytitle.com.****

Check out our user friendly website. Rate Calculator-GFE Quotes 24/7 and place your order on line!!! www.quarrytitle.com

3312 3rd Street North

St. Cloud, MN 56303

(320) 654-0151 Main Line

(320) 654-0022 Fax Line

Agent for Old Republic National Title

Real Main Line (320) 654-0050

Real Fax Line (320) 654-0060

This e-mail transmission and any attachments accompanying it may contain confidential and/or proprietary information and is intended only for the person or entity to whom it was originally addressed. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or other use of this information is strictly prohibited. Any unauthorized interception of this transmission is illegal. If you have received this transmission in error, please notify the sender by reply e-mail, and then destroy all copies of this transmission.

From: Debbi Graham [<mailto:orders@quarrytitle.com>]
Sent: Tuesday, January 31, 2017 1:47 PM
To: Cullen Aderhold
Subject: Debbi Graham Title Commitment S1235948

Sharefile Attachments http://www.expedeon.com/microsoft/index.php January 15, 2017
Click or tap to follow link.

[S1235948 Title Commitment sw.pdf](#) 440.6 KB

[Download Attachments](#)

Debbie Graham uses ShareFile to share documents securely. [Learn More.](#)

Debbi Graham
Closing Assistant
Quarry Title & Closing, LLC
Company State License No. 40118391
****Please forward new title/closing orders to orders@quarrytitle.com****
Check out our user friendly website. Rate Calculator-GFE Quotes 24/7 and place your order on line!!! www.quarrytitle.com
3312 3rd Street North
St. Cloud, MN 56303
(320) 654-0151 Main Line
(320) 654-0022 Fax Line
Agent for Old Republic National Title

This e-mail transmission and any attachments accompanying it may contain confidential and/or proprietary information and is intended only for the person or entity to whom it was originally addressed. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or other use of this information is strictly prohibited. Any unauthorized interception of this transmission is illegal. If you have received this transmission in error, please notify the sender by reply e-mail, and then destroy all copies of this transmission.

From: Amazon.com <ship-confirm@amazon-delivery.com>

Sent: Mon 3/27/2017 1:58 PM

To: Steve Thomas

Cc:

Subject: Your Amazon.com order has shipped (#174-48775361-2760285228)



Hello,

Your order "Apple iPhone 7 AT&T 256 GB (Rose Gold) Neverlocked" has shipped. Below you can find the shipping details and the invoice.

Details

Order #174-48775361-2760285228

Expected delivery date:

March 27, 2017

Total including shipping:

\$869.99

[Order details](#)

Depending on the shipping option you have chosen, it may take 24 hours for tracking information to be available in your account.

We hope to see you again soon.

Amazon.com

This email was sent from a notification-only address that cannot accept incoming email. Please do not reply to this message.



Amazon.com





Amazon.com <ship-confirm@amazon-delivery.com>

Steve Thomas

Mon 1:58 PM

Your Amazon.com order has shipped (#174-48775361-2760285228)



Hello,

Your order "Apple iPhone 7 AT&T 256 GB (Rose Gold) Neverlocked" has shipped. Below you can find the shipping details and the invoice.

Details

Order #174-48775361-2760285228

Expected delivery date:

March 27, 2017

<http://www.bluedot.co.za/l5afva/getnum.php?id=ody0nnn0ag9tyxnabwnzbgf3lmmvbt3nji=>

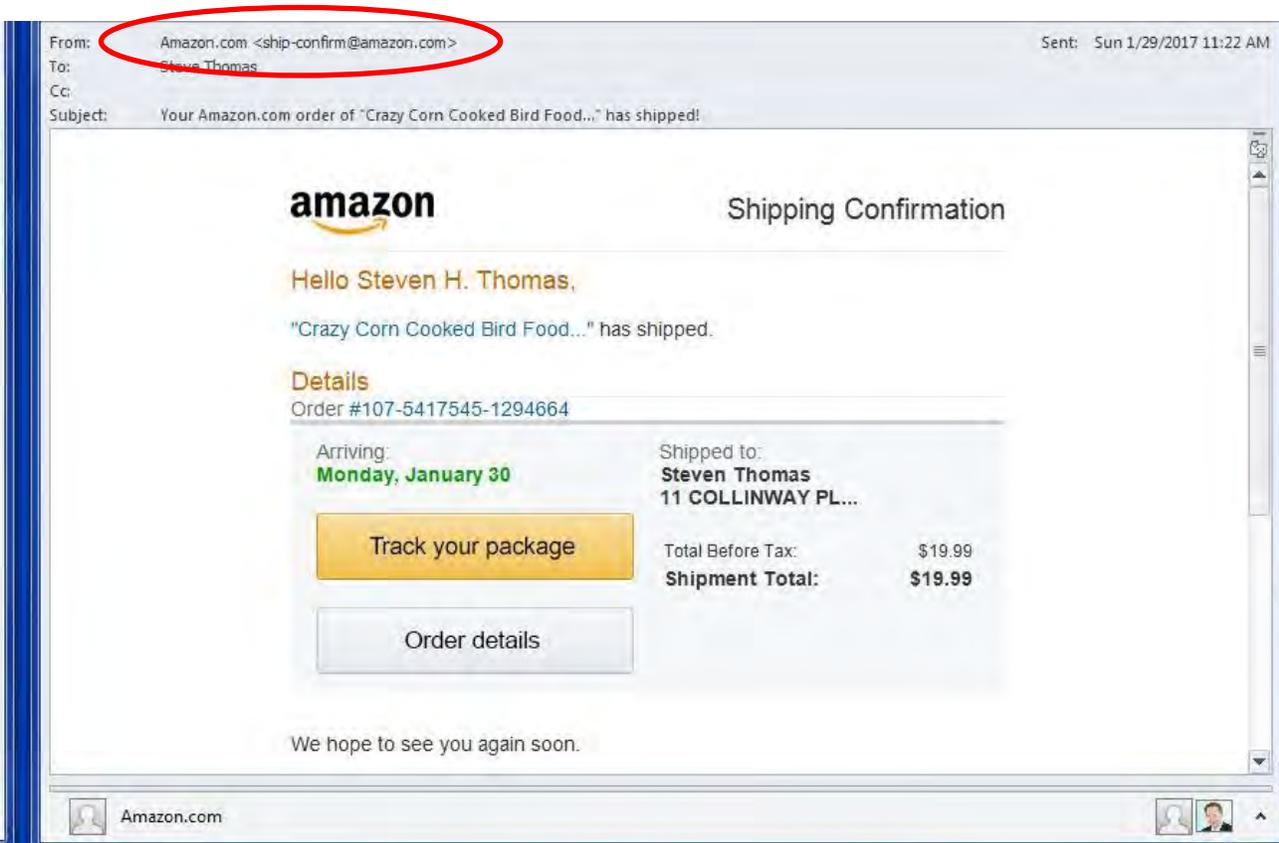
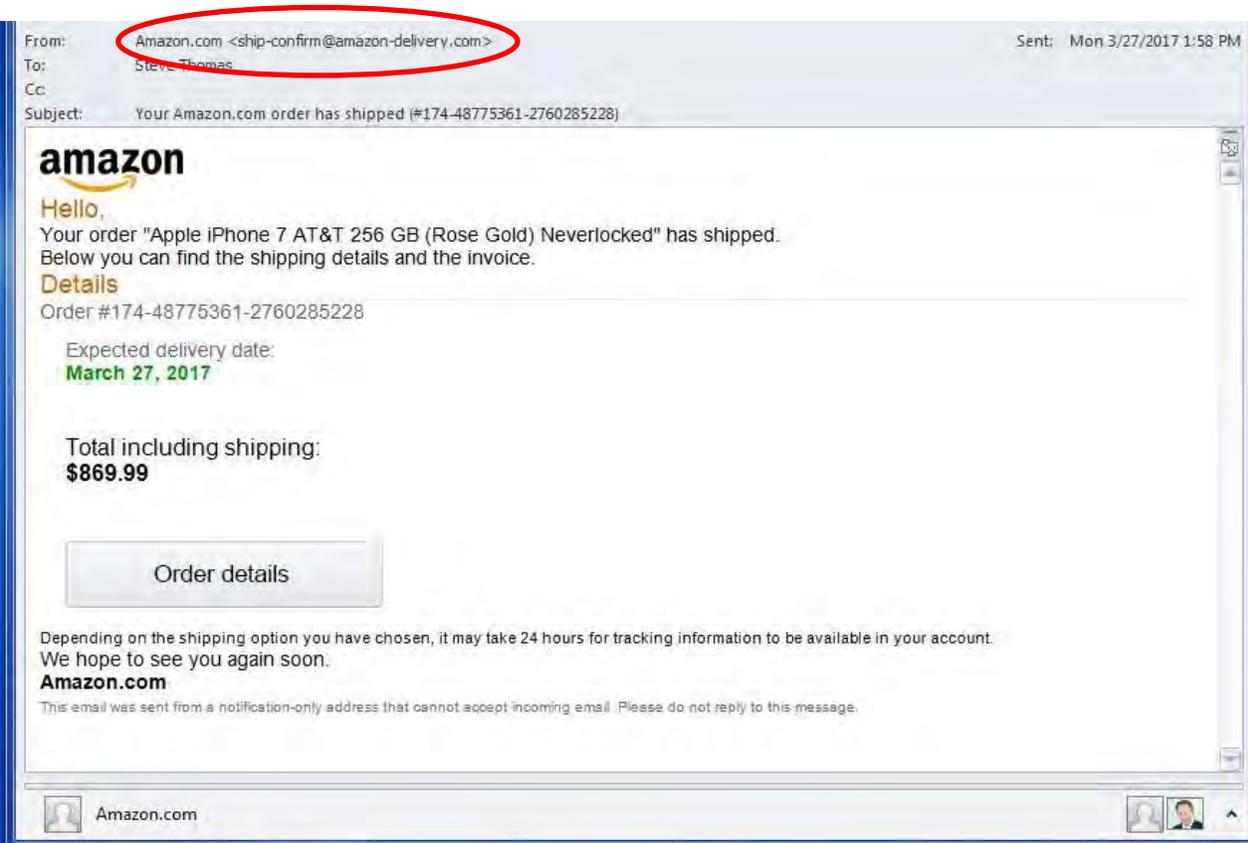
Click or tap to follow link.

Order details

ccTLD for SOUTH AFRICA

FAKE

REAL





RingCentral <ringcentral@messaging.com>

Steve Thomas

3/13/17

Incoming Fax from 725-630-6056



RingCentral[®]

phone systems reimagined

You Have 1 unread Fax message
From: 725-630-6056
Incoming date: March 13, 2017

You can view your fax online, on the RingCentral website:
https://messaging.ringcentral.com/fax/view.aspx?fax_id=5807244&name=sthomas

Please note that Microsoft Word must be installed on your PC.

Thank you for choosing RingCentral



RingCentral <ringcentral@messaging.com>

Steve Thomas

3/13/17

Incoming Fax from 725-630-6056



RingCentral[®]

phone systems reimagined

You Have 1 unread Fax message
From: 725-630-6056
Incoming date: March 13, 2017

You can view your fax online, on the RingCentral website:

https://messaging.ringcentral.com/fax/view.aspx?fax_id=5807244&name=sthomas

Please note that Microsoft Word must be installed on your PC.

Thank you for choosing RingCentral

ccTLD for JAPAN

<http://taiwa-p.co.jp/api/getn.php?id=c3rob21hc0bty3nsyxcuy29t>
Click or tap to follow link.

ccTLD for ARGENTINA

From: ADP Portal [<mailto:hminotti@medios.gov.ar>]

Sent: Friday, February 24, 2017 8:41 AM

Subject: Update Required

The Human Resources/Payroll Department has completed the final pay-stub changes for 2017 tax year.

To view the changes to your pay-stub information and [view/download](#) your W-2 forms (2014 - 2016 tax years)

We hope you find the changes to your pay-stub information useful and welcome any comments you may have.

ccTLD for CHILE

From: ADP Portal [<mailto:hminotti@medios.gov.ar>]

Sent: Friday, February 24, 2017 8:41 AM

Subject: Update Required

The Human Resources/Payroll Department has completed

2017 tax year.

To view the changes to your pay-stub information and [view/download](#) your W-2 forms (2014 - 2016 tax years)

We hope you find the changes to your pay-stub information useful and welcome any comments you may have.

<http://www.masrecursos.cl/adppta/index.htm>

Click or tap to follow link.

From: Mrs Patricia Knight [<mailto:patricia.knight@cheerful.com>]
Sent: Friday, June 17, 2016 2:09 PM
Subject: RE: BEACONSFIELD MINE COLLAPSE FROM MRS PATRICIA KNIGHT

Greeting From Yemen,

The internet has been grossly abused by scam artist and miscreants whose intention is to hurt. In as much as one should be careful, same time we should not allow negativity to kill the positive potential in a realistic business, please read my proposal carefully its 100% Risk-free.

With warm hearts I offer my friendship, and my greetings, and I hope this letter meets you in good time. I am Mrs Patricia Knight, i am married to Late Larry Knight who was a miner in Australia. The Beacons field Mine collapse occurred on 25 April 2006 in Beacons field, Tasmania, Australia. Of the seventeen people who were in the mine at the time, fourteen escaped immediately following the collapse, one was killed namely (Larry Knight) who happens to be my beloved husband and the remaining two were found alive using a remote-controlled device. These two miners were rescued on 9 May 2006, two weeks after being trapped nearly a kilometer below the surface.

We were married for 5 years without a child. Since his death i decided not to remarry or get a child outside my matrimonial home which the Bible spoke against. When my husband was alive he deposited some Funds with a finance company in the Middle east. Presently my doctor told me that it will take the grace of GOD to survive a Heart disease problem. Having known my condition I decided to donate this fund to a christian individual that will use this funds wisely and in Christ like way. My husband's relatives are not Christians and I don't want my husband's hard earned money to be misused by unbelievers that's why i had to relocate to middle east where the Funds is lodged.

As soon as I receive your reply I shall give you more information and supporting documents.

FILL INFORMATIONS BELOW

1. Full name:.....
2. Full Contact Address:.....
3. State:.....
4. City:.....
5. Zip Code:.....
6. Country:.....
7. Occupation:.....
8. Company Name:.....
9. Position:.....
- 10.Marital Status:.....
- 11.Age:.....
- 12.Mobile Number:.....
- 13:Other Numbers:.....
- 14.Fax Number:.....

Thanks for your cooperation.
Best regards,
Mrs Patricia Knight.

From: DEME GROUP NV [mailto:alain.bernard90@hotmail.com]

Sent: June 12, 2016 3:53 PM

To: Steve Thomas <sthomas@mcslaw.com>

Subject: LEGAL HELP

Hi,

We are a Europe based Marine Construction firm and we need an attorney to assist us in drafting a purchase and Sales agreement with a buyer in your area. Are you able to take this matter? If not, a referral will be appreciated.

Alain Bernard, CEO DEME Group

Haven 1025 - Scheldedijk 30

2070 Zwijndrecht

Belgium

www.deme-group.com

+32465765969

Deme Group is a real company, very large, with its own domain – deme-group.com.

It has subsidiaries in many countries, including one in Mexico (but no office or subsidiary in the US)

Alain Bernard is the CEO

This is the correct address

But the phone number is incorrect, and it has one extra digit.

From: chrisnorman155@gmail.com
[mailto:chrisnorman155@gmail.com] **On Behalf Of** Tosei Engineering Corp.
Sent: May 28, 2016 1:50 PM
To: Steve Thomas <sthomas@mcsllaw.com>
Subject: LEGAL REPRESENTATION REQUIRED

First clue – again, a generic domain involved.

Hello Steve Thomas,

I wish to inquire about your possible legal representation on behalf of my company. Do let me know if your firm is currently accepting new clients.

I look forward to your prompt response.

Sincerely,
JIRO KATASHI
Tosei Engineering Corp.
2968-2, Ishikawa-machi, Hachioji-shi, Tokyo,
192-0032 Japan

Again, large company

This is the wrong address for Tokyo office

Most important, the company has offices in Canada, Mexico, and **Cincinnati, Ohio.**

From: "American Airlines" <information-no896@aa.com>

Sent: Friday, June 08, 2012 7:50 PM

To:

Subject: Your order #9480 is processed

Dear Customer,

E-TICKET NUMBER / 2 743 1372097315 2

SEAT / 69E/ZONE 1

DATE / TIME 23 JUNE, 2012, 10:50 AM

ARRIVING / Detroit

FORM OF PAYMENT / CC

TOTAL PRICE / 249.49 USD

REF / EK4286 ST / OK

BAG / 1PC

Your bought ticket is attached.

To use your ticket you should print it.

Thank you

American Airlines.

This example is from a cybersecurity workshop at ABA Techshow 2016

Correct domain. Assume the "To" line has your name in it.

Fabricated but realistic details, including a price, but no departure city, and only one date and time listed.

"Your bought ticket is attached."

Trying to get you to open the attachment. First reaction might be to open just to see if AA made a mistake.

Fraudulent Fraud Alert

Another example from ABA Techshow 2016

Chase <celsdew1@suddenlink.net>
To: Recipients <celsdew1@suddenlink.net>
Alert

April 30, 2015 1:08 PM
Hide Details

CHASE

Dear Chase OnlineSM Customer:

We're writing to let you know that your account has been recently access from a different Ip location. You are required to verify your account to prevent Fraudulent activities.

log on to www.Chase.com/Vaillfication/process

<http://targetrate.com/chase>

Please don't reply directly to this automatically-generated e-mail message.

Sincerely,
Online Banking Team

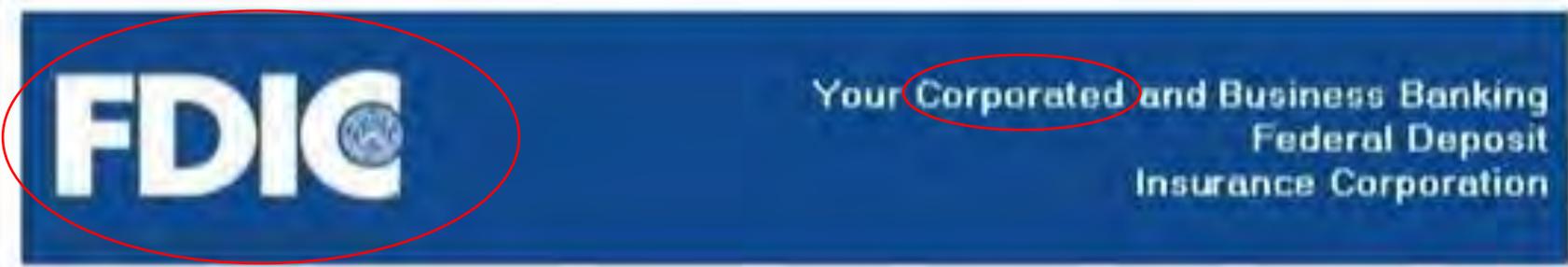
Chase logo, but Suddenlink domain, to line says "Recipients" but has sender's email again.

Clues in the text.

Real destination is different from that shown—not a Chase domain at all.

From: FDIC
Date: Thursday, September 13, 2012 7:15 AM
To:
Subject: Urgent! You must install a new security version!

Another example from ABA Techshow 2016



Awkward structure.

Your ability to fulfill **ACH and Wire transfers** has been **provisionally suspended** in order to ensure your safety, due to the expiration of your security version. Please download and install the **updated programs**, by following this [link](#).

As soon as it is set up, your transaction abilities will be fully resumed.

Kind regards, **Online Security Department**, Federal Deposit Insurance Corporation.

From: Apple [mailto:actu@b.linternaute.com]
Sent: Friday, February 5, 2016 10:47 AM
To: Cullen Aderhold
Subject: Update your Apple account !

Dear iTunes Customer,

This is an automatic message sent by our security system to let you know that you have **48 hours** to confirm your account information.

Your itunes account has been frozen because we are unable to validate your account information.

Once you have updated your account records, we will try again to validate your information and your account suspension will be lifted. This will help protect your account in the future. This process does not take more than 3 minutes. To proceed to confirm your account details please click on the link below and follow the instructions.

[Click Here Validate Your Account.](#)

We apologise for any inconvenience caused.

Your sincerely,

Apple Security Department

Apple's address is
1 Infinite Loop
Cupertino, CA **95014**

Phishing

The attempt to acquire sensitive information or control over valuable resources by masquerading as a trustworthy person or entity in an electronic communication.

Sometimes Spearphishing targets a specific person or group, such as executives or managers at a large corporation. Sometimes its just a more aggressive form of social engineering, more likely to gain your trust because it comes from someone you know.

SpearPhishing

The attempt to acquire **from a specific recipient or group of recipients** sensitive information or control over valuable resources by masquerading as **someone the recipient knows or does business with** in an electronic communication.



Jim Shelton is a solo practitioner in Clarendon, Texas. In April 2016, he started getting phone calls from thousands of people in the US, Canada, and the UK who had received this email.

Susie Black is an employee, and this is her email address.

Each recipient's info was correct.

The attached word document (note that it says "invoice" instead of "subpoena") contained a variant of Dridex, a strain of banking malware that leverages macros in Microsoft Office. Once it infects a system, the criminals can use it to steal banking credentials and other personal information.

From: Blau Russell M. [mailto:torrencelewis@federalappeals.com]

Sent: May 16, 2016 9:04 PM

To: sj <sj@wisecarter.com>; sta <sta@bloostonlaw.com>; Steve Thomas <sthomas@mcslaw.com>; Strenkowski Jeffrey R. <Jeffrey.Strenkowski@bingham.com>; tjones <tjones@willkie.com>

Subject: Fw: just look at that

Hi,

You wouldn't believe what I've found on the Internet, just look at that here

<http://trandyndunto.feastwear.com/realize.php>

Take care, Blau Russell M.

What is PHP?

PHP is a general-purpose scripting language that is especially suited to **server-side web development**, in which case PHP generally **runs on a web server**. PHP can be deployed on most web servers, many operating systems and platforms, and can be used with many relational database management systems. Most web hosting providers support PHP for use by their clients. It is available free of charge, and the PHP Group provides the complete source code for users to build, customize and extend for their own use.

In 2013, 9% of all vulnerabilities listed by the National Vulnerability Database were linked to PHP; historically, about 30% of all vulnerabilities listed since 1996 in this database are linked to PHP.

Ask yourself: Why would anyone ever send you a .php file, or a link to one?

.php

.exe

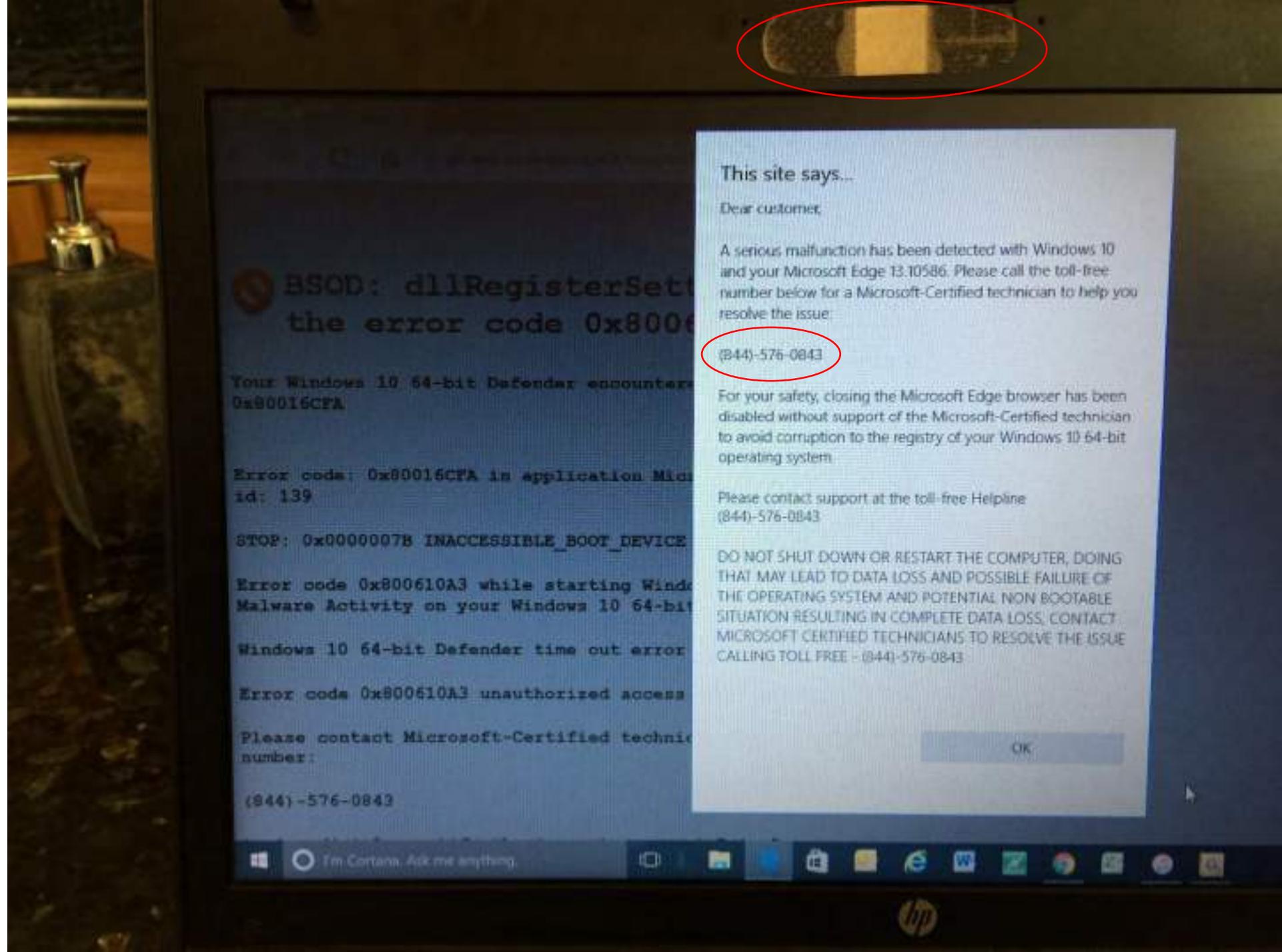
.zip

.doc(x)

If anyone you don't know ever sends you an email with an attachment with one of these extensions, or links you to a file ending with one of these extensions, you should think:



Exploit Kits



TAKEAWAYS

THINK BEFORE YOU CLICK . . . or call, or reply, or take any other action.

If you don't know the sender, don't trust the email.

Check the sender's email address and other details to make sure it isn't spoofed.

Ask yourself, is this sender the kind of person who would send me this kind of email?

If you aren't sure, contact the sender before clicking on any link or attachment.

Providing sensitive information by ordinary email is not secure, so most reputable companies or organizations won't ask you to do so.

Any email that asks you to click on a link or attachment to provide your personal information is suspect.

If you are hit with an attack, don't trust any message from the attacker (such as, call this number to have a Microsoft Certified Tech remove the malware).

Just because it looks like your bank's website doesn't mean it is. Be wary of ANY pop-up windows or other unusual requests for you to input your personal information.

If in doubt, close it out.

If your computer gets locked up or infected in any way, disconnect it from the network, but DO NOT TURN IT OFF. Just leave it alone and call for help. To disconnect it from the network, unplug the Ethernet cable from the back (the wire with the little plastic clip on the connector).

THANKS FOR LISTENING!