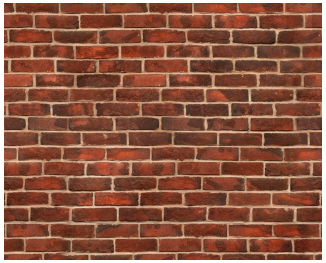
Social Engineering Attacks

Mariano Ceccato

mariano.ceccato@univr.it

What is social engineering

- Psychological manipulation of people into performing actions or divulgating personal information



Firewall

Access control

Anti virus

End users

President Macron's Identity Theft

WORLD NEWS

Two Frenchmen on trial for stealing President Macron's online identity

The main defendant is accused of using a Gmail address purporting to belong to Macron to send a long political email titled "10 good reasons not to vote for me."

By Associated Press | Associated Press, Paris

UPDATED ON MAR 14, 2018 05:01 PM IST

French President Emmanuel Macron addresses the media at the Elysee Palace in Paris, France, March 8, 2018.(Reuters)

https://www.hindustantimes.com/world-news/two-frenchmen-on-trial-for-stealing-president-macron-s-online-identity/story-tpElBRZRGi1PYToHTGlHxO.html

Facebook Lottery Scam

- Notification of 500k$ winning
- FBI is involved
- A friend in your network contacts you with a positive experience with this
- Some money are needed to unlock the winning

https://www.scamwatch.gov.au/get-help/real-life-stories/unexpected-prize-lottery-scam-davins-fictional-facebook-lottery-win

Types of Social Engineering Attacks

Computer Based

- Phishing
- Spear phishing
- Whaling
- Viral hoax

Human Based

- Vishing
- Impersonation
- SMiShing
- Tailgating

Phishing

Agenzia delle Entrate - Amministrazione fiscale

Con la presente ti informiamo che nel tentativo di rimborsare l'account l'operazione non è andata a buon fine.

Accedi al tuo portale di rimborso delle tasse per elaborare manualmente il rimborso. Durante il processo, è possibile aggiornare le informazioni dell'account fornite. AGGIORNARE.

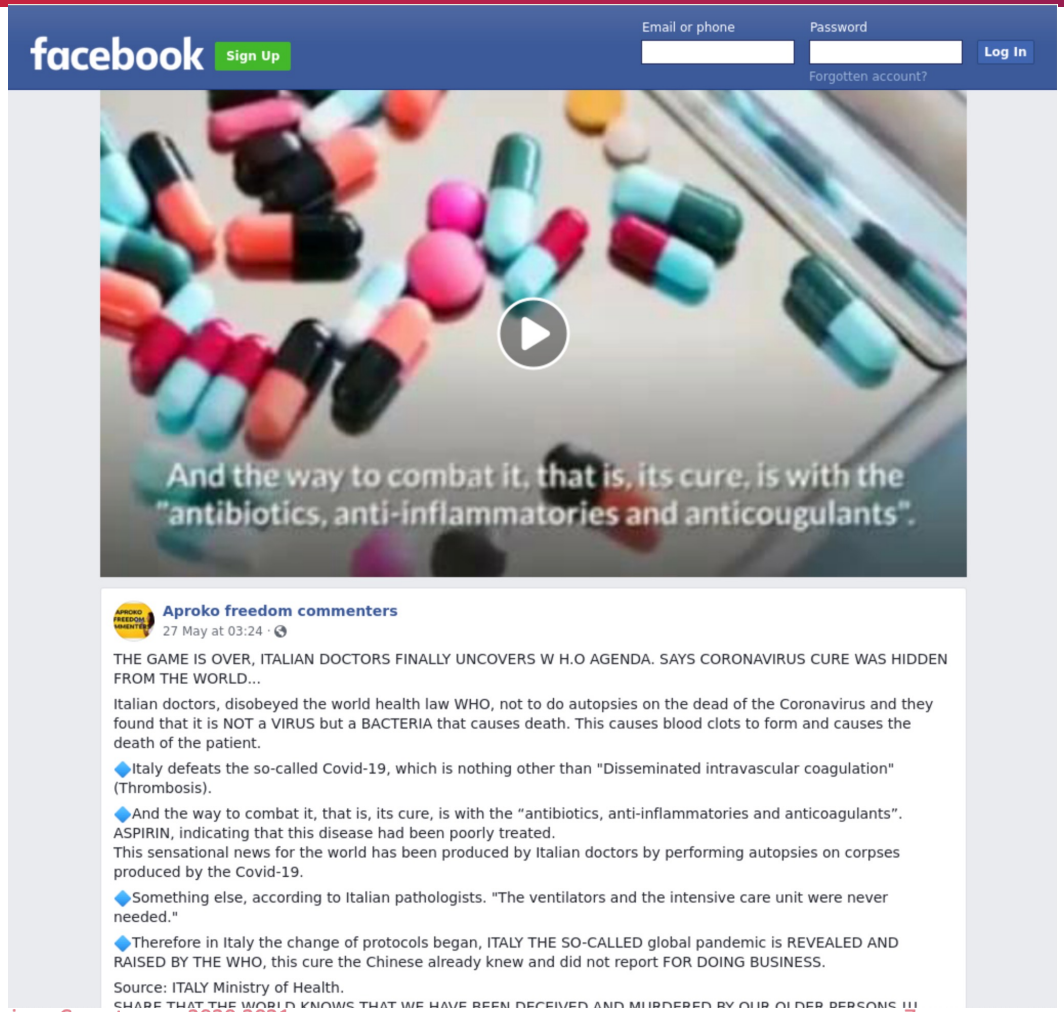
Data di pagamento: 30 Giugno 2018
Numero della fattura: ADE / P881P29 / IT2001
Importo: €1,482.05 EUR

NOTA BENE: Questa E-Mail è un documento di fatturazione ufficiale per il rimborso.

https://www.agenziaentrate.gov.it/portale/web/guest/-/cs-30072018-mail-truffa

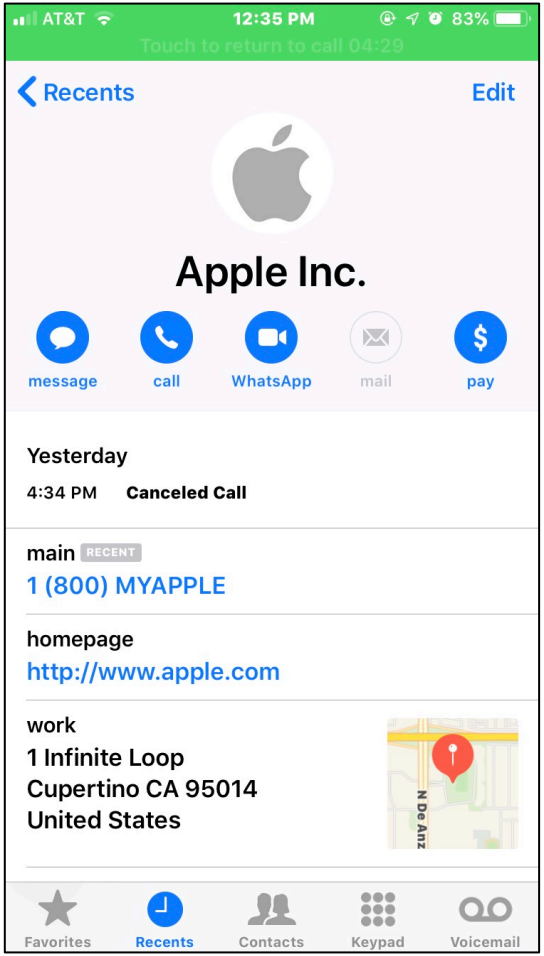
Viral hoax

- Coronavirus: pandemic virus conspiracy video spreads across social media

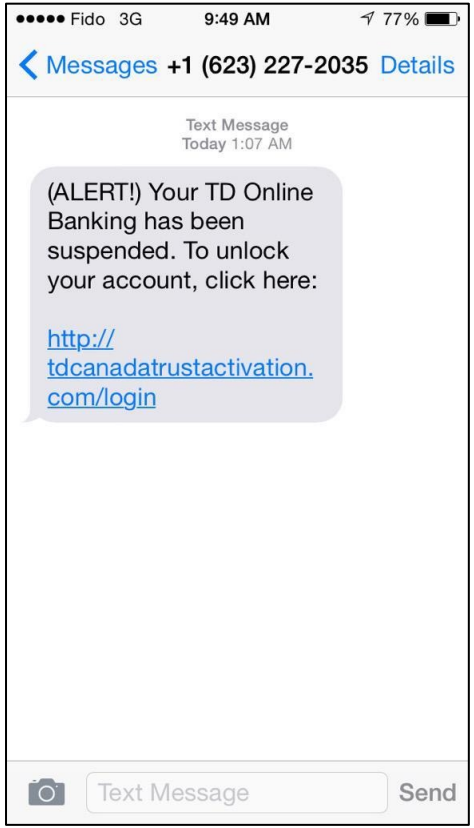


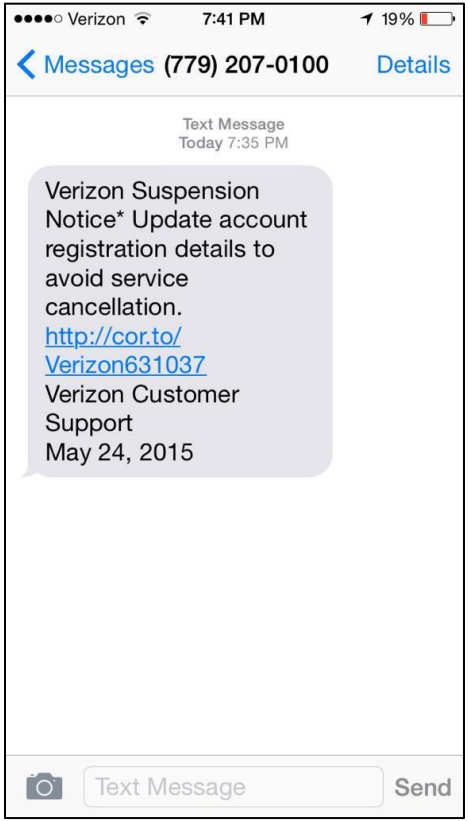
Vishing – voice phising

- Receiving phone calls that look legitimate
- Asking for personal information to solve security issues



SMiShing – SMS Phishing



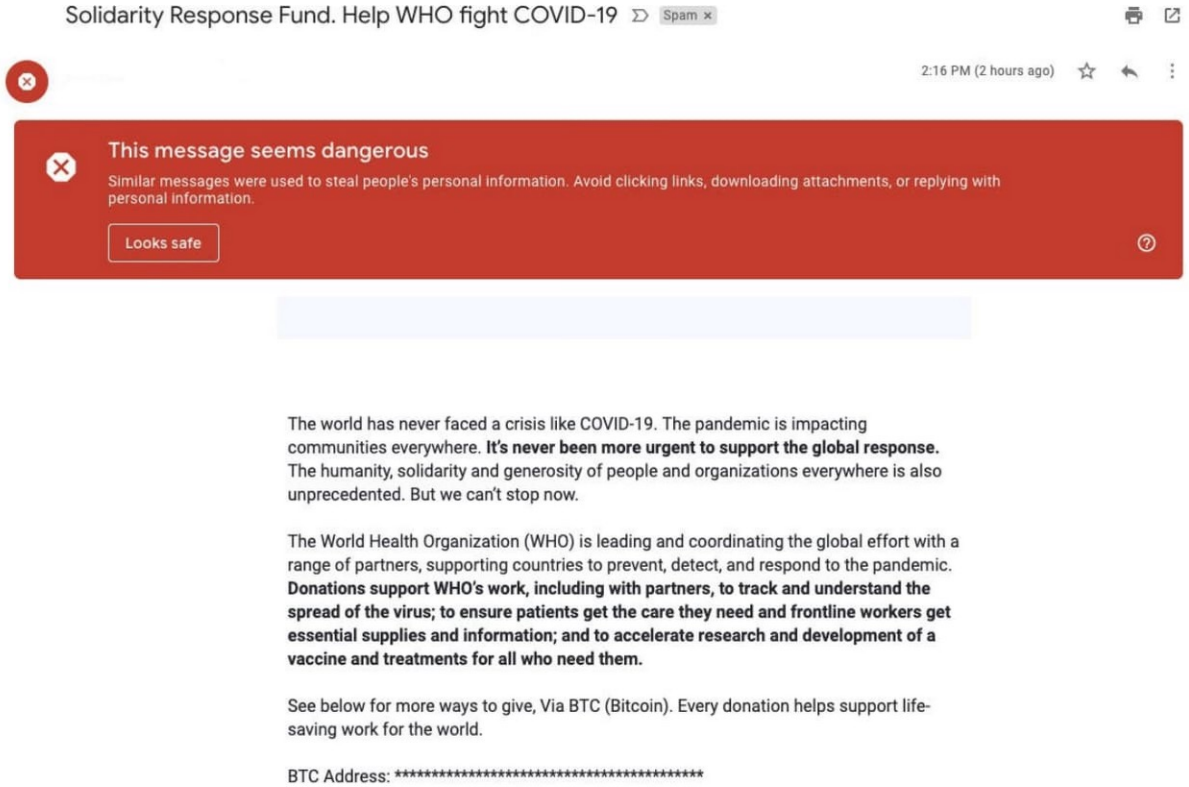


Tailgating, Piggybacking

Phishing

- Attempt to acquire sensitive information (often for malicious reasons) by masquerading as a trustworthy entity in an electronic communication
  - Information: usernames, passwords, and credit card details (and sometimes, indirectly, money)

Gmail blocked more than 100M phishing emails



Solidarity Response Fund. Help WHO fight COVID-19 Spam ×

2:16 PM (2 hours ago)

This message seems dangerous

Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments, or replying with personal information.

Looks safe

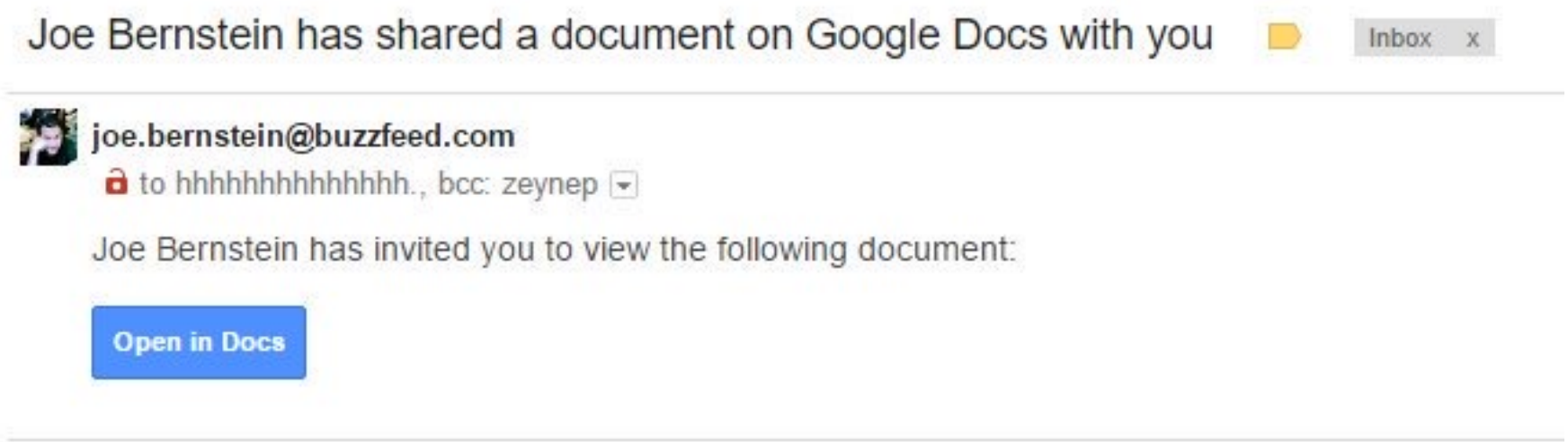
The world has never faced a crisis like COVID-19. The pandemic is impacting communities everywhere. **It's never been more urgent to support the global response.** The humanity, solidarity and generosity of people and organizations everywhere is also unprecedented. But we can't stop now.

The World Health Organization (WHO) is leading and coordinating the global effort with a range of partners, supporting countries to prevent, detect, and respond to the pandemic. **Donations support WHO's work, including with partners, to track and understand the spread of the virus; to ensure patients get the care they need and frontline workers get essential supplies and information; and to accelerate research and development of a vaccine and treatments for all who need them.**

See below for more ways to give, Via BTC (Bitcoin). Every donation helps support life-saving work for the world.

BTC Address: **********

Massive Phishing Attack against Gmail users



Target data breach

Target to Pay $18.5 Million to 47 States in Security Breach Settlement

Target's headquarters in Minneapolis. A settlement by the company ended an investigation into how the data of millions of customers was compromised in 2013. Glen Stubbe/Star Tribune, via Associated Press

By Rachel Abrams

May 23, 2017

Target will pay $18.5 million to 47 states and the District of Columbia as part of a settlement with state attorneys general over a huge security breach that compromised the data of millions of customers.

The settlement ends a yearslong investigation into how hackers obtained names, credit card numbers and other information about tens of millions of people in 2013.

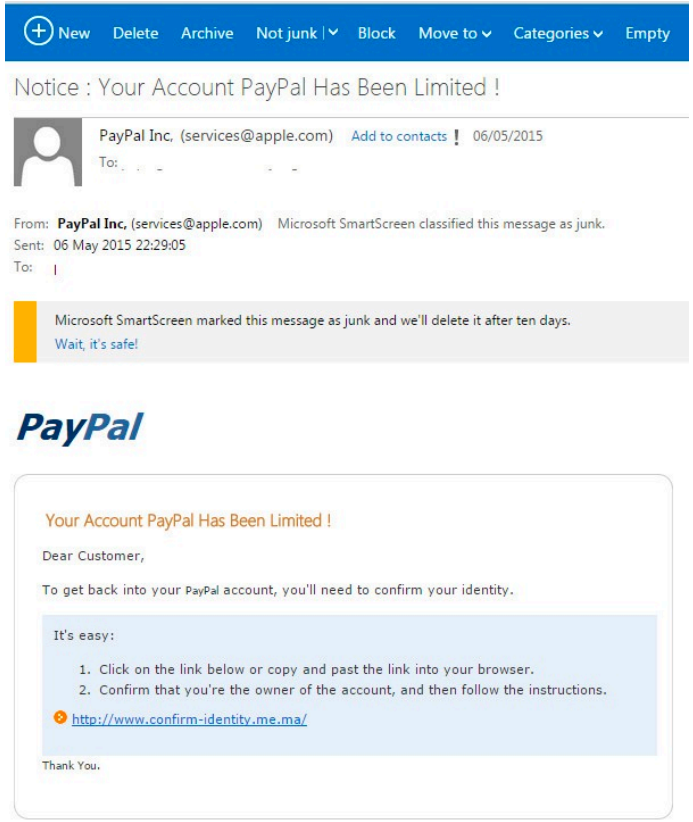
New York will receive $635,000, while California will receive $1.4 million, the largest amount of any state, according to the Eric T. Schneiderman, New York's attorney general. Dollar figures were determined "largely" based on each state's population size, his office said.

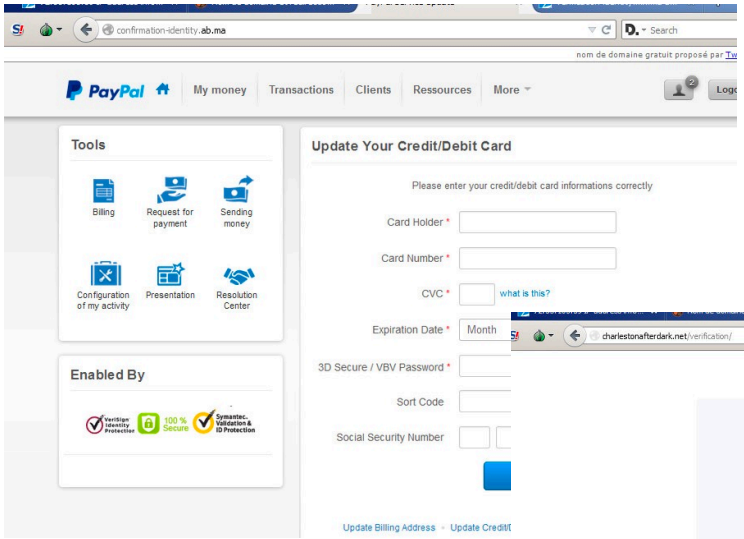
Wyoming, Wisconsin and Alabama were not included in Tuesday's announcement. Representatives for the attorneys general in those states did not have an immediate comment or could not be reached.

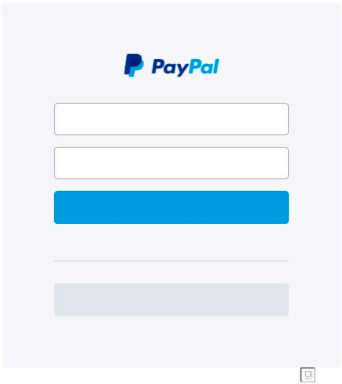
https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html

Phisching emails

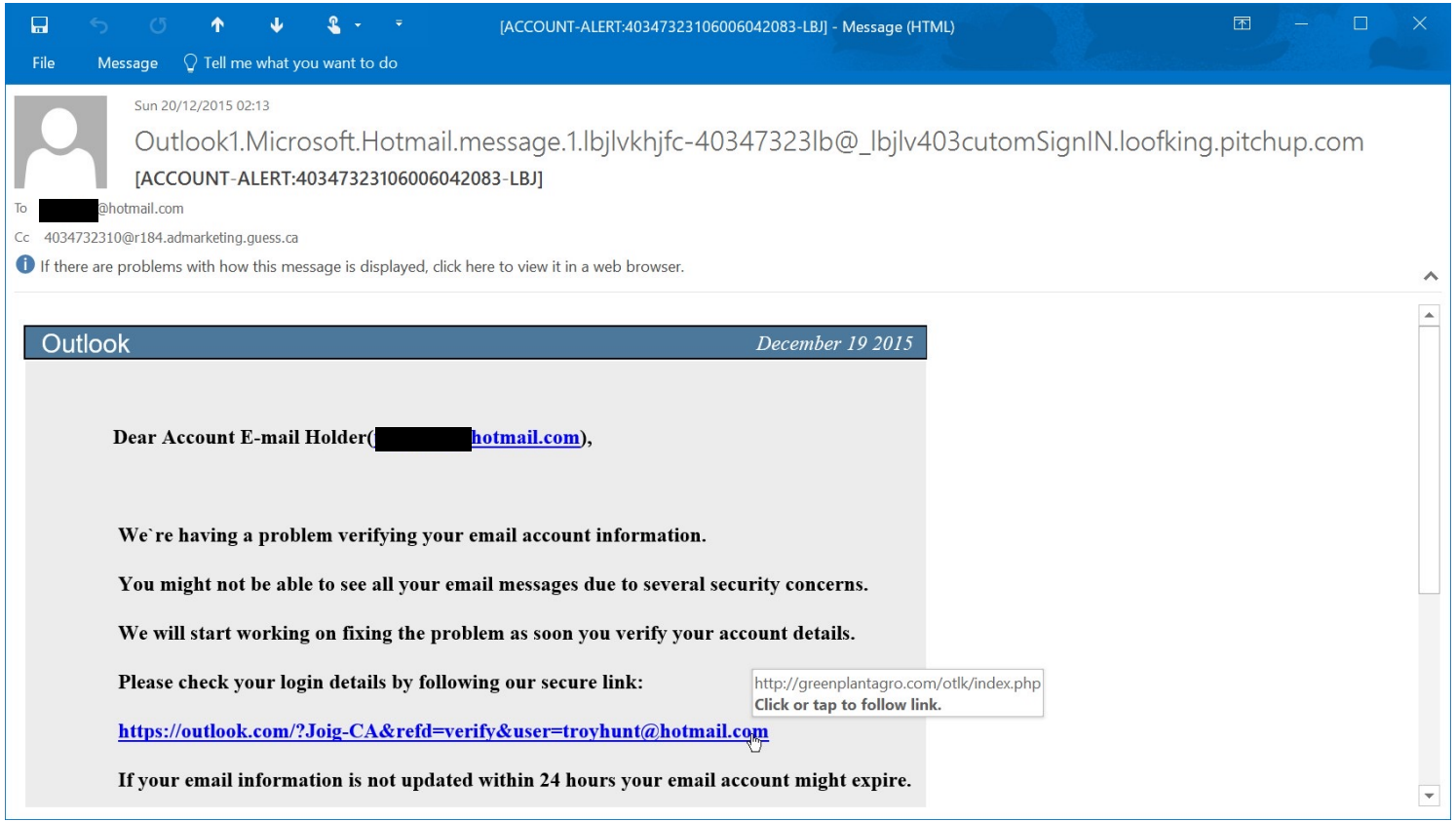
PayPal Phishing Scam







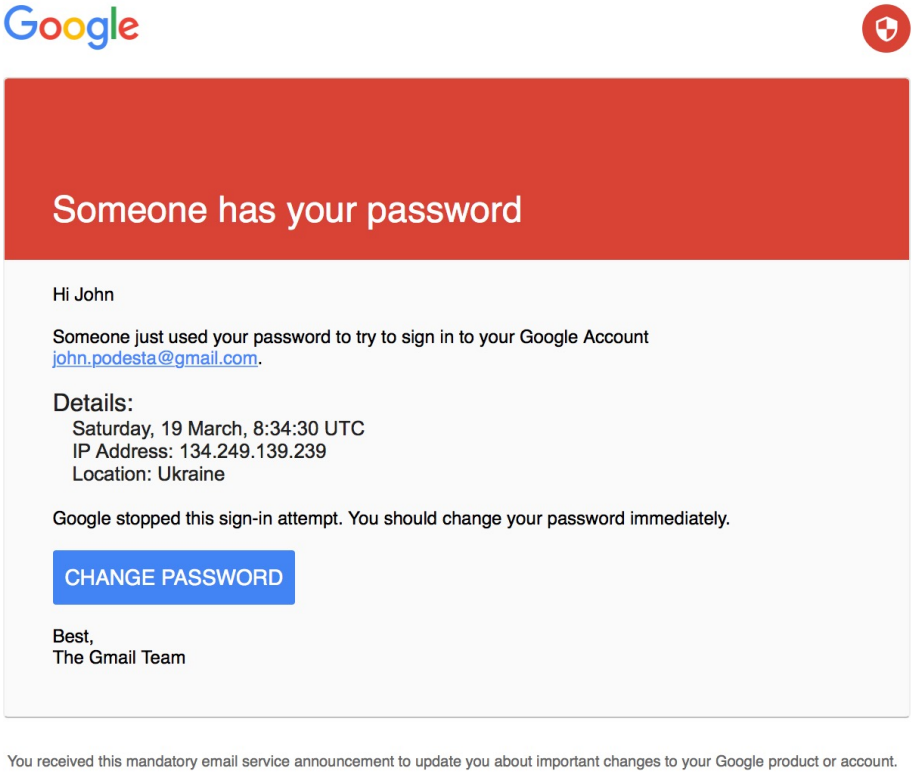
Hyperlink target mismatch



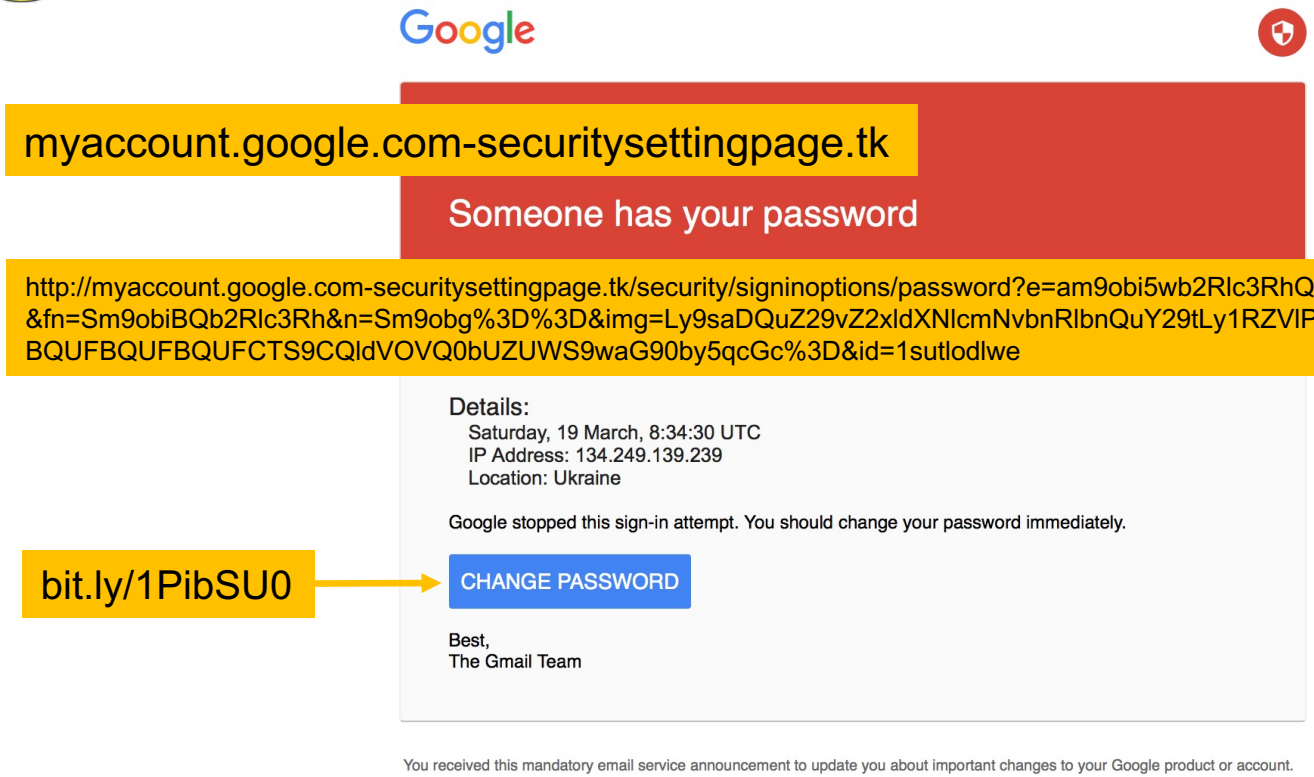
Spearphishing

- A phishing attack specifically mounted against a target organization or user
- Frequently tailored to the victim by representing information that is unique to them in order to build authenticity

John Podesta spearphishing attack

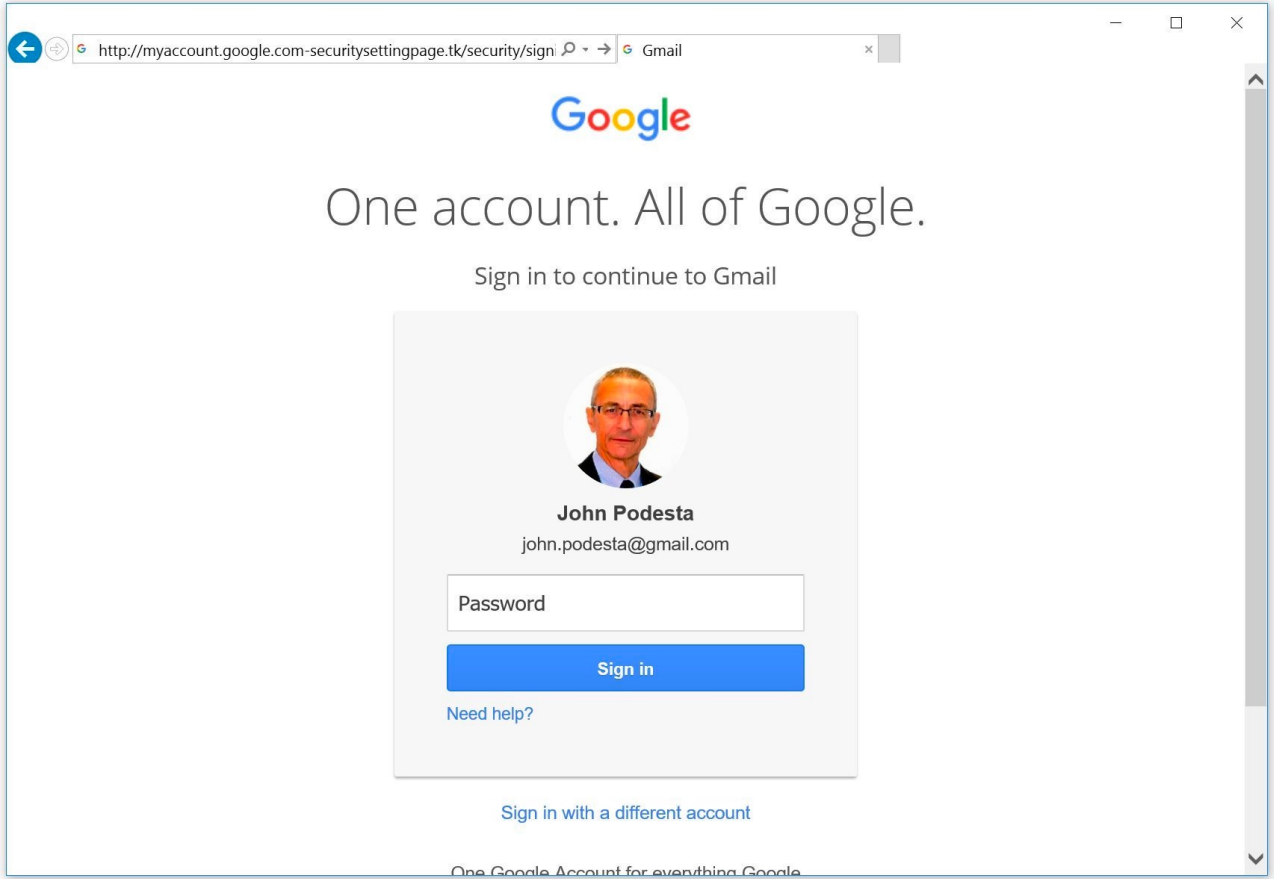


John Podesta spearphishing attack

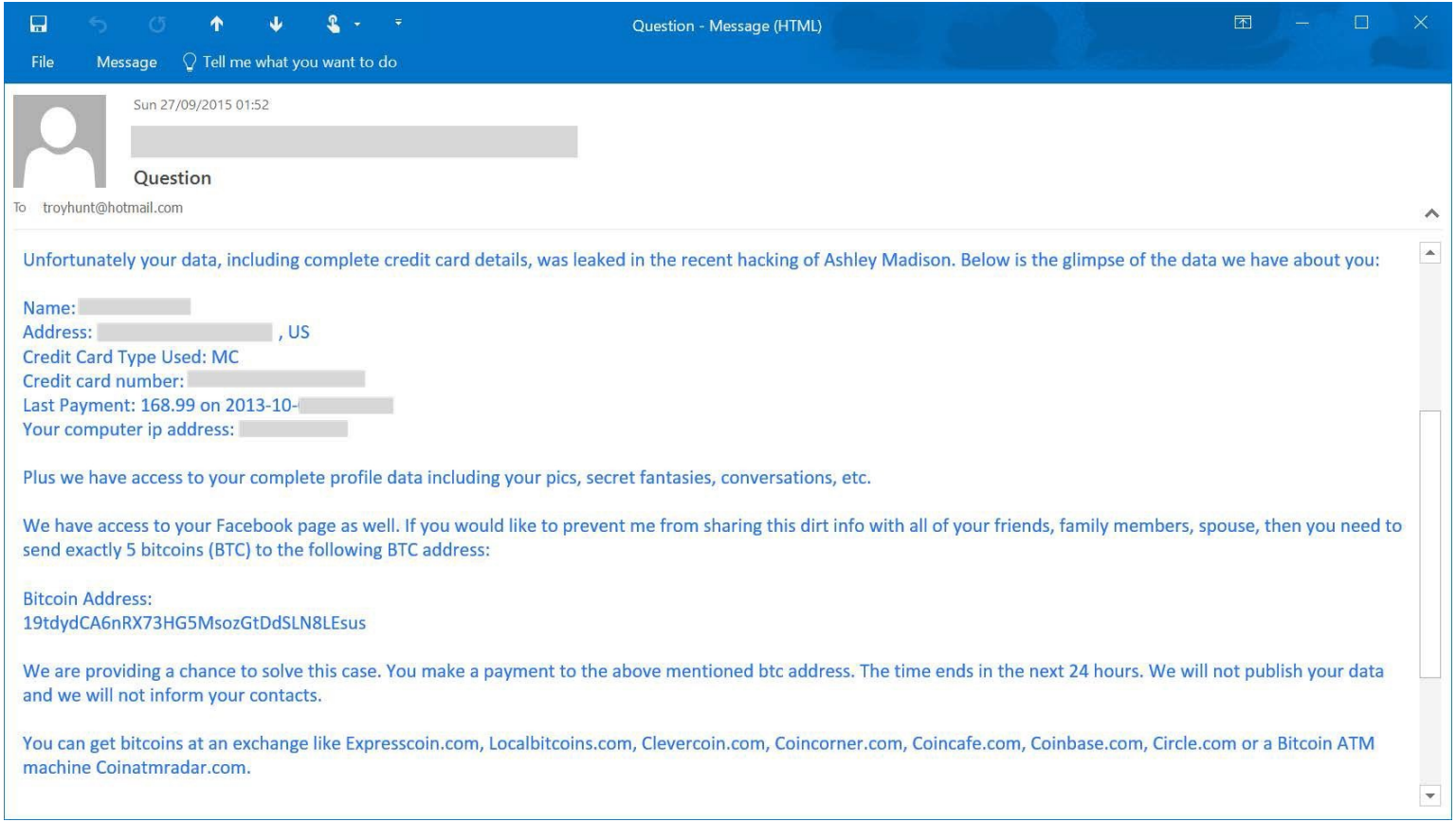


bit.ly/1PibSU0

John Podesta spearphishing attack



Spearphishing and Extorsion



Question - Message (HTML)

File Message Tell me what you want to do

Sun 27/09/2015 01:52

Question

To troyhunt@hotmail.com

Unfortunately your data, including complete credit card details, was leaked in the recent hacking of Ashley Madison. Below is the glimpse of the data we have about you:

Name:
Address: , US
Credit Card Type Used: MC
Credit card number:
Last Payment: 168.99 on 2013-10-
Your computer ip address:

Plus we have access to your complete profile data including your pics, secret fantasies, conversations, etc.

We have access to your Facebook page as well. If you would like to prevent me from sharing this dirt info with all of your friends, family members, spouse, then you need to send exactly 5 bitcoins (BTC) to the following BTC address:

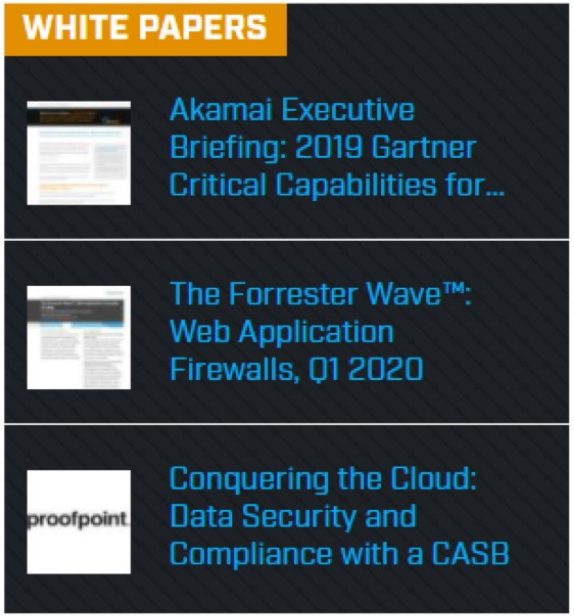
Bitcoin Address:
19tdydCA6nRX73HG5MsozGtDdSLN8LEsus

We are providing a chance to solve this case. You make a payment to the above mentioned btc address. The time ends in the next 24 hours. We will not publish your data and we will not inform your contacts.

You can get bitcoins at an exchange like Expresscoin.com, Localbitcoins.com, Clevercoin.com, Coincorner.com, Coincafe.com, Coinbase.com, Circle.com or a Bitcoin ATM machine Coinatmradar.com.

Whaling

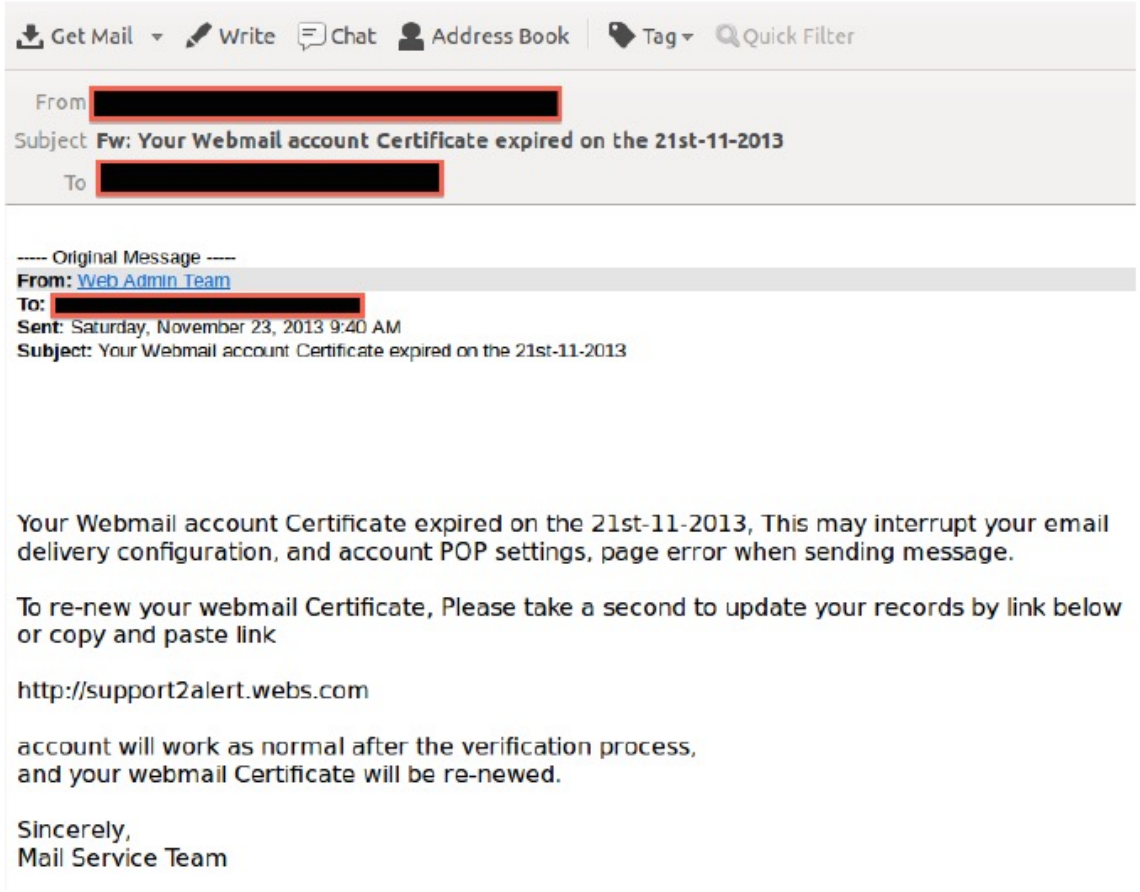
- A form of spearphishing that targets high-ranking victims within a company
  - E.g. CFO and CEO



Influence Tactics

Exploiting Authority

Exploiting Scarcity



Get Mail ▾ Write Chat Address Book Tag ▾ Quick Filter

From [redacted]
Subject **Fw: Your Webmail account Certificate expired on the 21st-11-2013**
To [redacted]

----- Original Message -----
From: Web Admin Team
To: [redacted]
Sent: Saturday, November 23, 2013 9:40 AM
Subject: Your Webmail account Certificate expired on the 21st-11-2013

Your Webmail account Certificate expired on the 21st-11-2013, This may interrupt your email delivery configuration, and account POP settings, page error when sending message.

To re-new your webmail Certificate, Please take a second to update your records by link below or copy and paste link

http://support2alert.webs.com

account will work as normal after the verification process,
and your webmail Certificate will be re-newed.

Sincerely,
Mail Service Team

Exploiting Commitment

----- Original Message -----
From: Notice to Appear
To: [redacted]
Sent: Monday, December 23, 2013 5:47 PM
Subject: [!! SPAM] Suspicious part has been deleted : Notice of appearance in court NR#9386

Notice to Appear,

Hereby you are notified that you have been scheduled to appear for your hearing that will take place in the court of Washington in January 14, 2014 at 10:00 am.

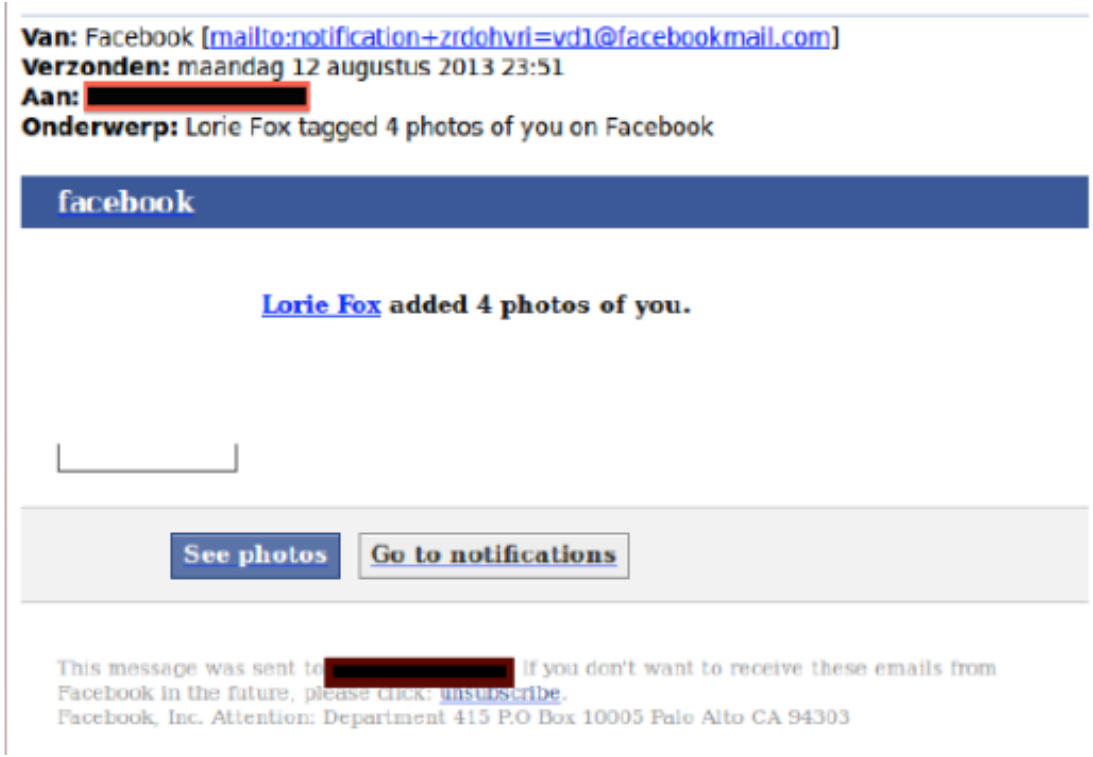
Please bring all documents and witnesses relating to this case with you to Court on your hearing date.

The copy of the court notice is attached to this letter.
Please, read it thoroughly.

Note: If you do not attend the hearing the judge may hear the case in your absence.

Yours truly,
Emily Smith
Clerk to the Court.

Exploiting Liking



Van: Facebook [mailto:notification+zrdohvrl=vd1@facebookmail.com]
Verzonden: maandag 12 augustus 2013 23:51
Aan: [redacted]
Onderwerp: Lorie Fox tagged 4 photos of you on Facebook

facebook

Lorie Fox added 4 photos of you.

See photos | Go to notifications

This message was sent to [redacted]. If you don't want to receive these emails from Facebook in the future, please click: unsubscribe.
Facebook, Inc. Attention: Department 415 P.O Box 10005 Palo Alto CA 94303

Exploiting Reciprocation

Congratulations, you have won $20 dollars towards your next purchase of edible goods. This money has been donated by APPLES Co., a non profit organization founded to promote the purchase of organic foods.

These $20 will be applicable in any local grocery supermarket.

You will receive it in the form a gift card that will be sent to your mailing address. In the meantime, please click the link below to vote for APPLES Co. as the top 10 non-profit of the year in our region!

malicious link

Exploiting Social Proof

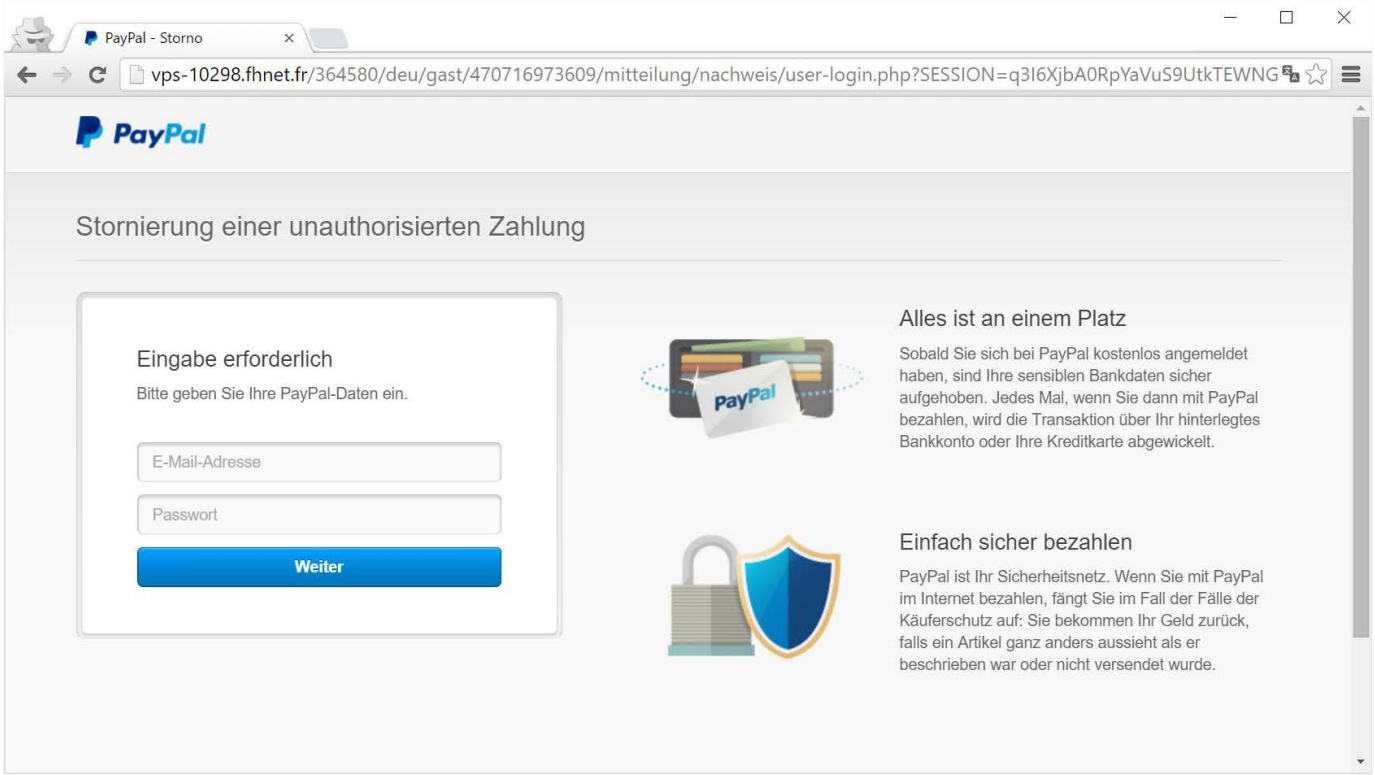
I would like to invite you to **join the thousands of other clients** who have experienced our vacation excursions. We are currently serving **ten clients in your neighborhood** and this is how we got your contact information.

Our company called Dunes was developed for clients to experience lavish vacation spots at an affordable price. We have earned the title of Top 10 Best Travel Agency from TripAdvisor.

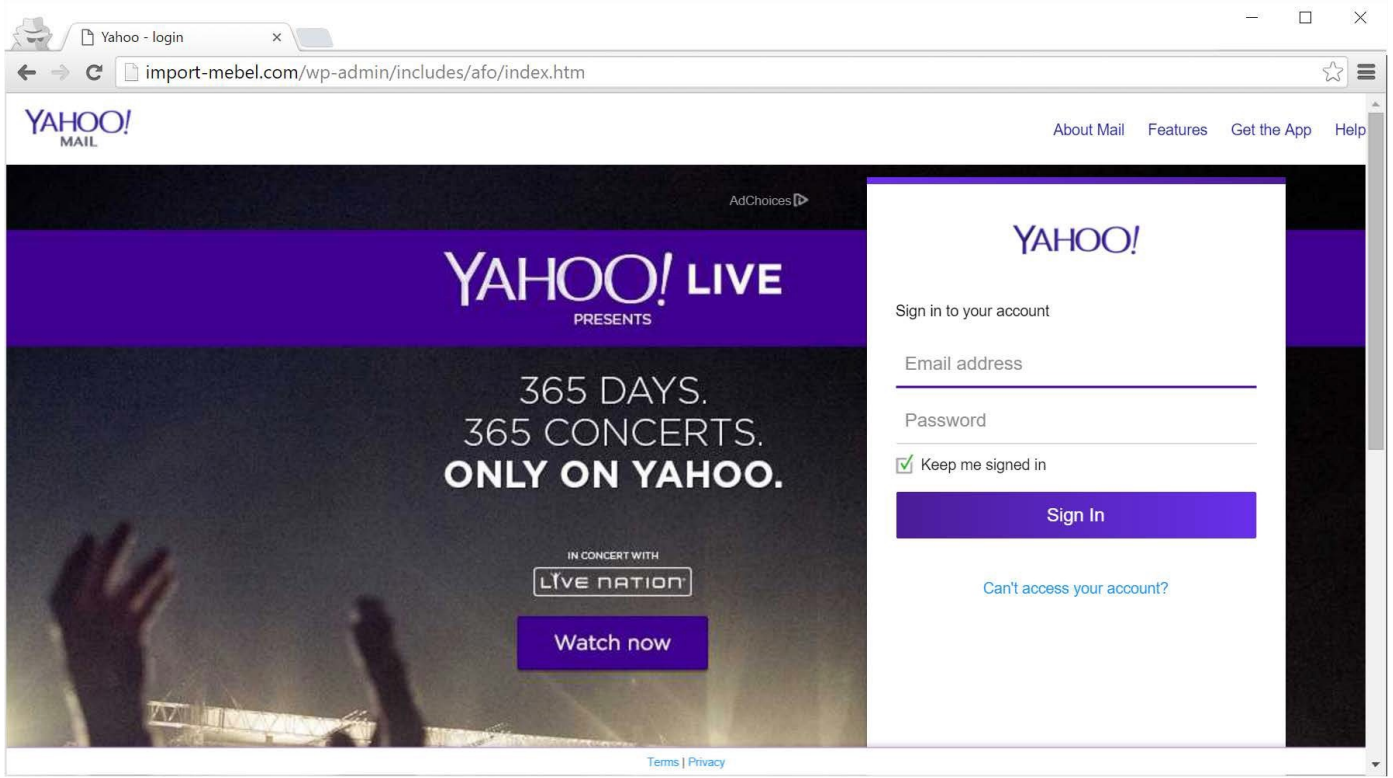
To learn more on how you can start planning your dream vacation, visit our website at malicious link

Phishing Websites

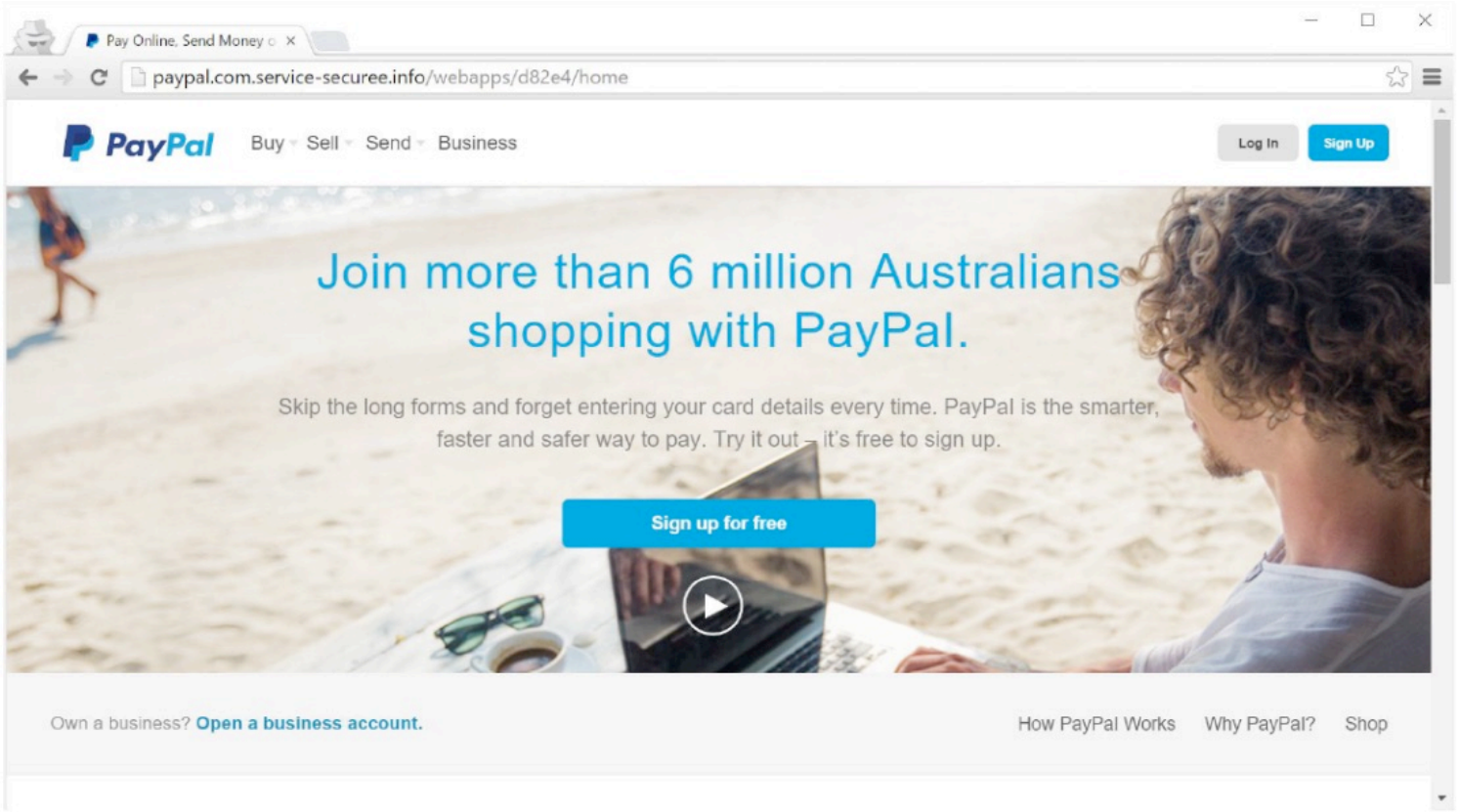
Irregular domain names



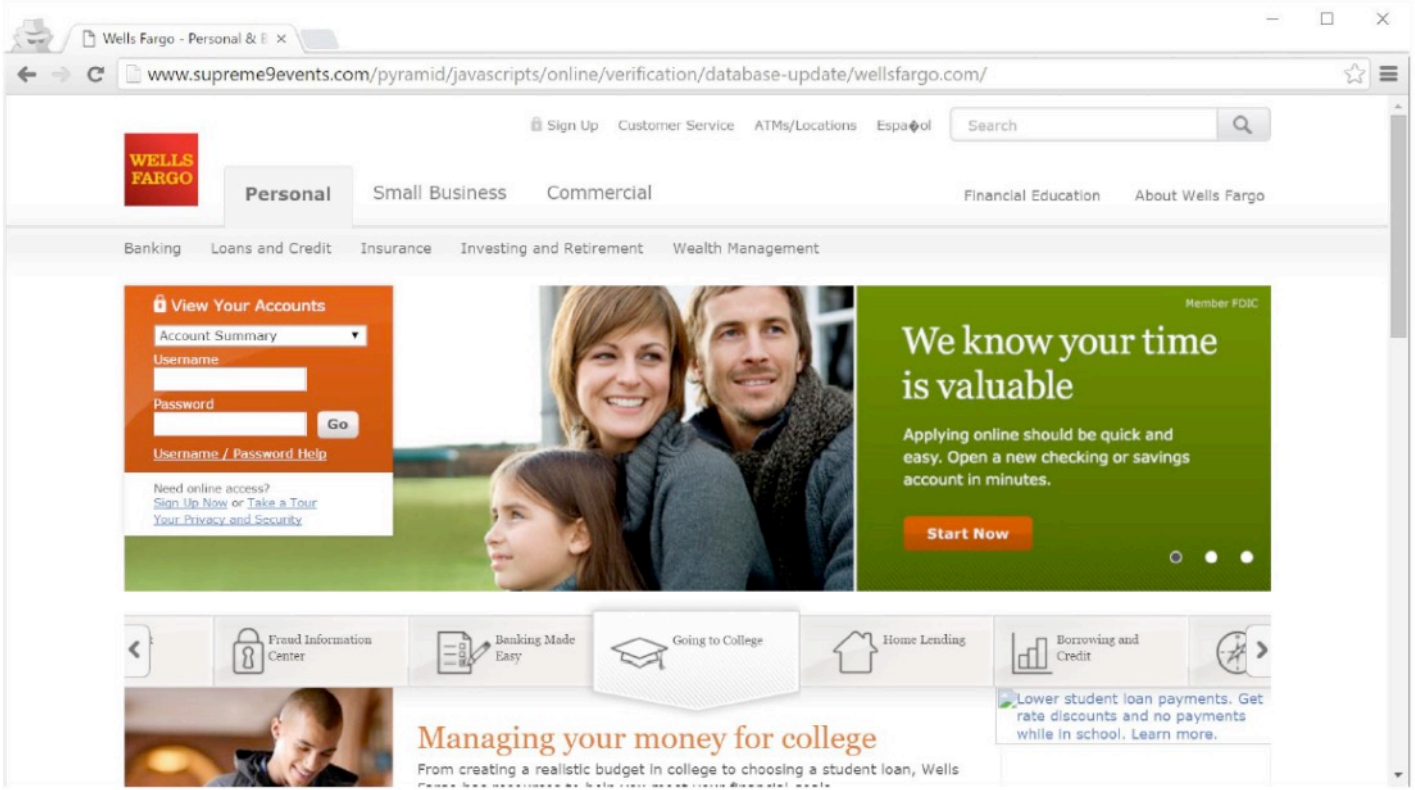
Missing HTTPS



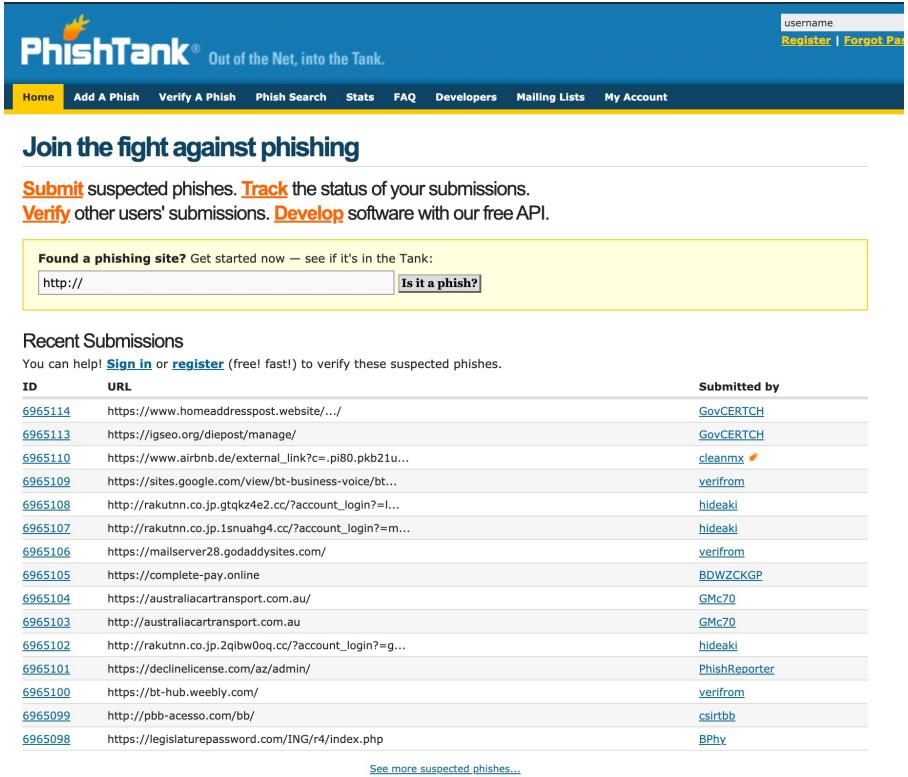
(Sub) domain name



Website Hijacking



Identifying Attacks with PhishTank



PhishTank® Out of the Net, into the Tank.

username
Register | Forgot Pas

Home | Add A Phish | Verify A Phish | Phish Search | Stats | FAQ | Developers | Mailing Lists | My Account

Join the fight against phishing

Submit suspected phishes. Track the status of your submissions.
Verify other users' submissions. Develop software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:

http:// Is it a phish?

Recent Submissions

You can help! Sign in or register (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
6965114	https://www.homeaddresspost.website/.../	GovCERTCH
6965113	https://igseo.org/diepost/manage/	GovCERTCH
6965110	https://www.airbnb.de/external_link?c=.pi80.pkb21u...	cleanmx
6965109	https://sites.google.com/view/bt-business-voice/bt...	verifrom
6965108	http://rakutnn.co.jp.gtqkz4e2.cc/?account_login?=l...	hideaki
6965107	http://rakutnn.co.jp.1snuahg4.cc/?account_login?=m...	hideaki
6965106	https://mailserver28.godaddysites.com/	verifrom
6965105	https://complete-pay.online	BDWZCKGP
6965104	https://australiacartransport.com.au/	GMc70
6965103	http://australiacartransport.com.au	GMc70
6965102	http://rakutnn.co.jp.2qibw0oq.cc/?account_login?=g...	hideaki
6965101	https://declinelicense.com/az/admin/	PhishReporter
6965100	https://bt-hub.weebly.com/	verifrom
6965099	http://pbb-acesso.com/bb/	csirtbb
6965098	https://legislaturepassword.com/ING/r4/index.php	BPhy

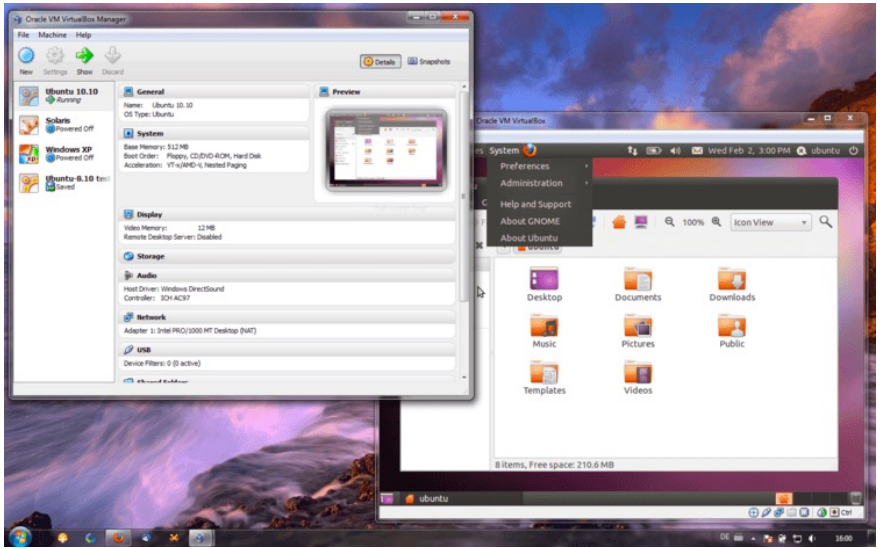
See more suspected phishes...

New to PhishTank?

Subscribe to the PhishTank mailing lists.

Virtual box

- High performance virtualization tool, to run a *guest OS* in your *host OS*
- Support for multiple host OSes
- https://www.virtualbox.org/



Kali Linux – offensive security

- Linux distribution maintained and funded by Offensive Security
- Designed for digital forensics and penetration testing
- Many security auditing tools are pre-installed and configured
  - exploiting a victim network or application
  - performing network discovery/scanning
  - scanning a target IP address
  - penetration testing
  - password crack

- https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/