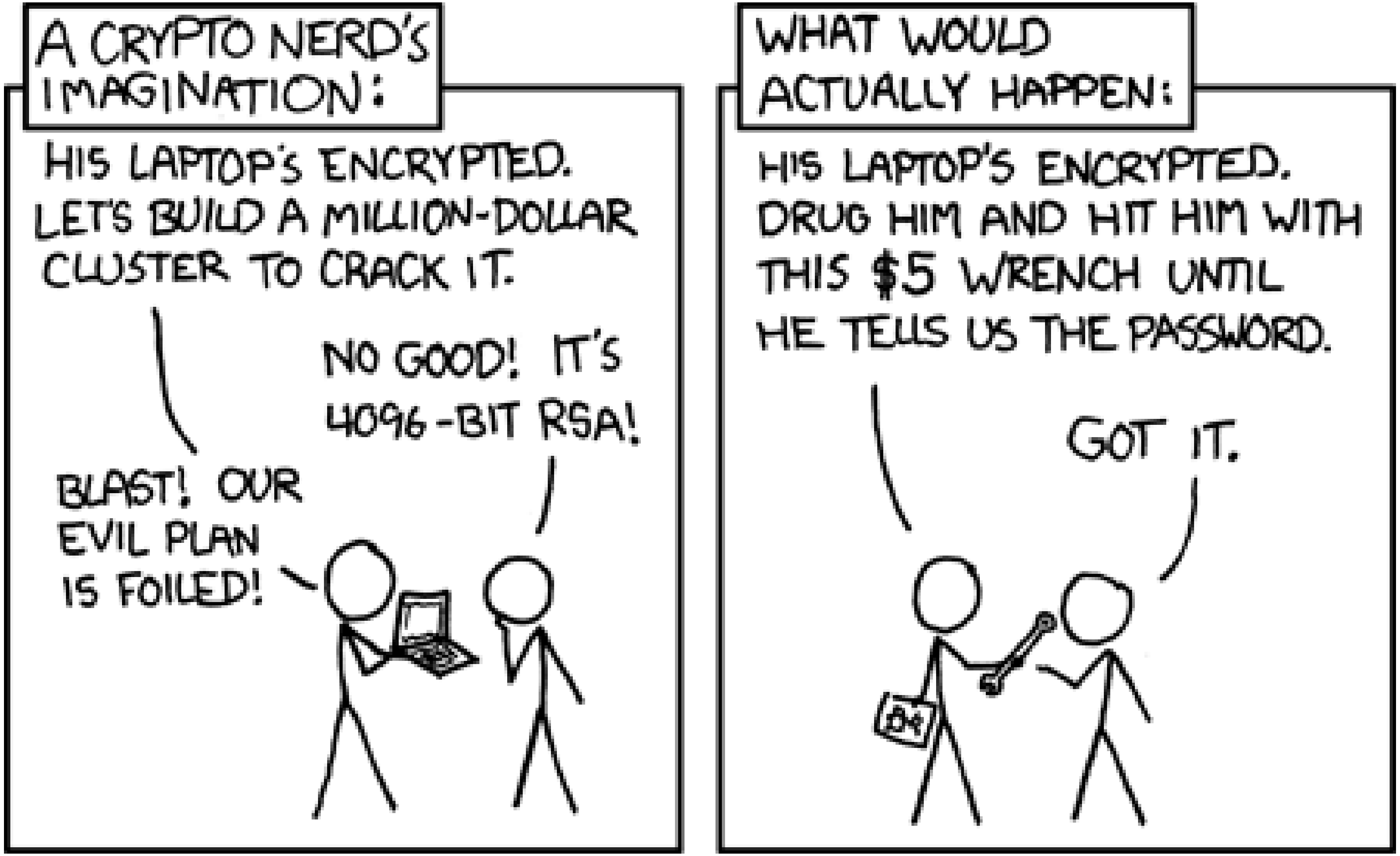
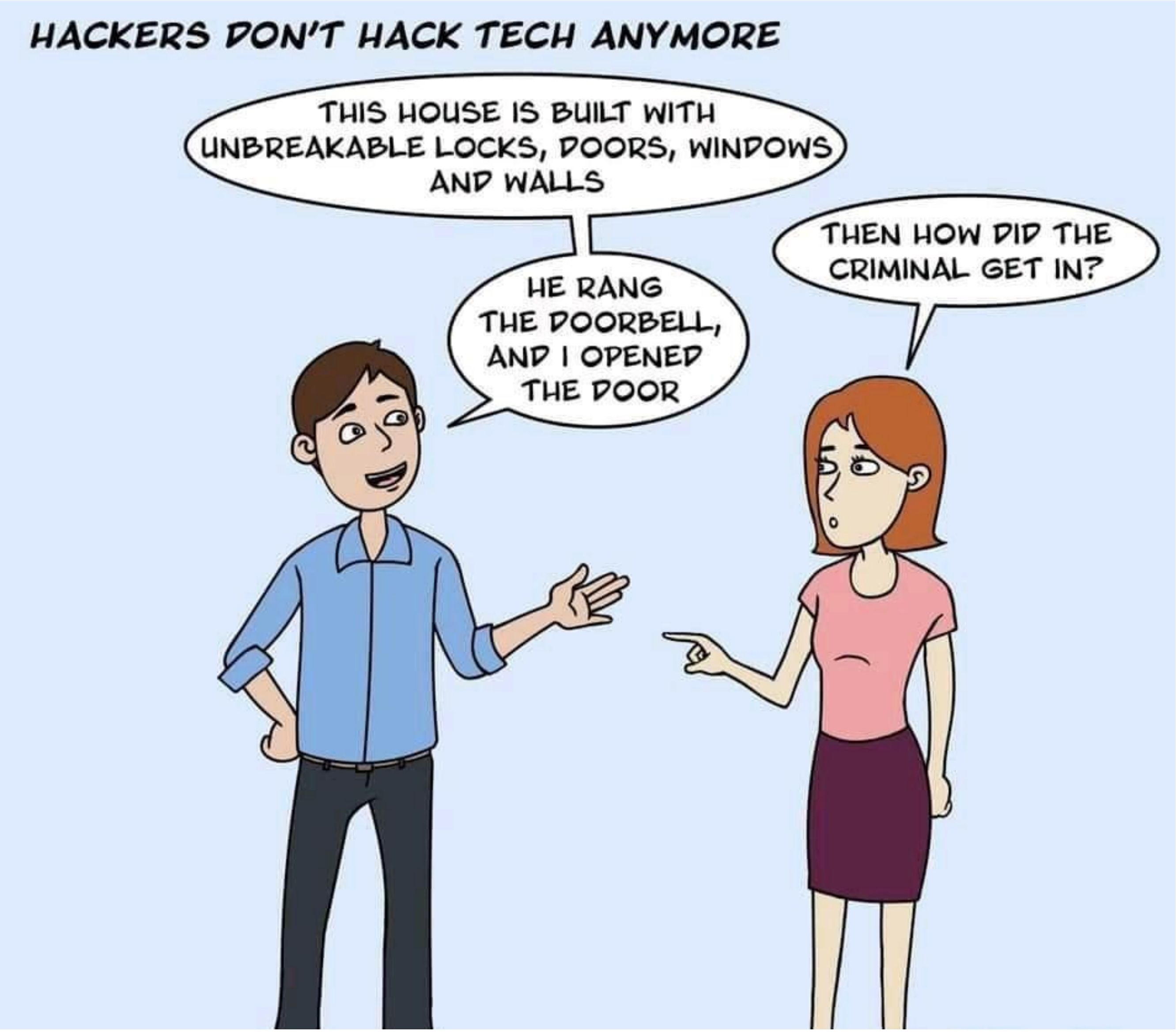
2550 Intro to cybersecurity

L13: Social Engineering

abhi shelat/Ran Cohen


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

https://xkcd.com/538/


HACKERS DON'T HACK TECH ANYMORE
THIS HOUSE IS BUILT WITH UNBREAKABLE LOCKS, DOORS, WINDOWS AND WALLS
THEN HOW DID THE CRIMINAL GET IN?
HE RANG THE DOORBELL, AND I OPENED THE DOOR

https://www.kratikal.com/blog/social-engineering-attack-hack-to-manipulate-human-psychology/

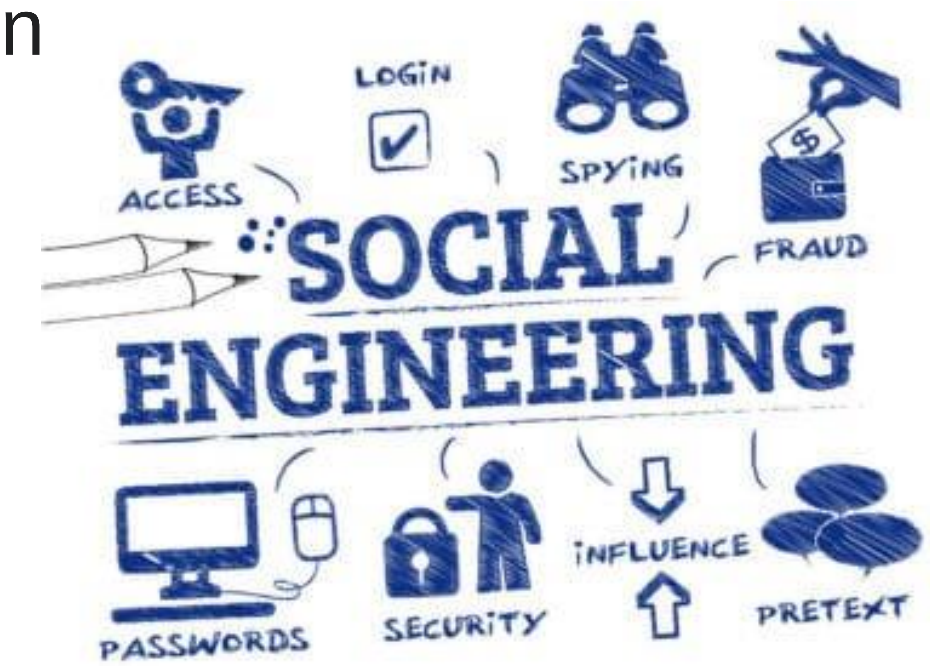
Social Engineering

A term used for a broad range of malicious activities accomplished through human interactions

Mainly using psychological manipulation to trick users into making security mistakes

- Disclose confidential/sensitive information
- Transfer money
- Enable access to restricted systems

Demonstration from Jimmy Kimmel
https://www.youtube.com/watch?v=opRMrEfAIiI

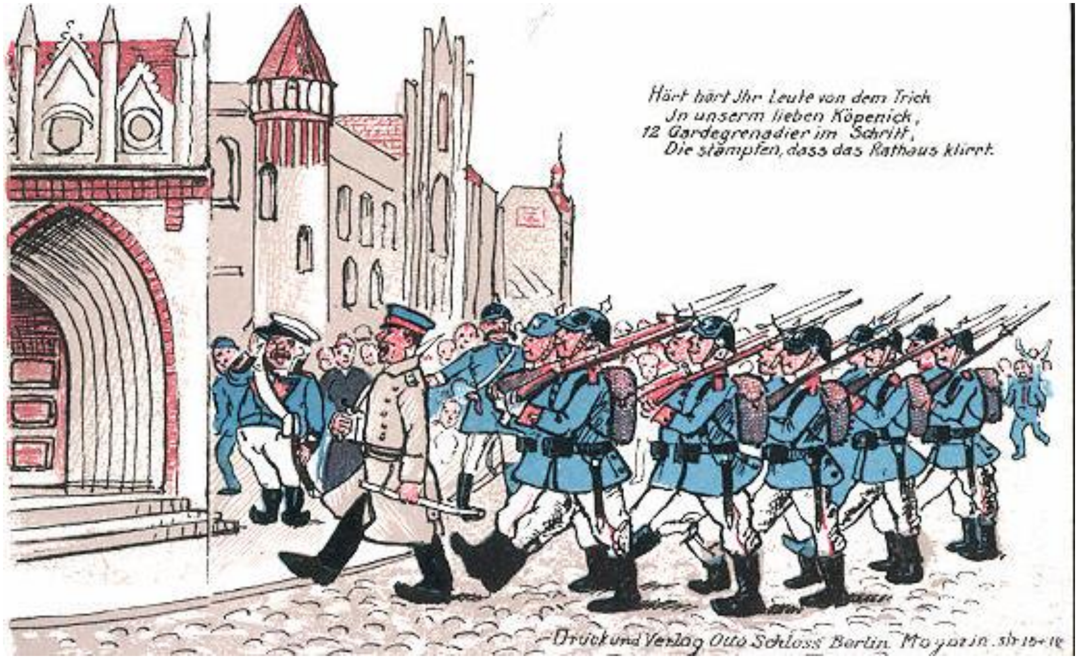


https://realsecure.ae/blog/social-engineering

Social engineering 100 years ago

In 1906 Friedrich Wilhelm Voigt, a shoemaker,

- Purchased a used military officer uniform
- Gathered 10 soldiers and took a train to Köpenick
- Arrested the mayor and treasurer for crooked bookkeeping
- Confiscated 4000 marks (left a receipt)
- When the police came he had them serve coffee to the soldiers

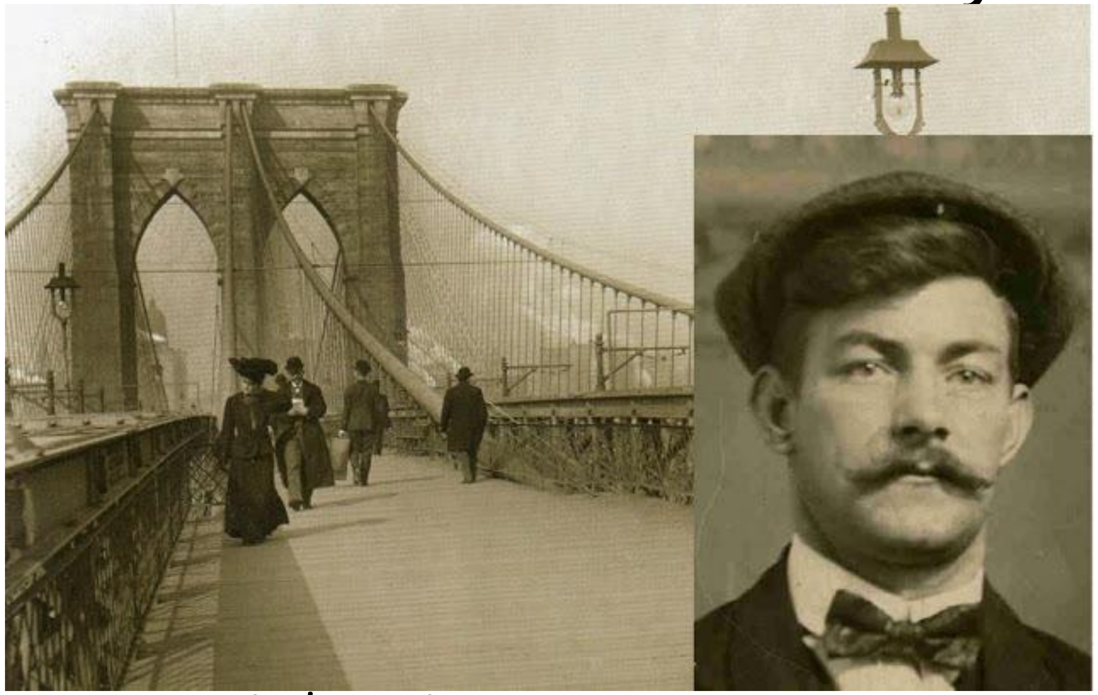

Hört hört Jhr Leute von dem Trick
Jn unserm lieben Köpenick,
12 Gardegrenadier im Schritt,
Die stampfen, dass das Rathaus klirrt.
Druck und Verlag Otto Schloss Berlin Moyerin.str 15+16

www.ak-ansichtskarten.de

Social engineering 100 years ago

In 1908 George C. Parker sold the Brooklyn bridge, several times

- Forged ownership documents
- Targeted newcomers to the ‘land of opportunity’
- Convinced his buyers they could control access to the roadway
- Buyers started collecting toll fees
- Also sold the Statue of Liberty, …



www.gangsterismout.com

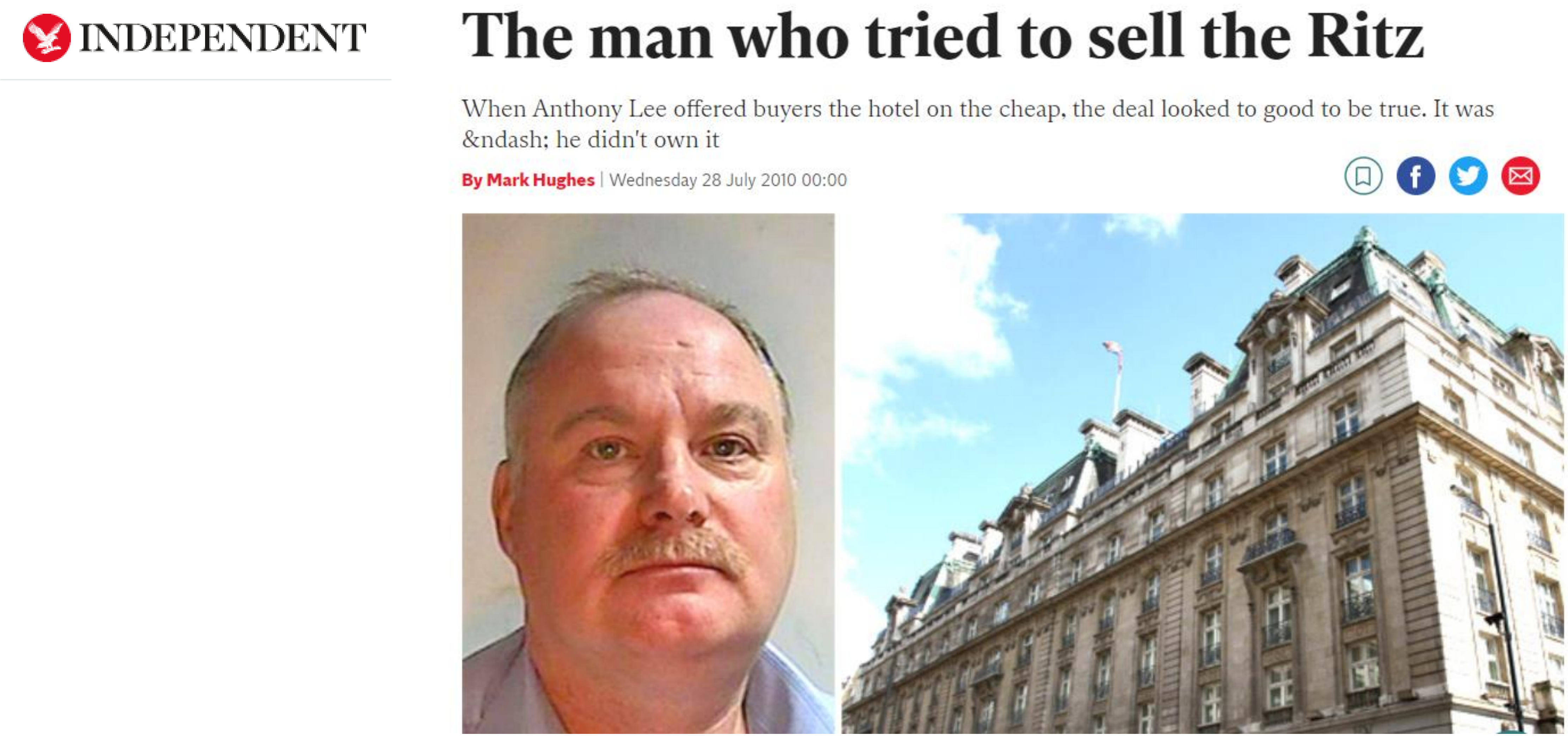
Social engineering 100 years ago

In 1925 Victor Lustig sold the Eiffel Tower, twice

- Read about the costly maintenance of the Eiffel tower
- Impersonated as a legitimate authority
- Forged official documents
- Profiling: targeted his victim
- Made an extremely good deal to the buyer

https://medium.com/

Social engineering 100 years ago



INDEPENDENT

The man who tried to sell the Ritz

When Anthony Lee offered buyers the hotel on the cheap, the deal looked to good to be true. It was &ndash; he didn't own it

By Mark Hughes | Wednesday 28 July 2010 00:00

Social engineering 50 years ago

Frank Abagnale impersonations in the ‘60s

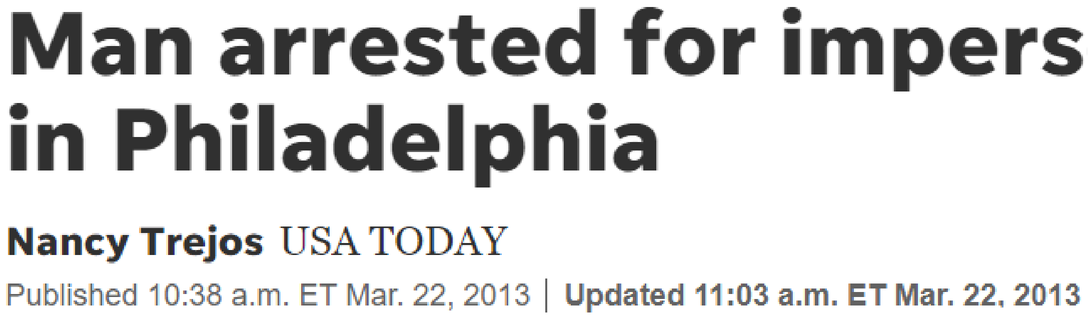
- Airline pilot at Pan Am
- TA at Brigham Young University
- Resident pediatrician in a Georgia hospital
- Forged a Harvard University law transcript and worked at the Louisiana State Attorney General's office

https://en.wikipedia.org/

Social engineering 50 years ago

www.taratara.com

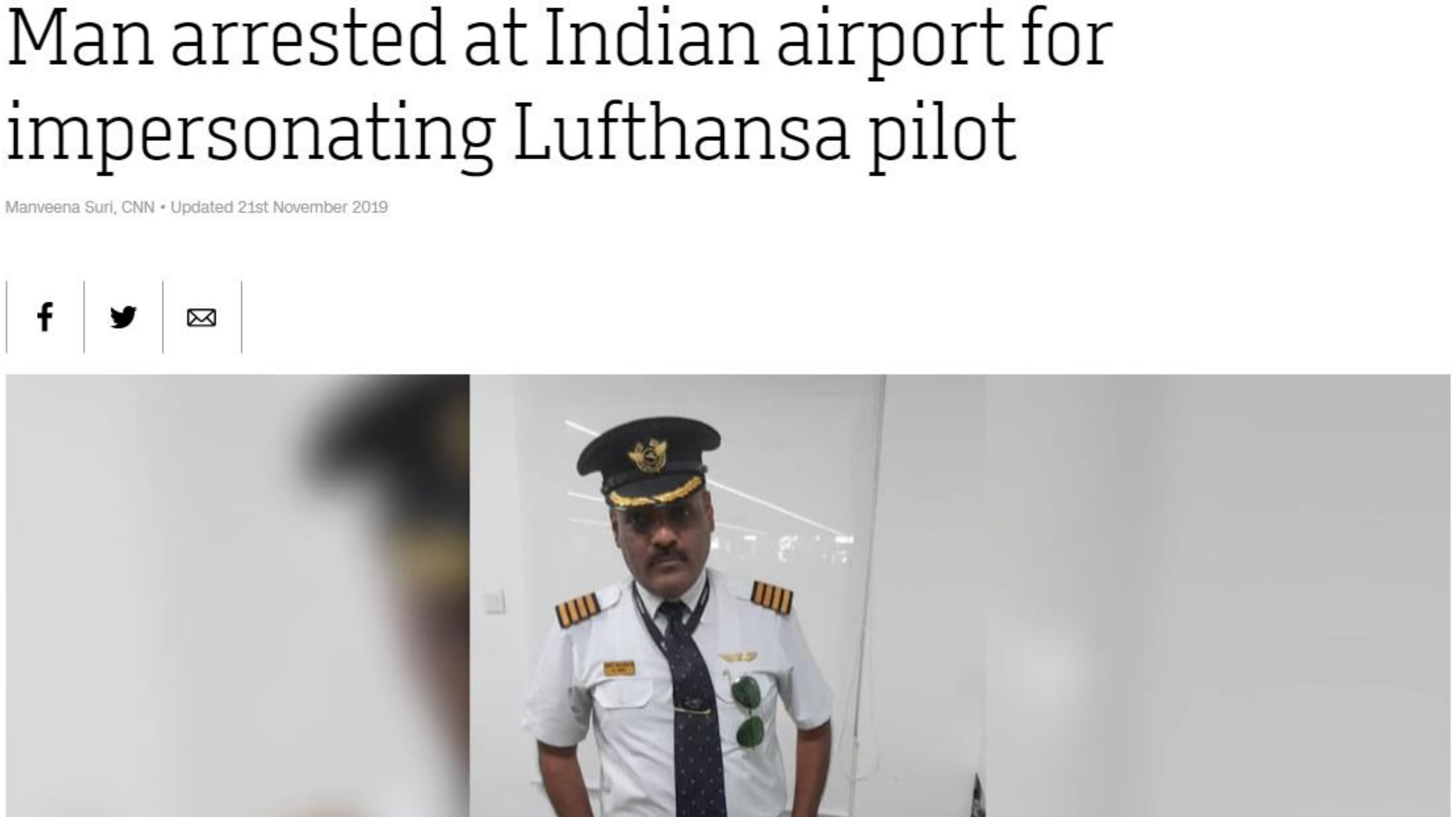
Social engineering 50 years ago



Man arrested for impersonating pilot in Philadelphia

Nancy Trejos USA TODAY

Published 10:38 a.m. ET Mar. 22, 2013 | **Updated 11:03 a.m. ET Mar. 22, 2013**



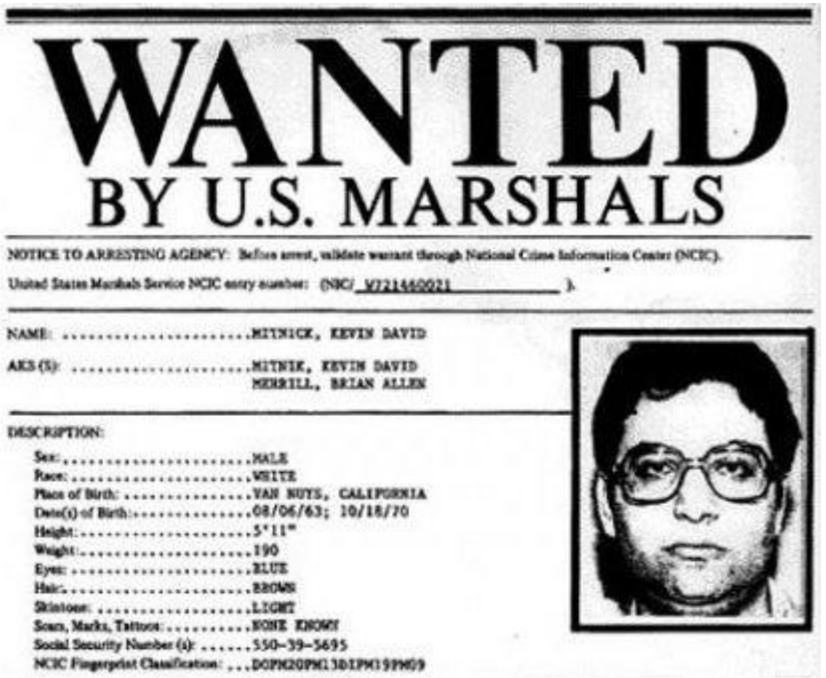
Man arrested at Indian airport for impersonating Lufthansa pilot

Manveena Suri, CNN • Updated 21st November 2019

Social engineering 30 years ago

Kevin Mitnick

- Most famous hacker in ’90s
- Termed ‘social engineering’ in the context of IT security
- Known for hacking phone companies, Pacific Bell
- High-profile arrest in 1995



WANTED

BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: ....MITNICK, KEVIN DAVID

AKS (S): ....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

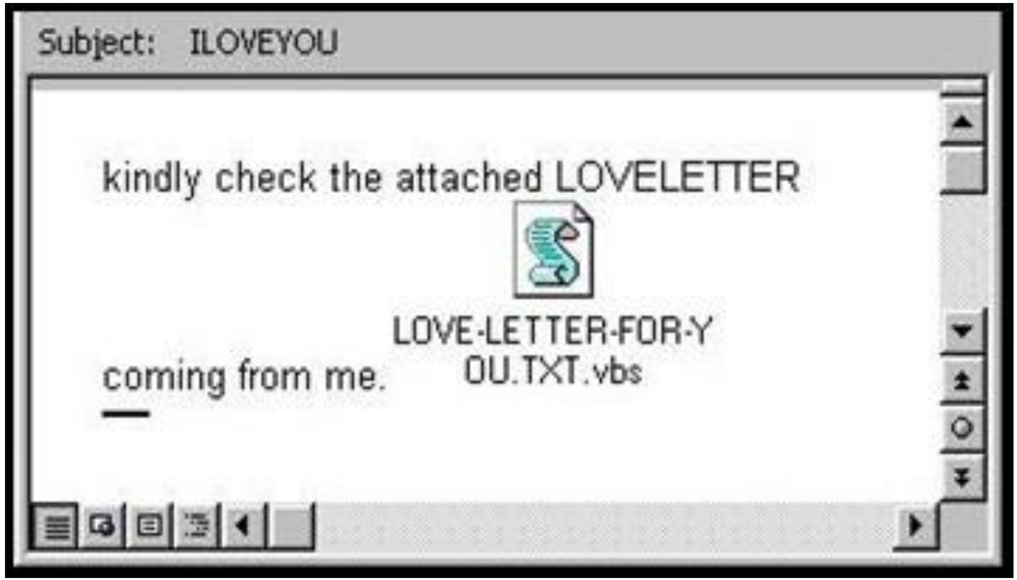
DESCRIPTION:

Sex: ....MALE
Race: ....WHITE
Place of Birth: ....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: ....5'11"
Weight: 190
Eyes: ....BLUE
Hair: ....BROWN
Skintone: ....LIGHT
Scars, Marks, Tattoos: ....NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19PM09

Social engineering 20 years ago

ILOVEYOU worm

- Spread via emails on May 4th, 2000
- Attachment: LOVE-LETTER-FOR-YOU.txt.vbs
- vbs extension was hidden in Windows by default
- Considered as 1st socially engineered computer virus
- Overwrote files
- Spread to all contacts
- Infected 10% of connected computers
- Over $5 billion damages



Subject: ILOVEYOU

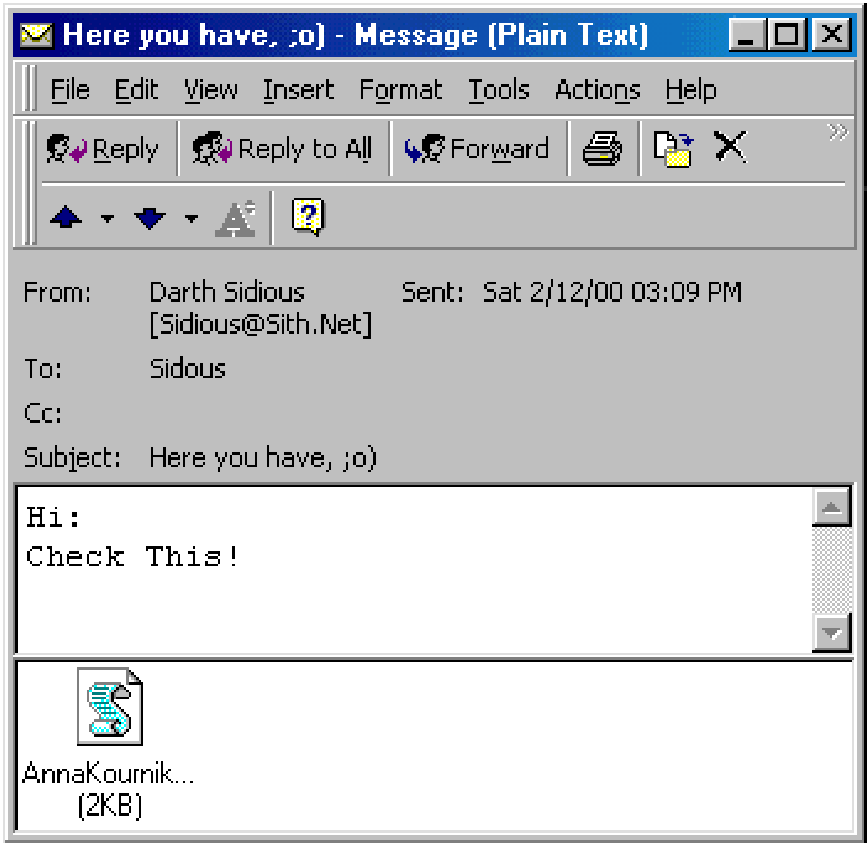
kindly check the attached LOVELETTER coming from me.

LOVE-LETTER-FOR-YOU.TXT.vbs

Social engineering 20 years ago

Anna Kournikova virus

- Spread via emails on Feb 11th, 2001
- Attachment: AnnaKournikova.jpg.vbs
- Very simple virus, written in hours
- No local damage, but mail servers crashed



Here you have, ;o) - Message (Plain Text)
File Edit View Insert Format Tools Actions Help
Reply
Reply to All
Forward

From: Darth Sidious [Sidious@Sith.Net]

Sent: Sat 2/12/00 03:09 PM

To: Sidous

Cc:

Subject: Here you have, ;o)

```
Hi:
Check This!
```

AnnaKournik...
(2KB)

Social Engineering Techniques

https://www.expressvpn.com/blog/the-art-of-social-engineering/

Baiting

Very simple physical attack

1) Preload USB keys with malware
2) Drop the keys in public, near victims
3) Wait for victims to pick up and plug in
4) Victim executes malware
   - Either by accident due to curiosity
   - Or autorun by the OS (e.g. Windows)

Baiting

Does dropping USB drives really work?

- Elie Bursztein, Black Hat 2016
- Dropped 297 USB sticks on the University of Illinois Urbana-Champaign campus
- “Solutions to final exam”
- 98% were picked up
- 45% were plugged in and someone clicked on files
- Black Hat presentation: https://www.youtube.com/watch?v=ZI5fvU5QKwQ

Baiting

- Stuxnet is a computer worm
- Targeted Iran’s nuclear program
- Discovered in 2010
- Very sophisticated (exploit four zero-day flaws)
- According to Snowden made by US and Israel
- Initially spread through infected USB flash drives

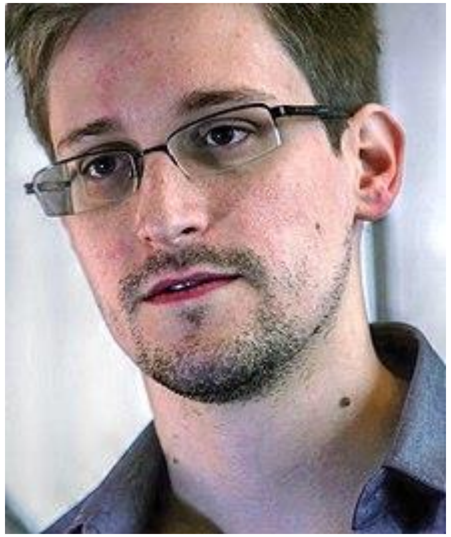
Quid Pro Quo

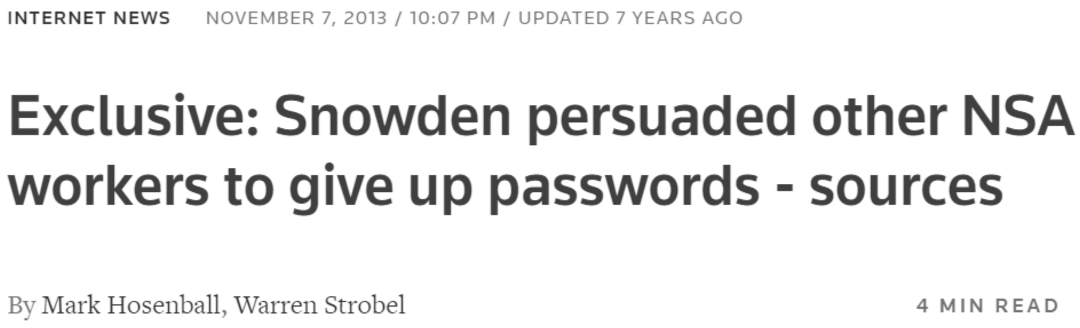
- The attacker provides a service, whereas baiting usually takes the form of a good.
- Impersonate as a government entity
  and ask to confirm the SSN
  for the purpose of committing identity theft.
- People would give their password for chocolate

www.digitalnewsasia.com

Quid Pro Quo

- Edward Snowden is an ex-contractor for NSA
- Since 2013 he published thousands of super-secret classified NSA documents
- When stationed in a spy base in Hawaii, 20-25 NSA employees gave their passwords to Snowden
- Snowden convinced them he needed the login details to do his job as a systems admin





INTERNET NEWS NOVEMBER 7, 2013 / 10:07 PM / UPDATED 7 YEARS AGO

Exclusive: Snowden persuaded other NSA workers to give up passwords - sources

By Mark Hosenball, Warren Strobel

4 MIN READ

Dumpster diving

Going through trashcans and dumpsters looking for information

- IP addresses, usernames, passwords, emails
- Medical records, resumes, bank statements
- Old computers

www.thebalancesmb.com

http://www.subliminalhacking.net/

Dumpster diving

ONLY ON 4
MEDICAL RECORDS FOUND IN DUMPSTER
HAMPTON TOWNSHIP, ALLEGHENY COUNTY
PITTSBURGH'S
ACTION NEWS 4

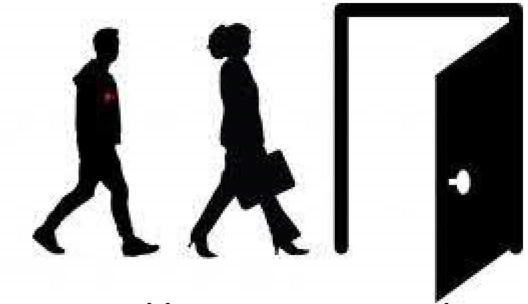
Pittsburgh’s Action News 4, 2017

Tailgaiting / Piggybacking

Enable an attacker entering a restricted area

- Walk behind an authorized person
- Impersonate delivery man holding packages asking to hold the door
- Join smokers next to a side door

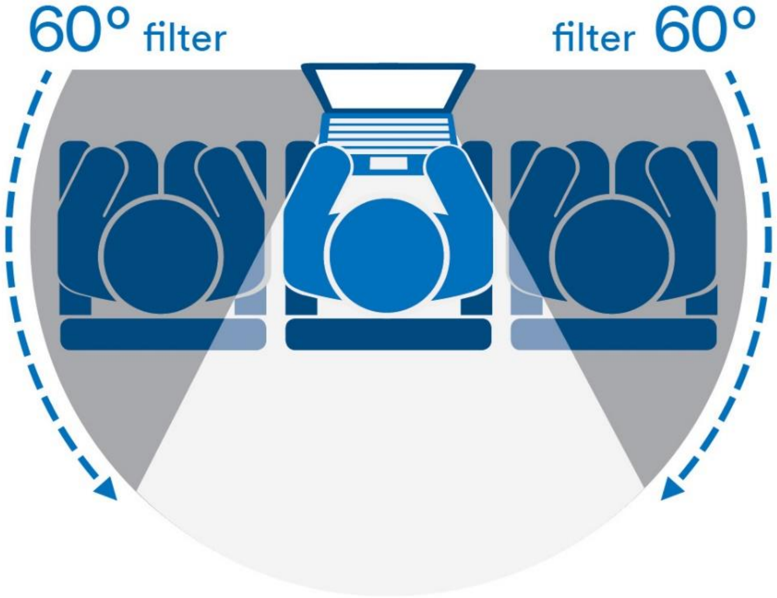
Once in the building can access to internal networks, workstations, etc.



https://trustaira.com/

https://en.wikipedia.org/

Shoulder surfing



Private screens, www.3m.com

https://travelskills.com/

Pretexting

- Manipulate victims into divulging sensitive information
- Creating false trust
- Email from head of IT support
- Illustration: https://www.youtube.com/watch?v=BIIvsJ3yi8o

Hi Amy,
This is Joe, from
IT...I'm working from
home today...

infosightinc.com

Phishing

- Attempt to steal users' sensitive data
- E.g., login credentials, credit card numbers, SSN, bank accounts, etc.
- Spreads via emails, SMS, IM, social media
- The recipient is tricked into clicking a malicious link:
  - Install malware
  - Redirect to malicious website

www.123rf.com

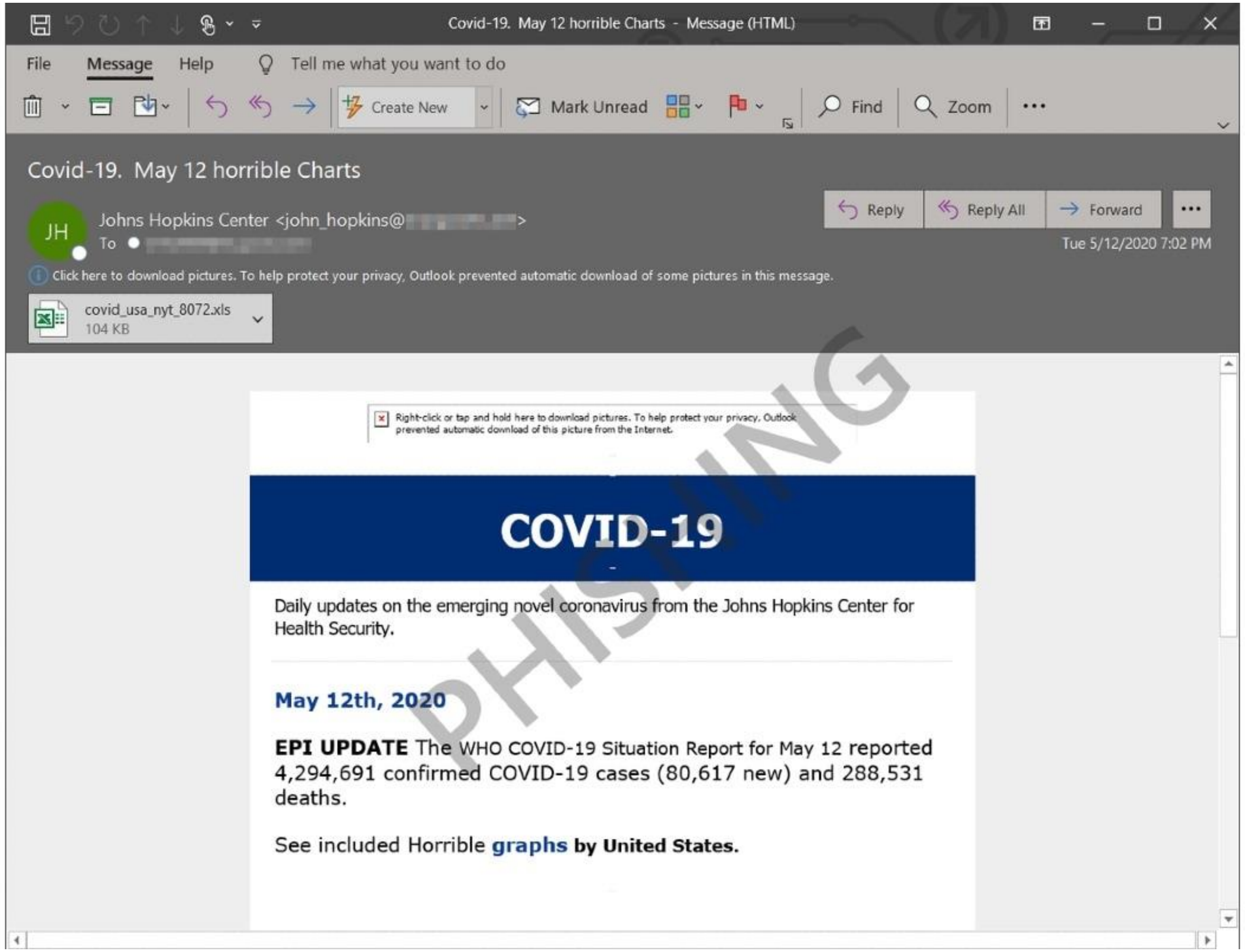
Phishing

- Most common form of social engineering cyber attack
- In 2014:
  - 90% of all emails are spam
  - 77% of SE-based attacks rely on phishing
  - 88% of recorded phishing involve clicking links in emails

https://www.social-engineer.org/social-engineering/social-engineering-infographic/

Phishing

- In April/May 2020, Microsoft discovered a phishing campaign based on COVID-19


Covid-19. May 12 horrible Charts - Message (HTML)
File
Message
Help
Tell me what you want to do
Create New
Mark Unread
Find
Zoom
Reply
Reply All
Forward
PHISHING

Covid-19. May 12 horrible Charts

JH Johns Hopkins Center <john_hopkins@[redacted]>

To [redacted]

Tue 5/12/2020 7:02 PM

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

covid_usa_nyt_8072.xls
104 KB

☒ Right-click or tap and hold here to download pictures. To help protect your privacy, Outlook prevented automatic download of this picture from the Internet.

COVID-19

Daily updates on the emerging novel coronavirus from the Johns Hopkins Center for Health Security.

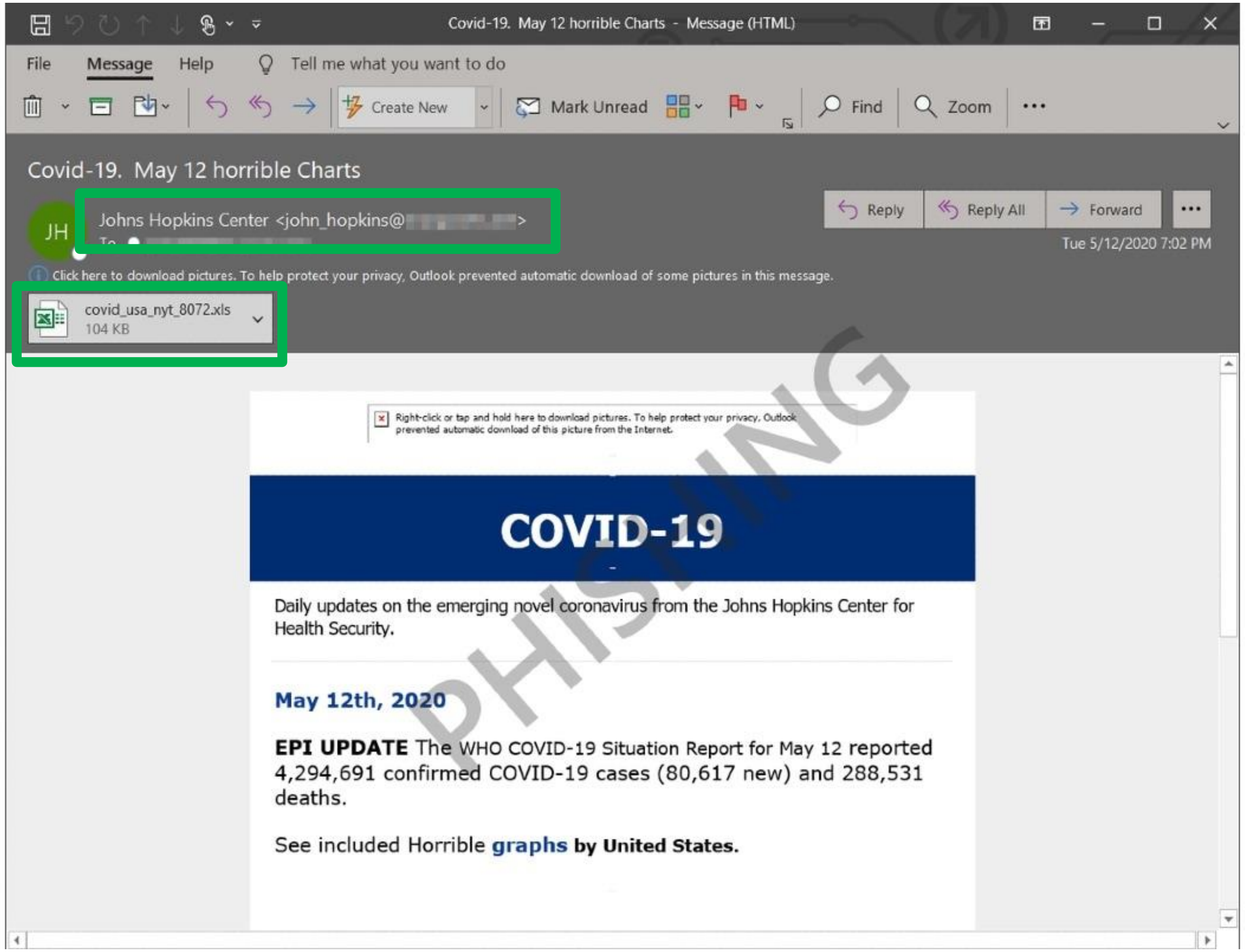
May 12th, 2020

EPI UPDATE The WHO COVID-19 Situation Report for May 12 reported 4,294,691 confirmed COVID-19 cases (80,617 new) and 288,531 deaths.

See included Horrible **graphs by United States.**

Phishing

- In April/May 2020, Microsoft discovered a phishing campaign based on COVID-19
- Opening the Excel file opens a pop-up to enable macros
- Accepting installs a RAT (Remote Access Trojan)


Covid-19. May 12 horrible Charts - Message (HTML)
File
Message
Help
Tell me what you want to do
Create New
Mark Unread
Find
Zoom
Reply
Reply All
Forward
PHISHING

Covid-19. May 12 horrible Charts

JH Johns Hopkins Center <john_hopkins@[redacted]>

To [redacted]

Tue 5/12/2020 7:02 PM

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

covid_usa_nyt_8072.xls
104 KB

Right-click or tap and hold here to download pictures. To help protect your privacy, Outlook prevented automatic download of this picture from the Internet.

COVID-19

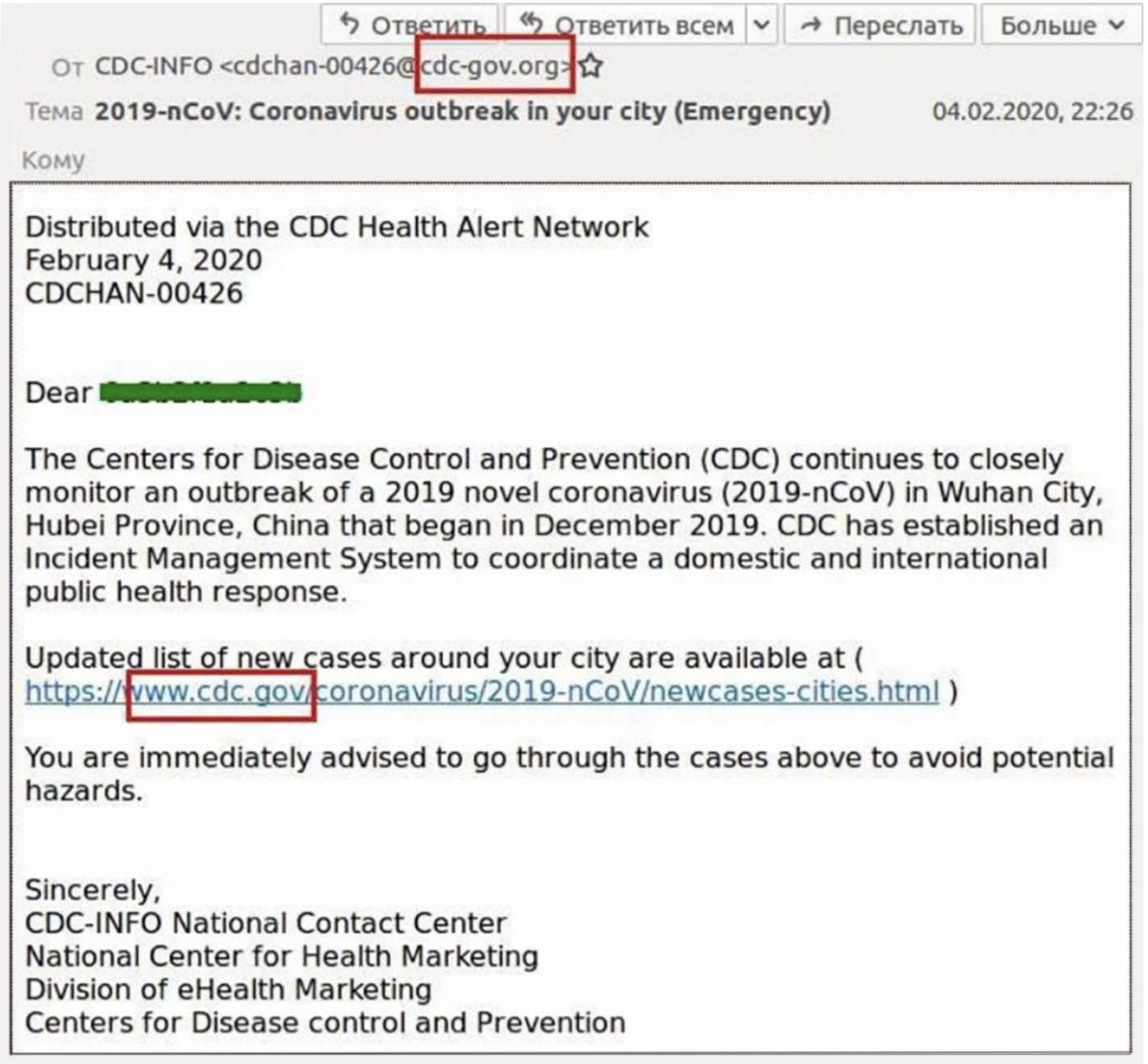
Daily updates on the emerging novel coronavirus from the Johns Hopkins Center for Health Security.

May 12th, 2020

EPI UPDATE The WHO COVID-19 Situation Report for May 12 reported 4,294,691 confirmed COVID-19 cases (80,617 new) and 288,531 deaths.

See included Horrible **graphs by United States.**

Phishing



От CDC-INFO <cdchan-00426@cdc-gov.org>

Тема **2019-nCoV: Coronavirus outbreak in your city (Emergency)** 04.02.2020, 22:26

Кому

Distributed via the CDC Health Alert Network
February 4, 2020
CDCHAN-00426

Dear [redacted]

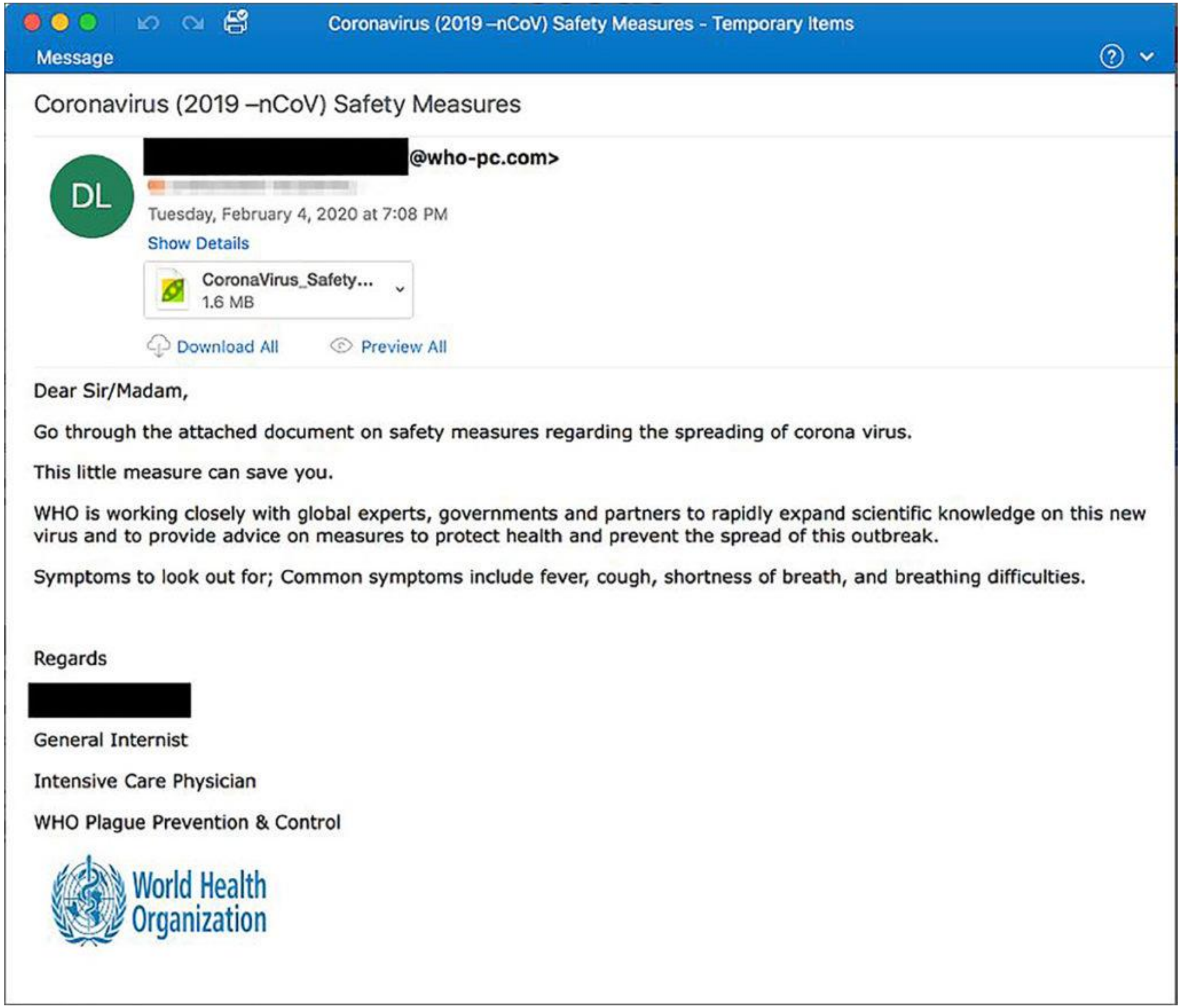
The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above to avoid potential hazards.

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention

Phishing



Coronavirus (2019 –nCoV) Safety Measures - Temporary Items
Message
DL
Show Details
CoronaVirus_Safety...
1.6 MB
Download All
Preview All
World Health Organization

Coronavirus (2019 –nCoV) Safety Measures

[redacted]@who-pc.com>

[redacted]

Tuesday, February 4, 2020 at 7:08 PM

Dear Sir/Madam,

Go through the attached document on safety measures regarding the spreading of corona virus.

This little measure can save you.

WHO is working closely with global experts, governments and partners to rapidly expand scientific knowledge on this new virus and to provide advice on measures to protect health and prevent the spread of this outbreak.

Symptoms to look out for; Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards

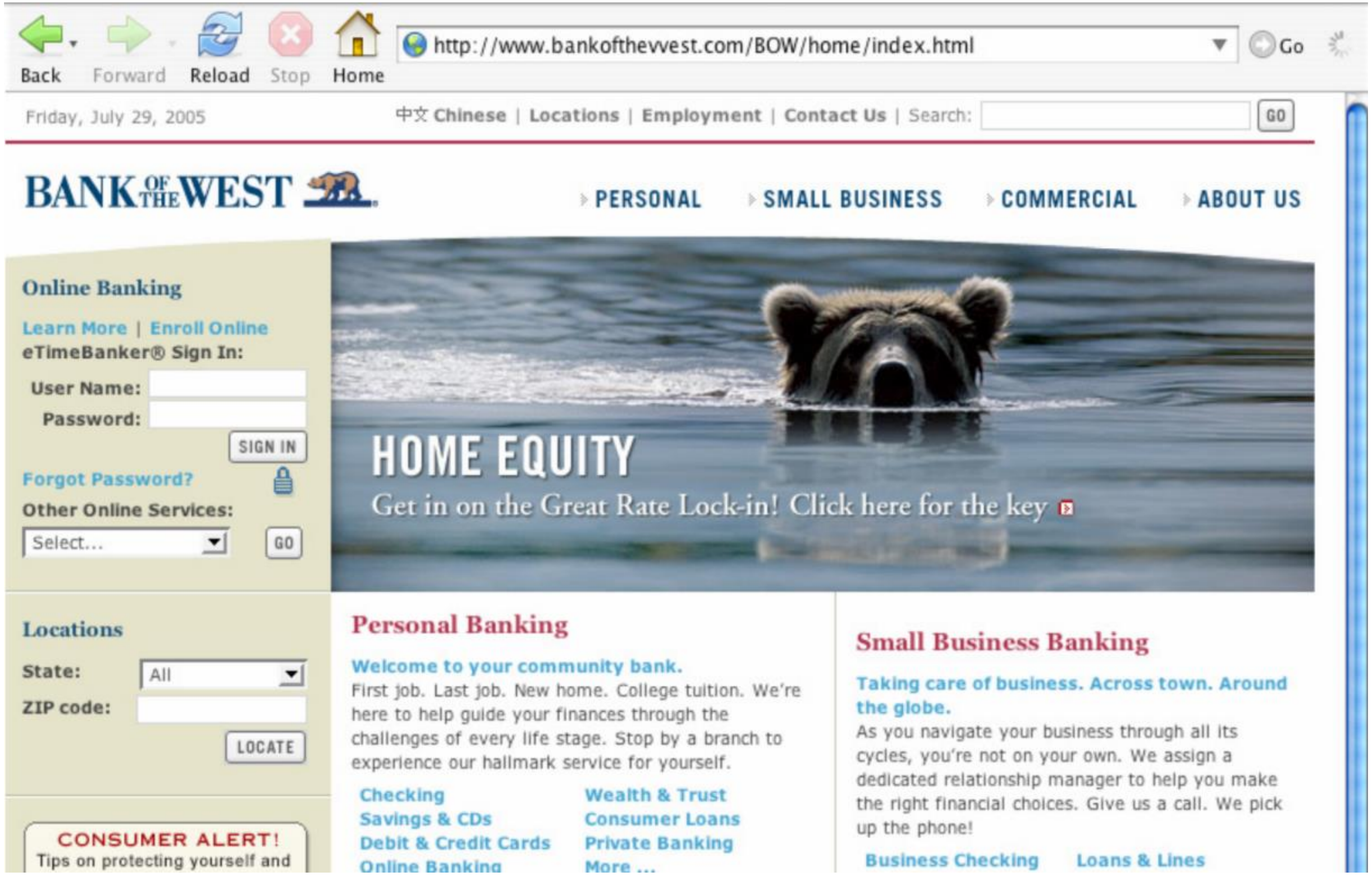
[redacted]

General Internist

Intensive Care Physician

WHO Plague Prevention & Control

Phishing



http://www.bankofthevvest.com/BOW/home/index.html

Friday, July 29, 2005

中文 Chinese | Locations | Employment | Contact Us | Search:
GO
BANK OF THE WEST
PERSONAL
SMALL BUSINESS
COMMERCIAL
ABOUT US

Online Banking

eTimeBanker® Sign In:

User Name:

Password:

Other Online Services:

HOME EQUITY

Get in on the Great Rate Lock-in! Click here for the key

Locations

State: All

ZIP code:

CONSUMER ALERT!

Tips on protecting yourself and

Personal Banking

Welcome to your community bank.

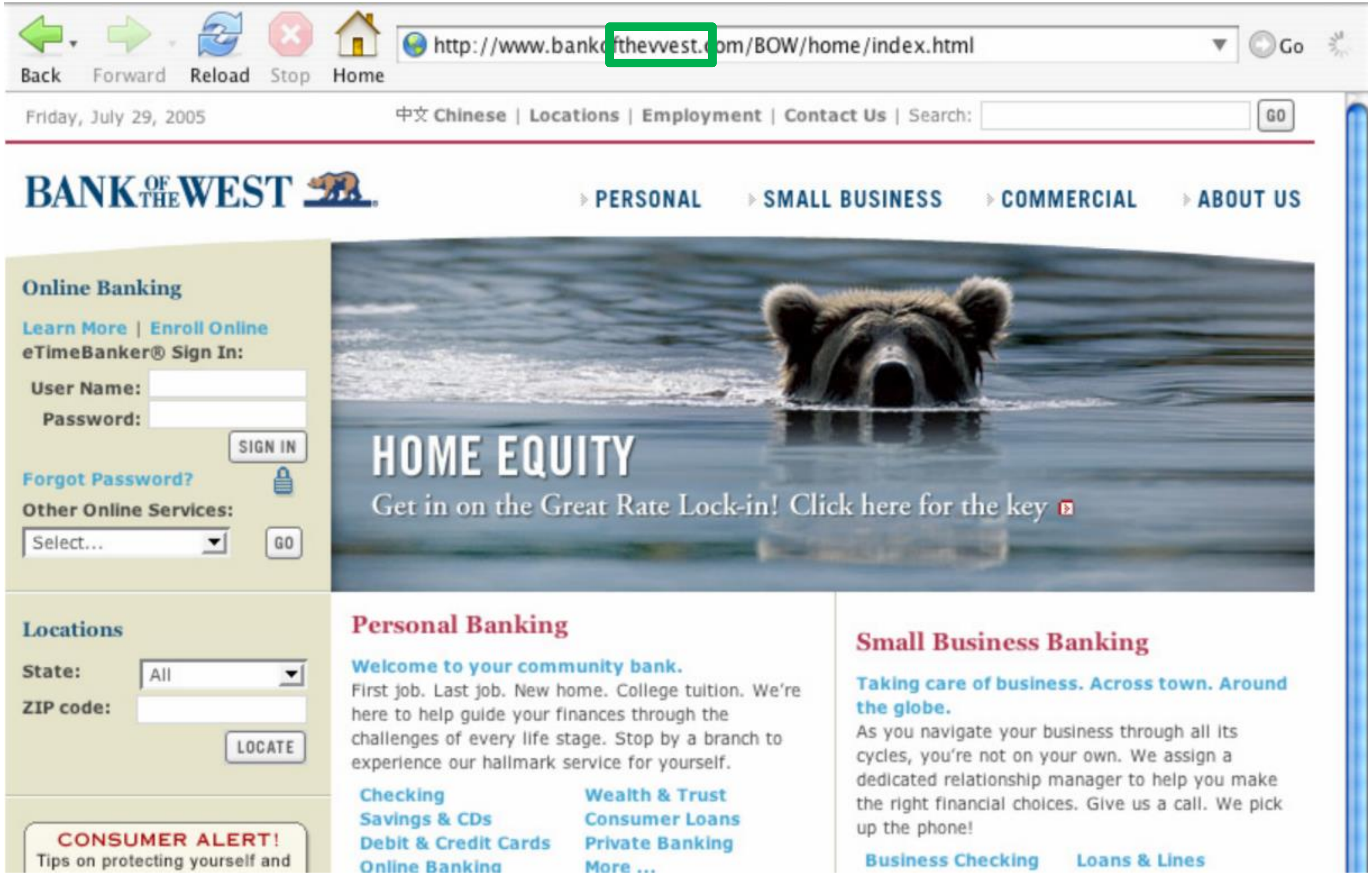
First job. Last job. New home. College tuition. We're here to help guide your finances through the challenges of every life stage. Stop by a branch to experience our hallmark service for yourself.

Small Business Banking

Taking care of business. Across town. Around the globe.

As you navigate your business through all its cycles, you're not on your own. We assign a dedicated relationship manager to help you make the right financial choices. Give us a call. We pick up the phone!

Phishing



http://www.bankofthevvest.com/BOW/home/index.html

Friday, July 29, 2005

Online Banking

Learn More | Enroll Online

eTimeBanker® Sign In:

User Name:

Password:

Forgot Password?

Other Online Services:

Get in on the Great Rate Lock-in! Click here for the key

Locations

State: All

ZIP code:

CONSUMER ALERT!
Tips on protecting yourself and

Personal Banking

Welcome to your community bank.

First job. Last job. New home. College tuition. We're here to help guide your finances through the challenges of every life stage. Stop by a branch to experience our hallmark service for yourself.

Checking
Savings & CDs
Debit & Credit Cards
Online Banking
Wealth & Trust
Consumer Loans
Private Banking
More ...

Small Business Banking

Taking care of business. Across town. Around the globe.

As you navigate your business through all its cycles, you're not on your own. We assign a dedicated relationship manager to help you make the right financial choices. Give us a call. We pick up the phone!

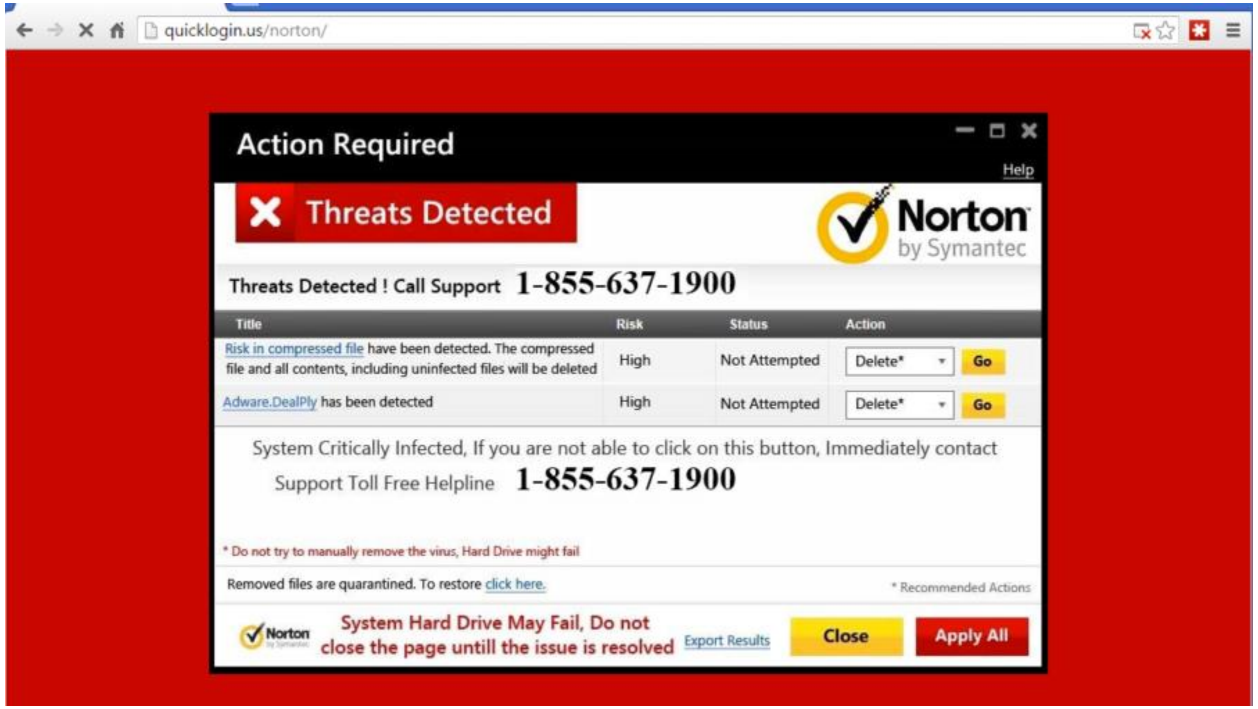
Business Checking
Loans & Lines

Phishing

https://www.phishingbox.com/phishing-test

Vishing

- Phone-based phishing
- Using caller-id spoofing
- Get the target to call a bogus 1-800 number



Action Required

Threats Detected

Threats Detected ! Call Support 1-855-637-1900

Title	Risk	Status	Action
Risk in compressed file have been detected. The compressed file and all contents, including uninfected files will be deleted	High	Not Attempted	Delete* Go
Adware.DealPly has been detected	High	Not Attempted	Delete* Go

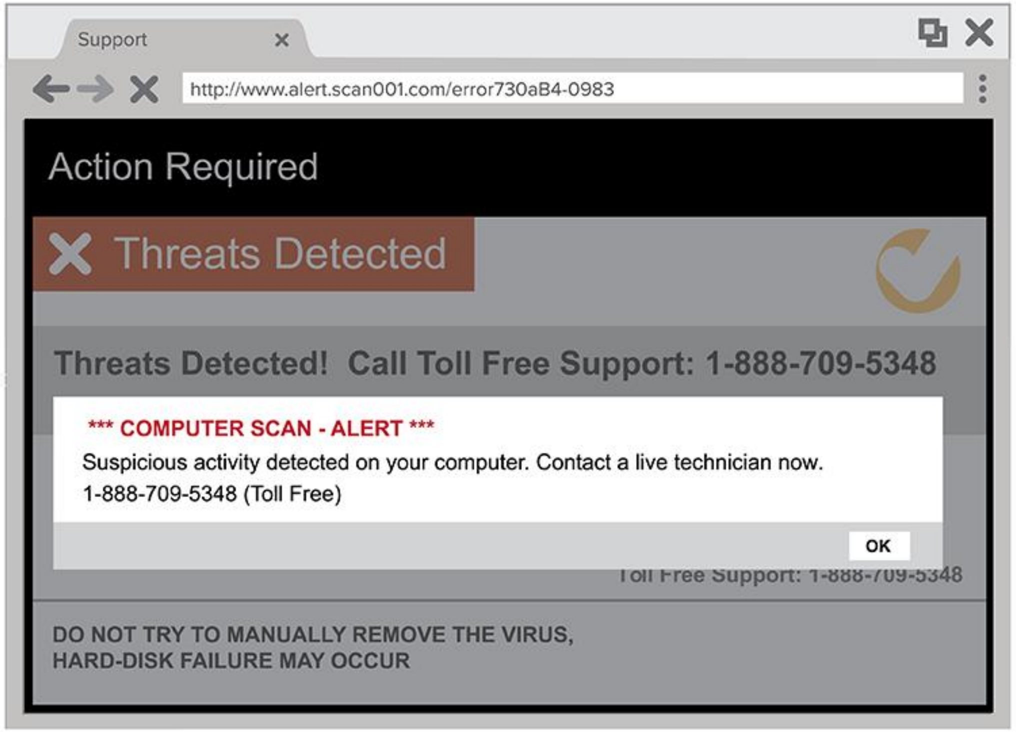
System Critically Infected, If you are not able to click on this button, Immediately contact Support Toll Free Helpline 1-855-637-1900

* Do not try to manually remove the virus, Hard Drive might fail

Removed files are quarantined. To restore click here.

* Recommended Actions

System Hard Drive May Fail, Do not close the page untill the issue is resolved



Action Required

Threats Detected

Threats Detected! Call Toll Free Support: 1-888-709-5348

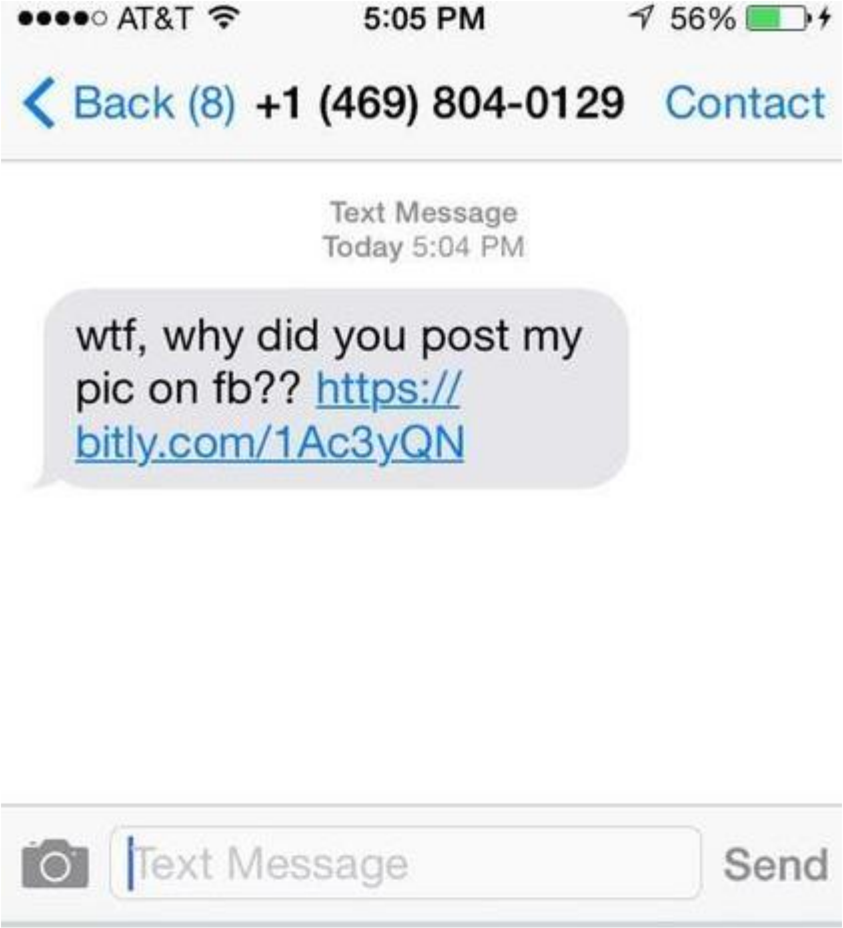
*** COMPUTER SCAN - ALERT ***

Suspicious activity detected on your computer. Contact a live technician now.
1-888-709-5348 (Toll Free)

Toll Free Support: 1-888-709-5348

DO NOT TRY TO MANUALLY REMOVE THE VIRUS,
HARD-DISK FAILURE MAY OCCUR

SMiShing



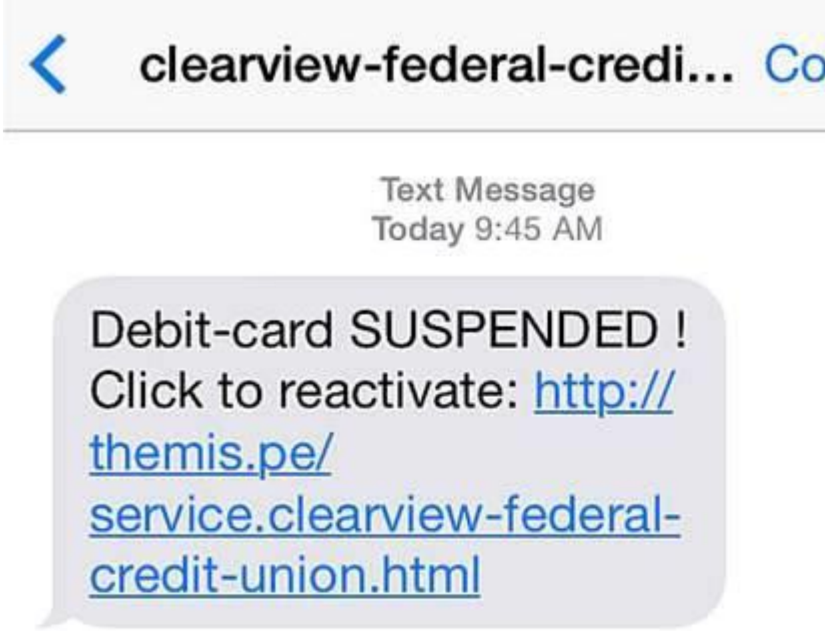
●●●●○ AT&T 5:05 PM 56%

Back (8) +1 (469) 804-0129 Contact

Text Message
Today 5:04 PM

wtf, why did you post my pic on fb?? https://bitly.com/1Ac3yQN

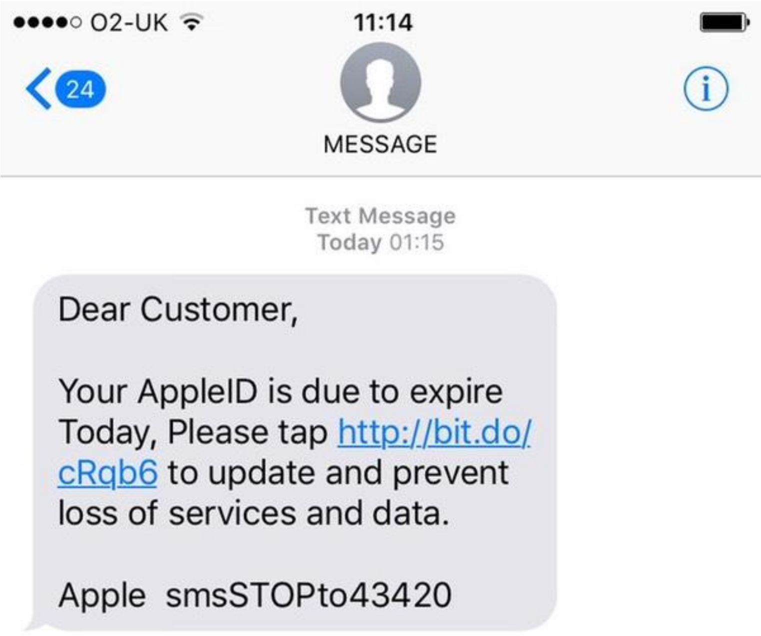
Text Message Send



clearview-federal-credi… Contact

Text Message
Today 9:45 AM

Debit-card SUSPENDED !
Click to reactivate: http://themis.pe/service.clearview-federal-credit-union.html



●●●●○ O2-UK 11:14

24

MESSAGE

Text Message
Today 01:15

Dear Customer,

Your AppleID is due to expire Today, Please tap http://bit.do/cRqb6 to update and prevent loss of services and data.

Apple smsSTOPto43420

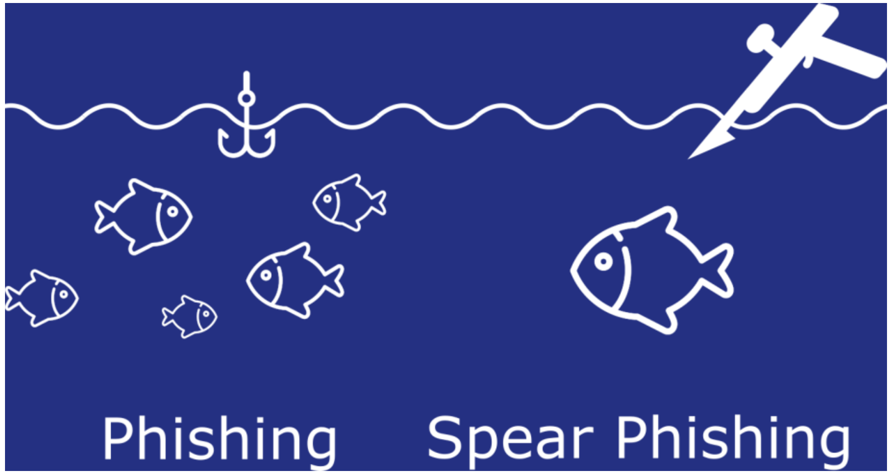
numbercop.tumblr.com

Water-hole attack

- “Phishing without a lure”
- Monitor which websites the targets browse
- If those websites are vulnerable infect them
- 2012 US Council on Foreign Relations was infected with 0-day vulnerability in Internet Explorer
  Triggered when language was set to English, Chinese, Japanese, Korean and Russian
- 2015 attack on Forbes.com showed malicious versions of ‘Thought of the Day’ leveraging 2 zero-day vulnerabilities (Internet Explorer & Flash)

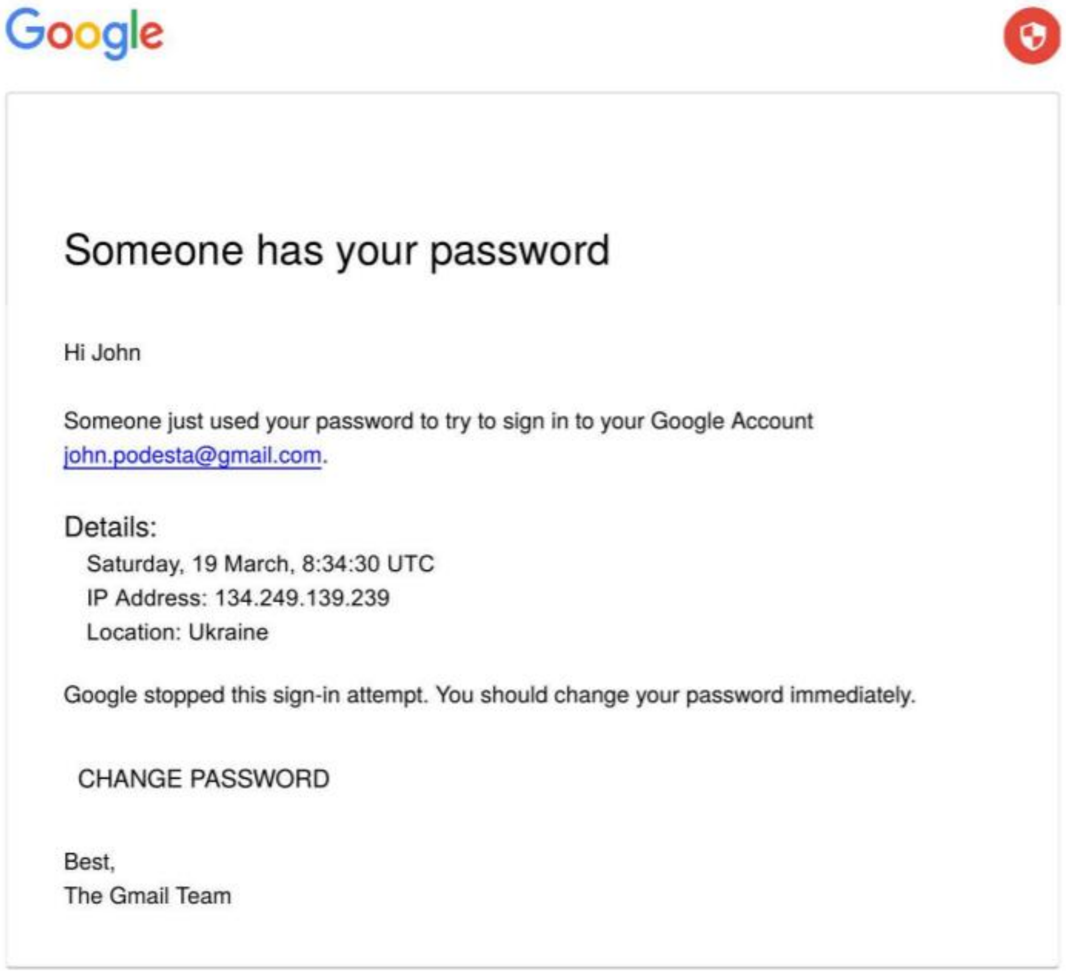
Spear Phishing

- Highly targeted phishing attack
- Involves a lot of background research: social media, corporate websites, publicly available information
- Does not trigger spam filters
- Very challenging to detect by people and anomaly detectors
- May be sent from hacked, legit email accounts



John Podesta Phishing Email

- Campaign manager of Hillary Clinton
- On March 19, 2016 received a Google security alert
- This was a spear-fishing attack by Russian intelligence



Someone has your password

Hi John

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

Details:

Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

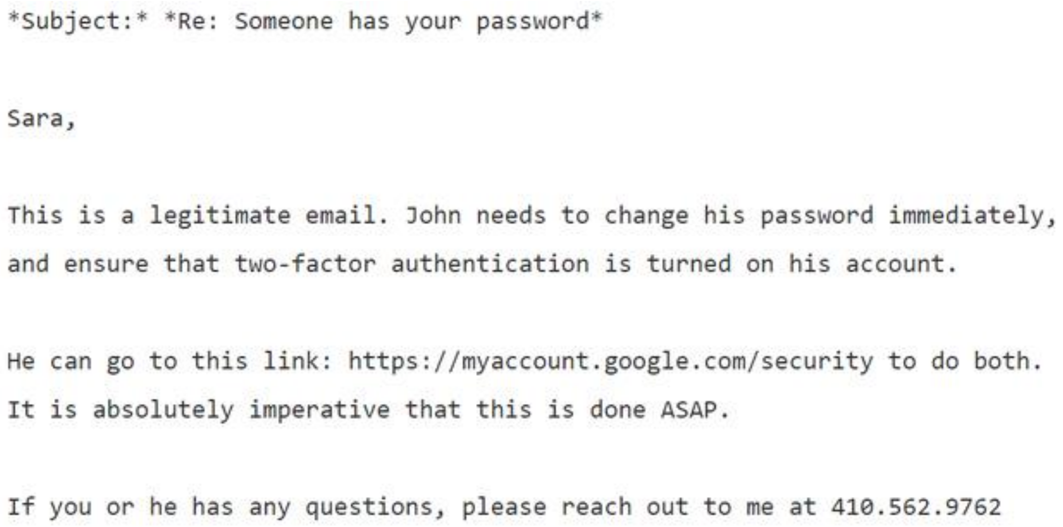
Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD

Best,
The Gmail Team

John Podesta Phishing Email

- Campaign manager of Hillary Clinton
- On March 19, 2016 received a Google security alert
- This was a spear-fishing attack by Russian intelligence
- Podesta forward the email to his chief of staff, Sara Latham, who asked IT support



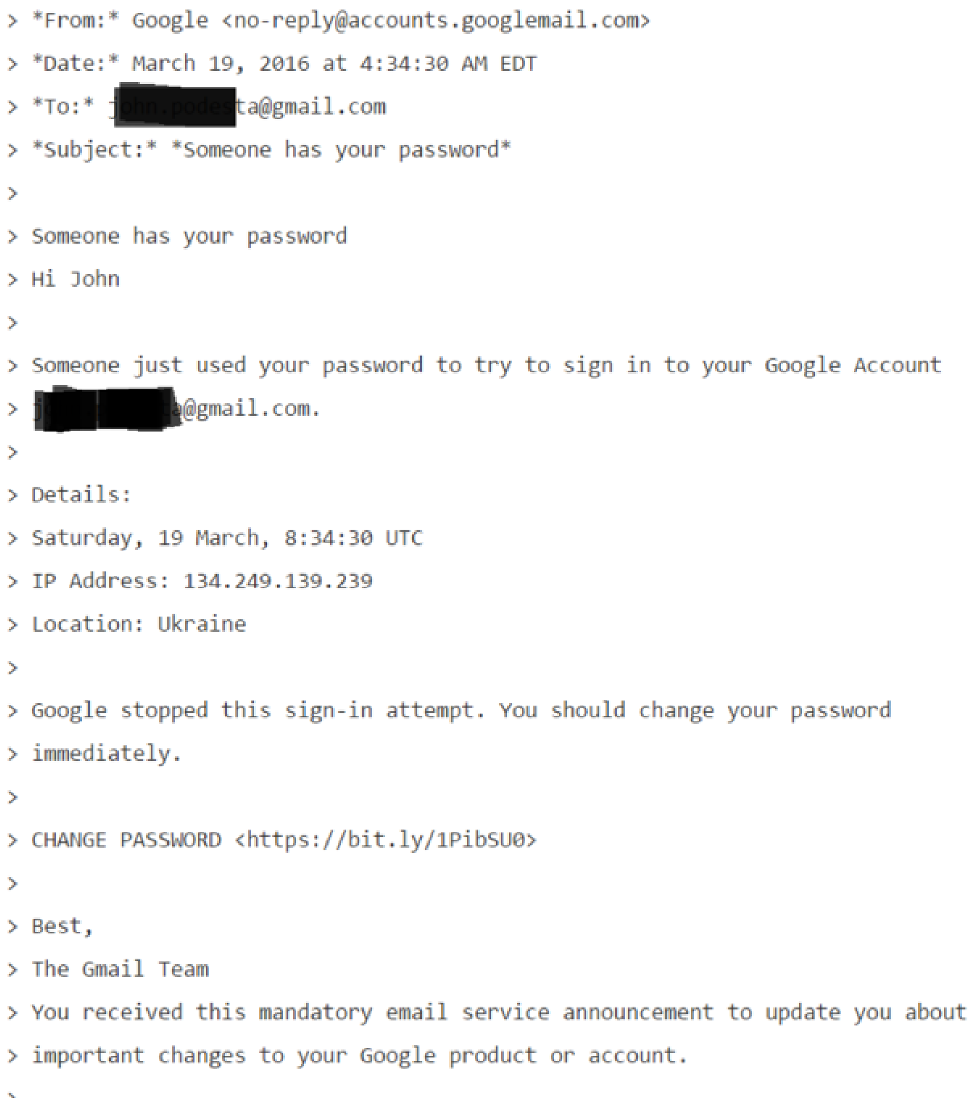
```
*Subject:* *Re: Someone has your password*

Sara,

This is a legitimate email. John needs to change his password immediately,
and ensure that two-factor authentication is turned on his account.

He can go to this link: https://myaccount.google.com/security to do both.
It is absolutely imperative that this is done ASAP.

If you or he has any questions, please reach out to me at 410.562.9762
```

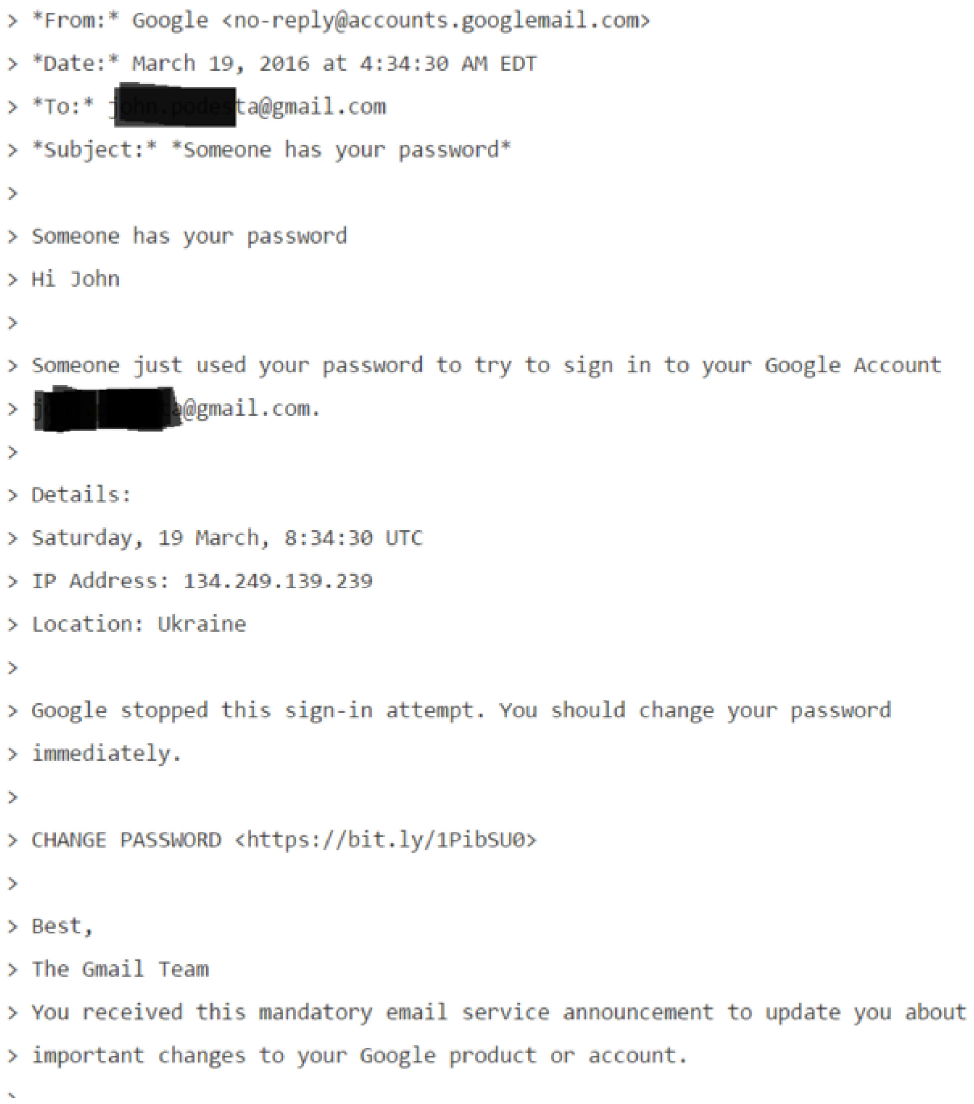


```
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* [redacted]ta@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [redacted]@gmail.com.
>
> 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.
```

www.cbsnews.com

John Podesta Phishing Email

- Campaign manager of Hillary Clinton
- On March 19, 2016 received a Google security alert
- This was a spear-fishing attack by Russian intelligence
- Podesta forward the email to his chief of staff, Sara Latham, who asked IT support
- IT erroneously responded ‘this is a legitimate email’
- Account compromised, emails dumped to Wikileaks
- Massive political scandal

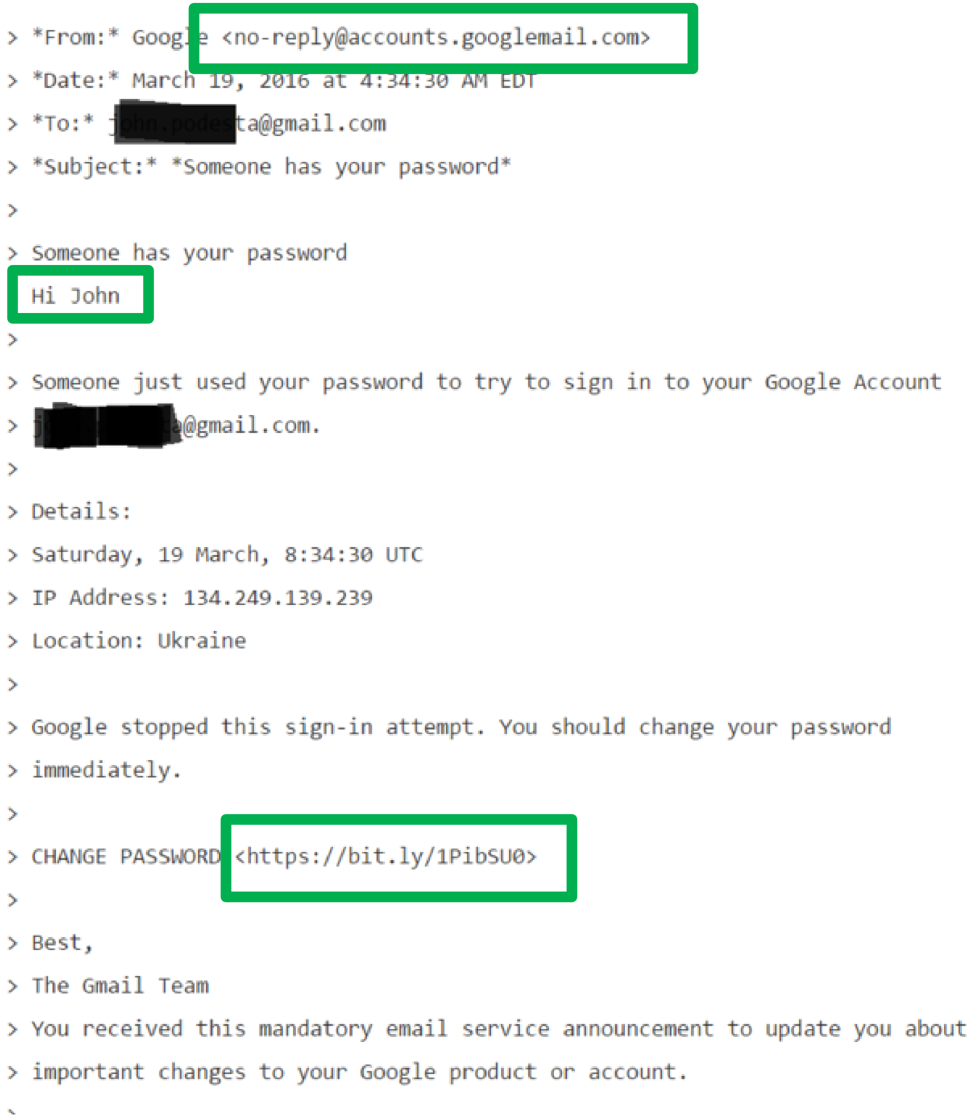


```
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* [redacted]ta@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [redacted]@gmail.com.
>
> 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.
```

www.cbsnews.com

John Podesta Phishing Email

- Campaign manager of Hillary Clinton
- On March 19, 2016 received a Google security alert
- This was a spear-fishing attack by Russian intelligence
- Podesta forward the email to his chief of staff, Sara Latham, who asked IT support
- IT erroneously responded ‘this is a legitimate email’
- Account compromised, emails dumped to Wikileaks
- Massive political scandal

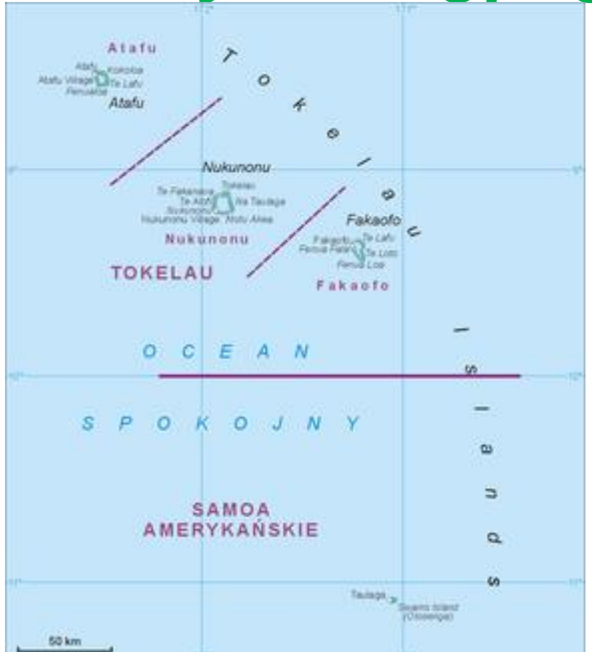


```
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* j[redacted]ta@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> j[redacted]@gmail.com.
>
> 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.
>
```

www.cbsnews.com

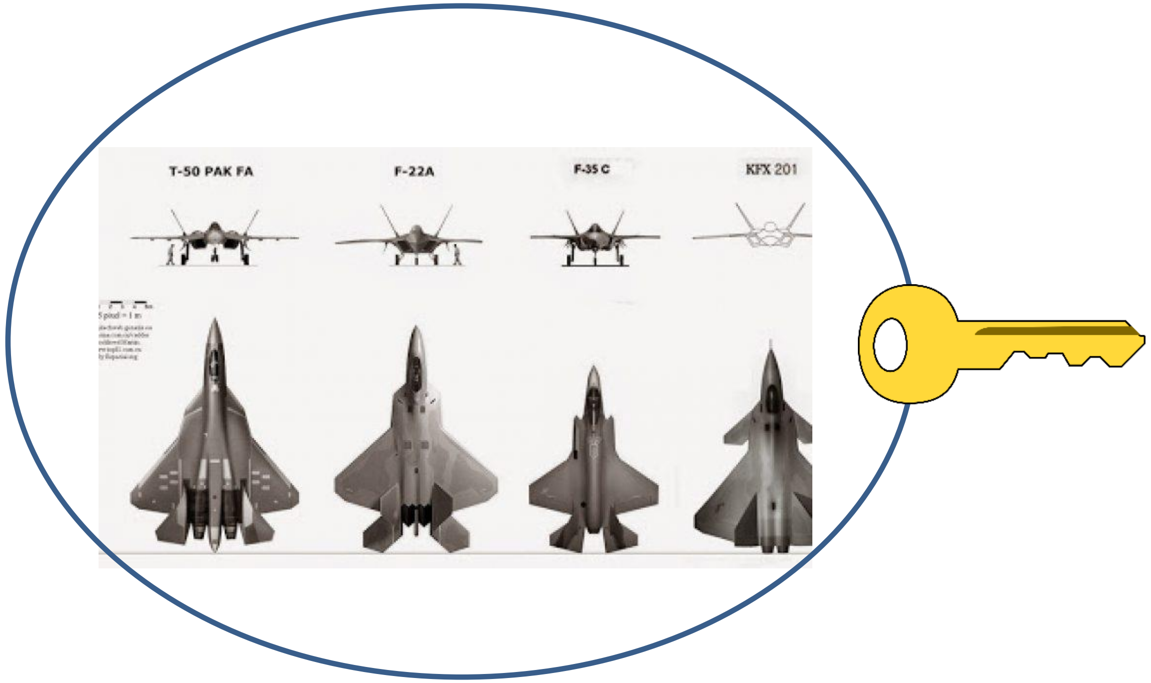
John Podesta Phishing Email

- Bitly is a URL shortening service
- Bitly link is https://bit.ly/1PibSU0
- Expands to http:// myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ==&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg== ...
- The top-level domain is **com-securitysettingpage.tk**



Tokelau

Lockheed Martin

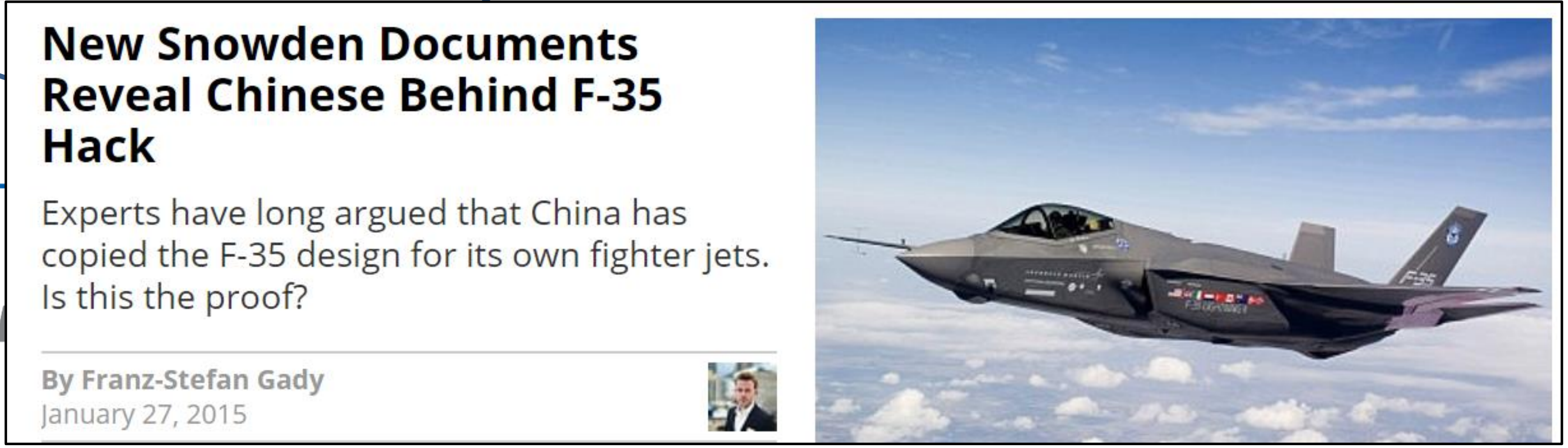


LOCKHEED MARTIN

Lockheed Martin

Defense Contractor Lockheed Martin Gets Hacked

Hackers stole data on Pentagon's newest fighter jet



New Snowden Documents Reveal Chinese Behind F-35 Hack

Experts have long argued that China has copied the F-35 design for its own fighter jets. Is this the proof?

By Franz-Stefan Gady
January 27, 2015

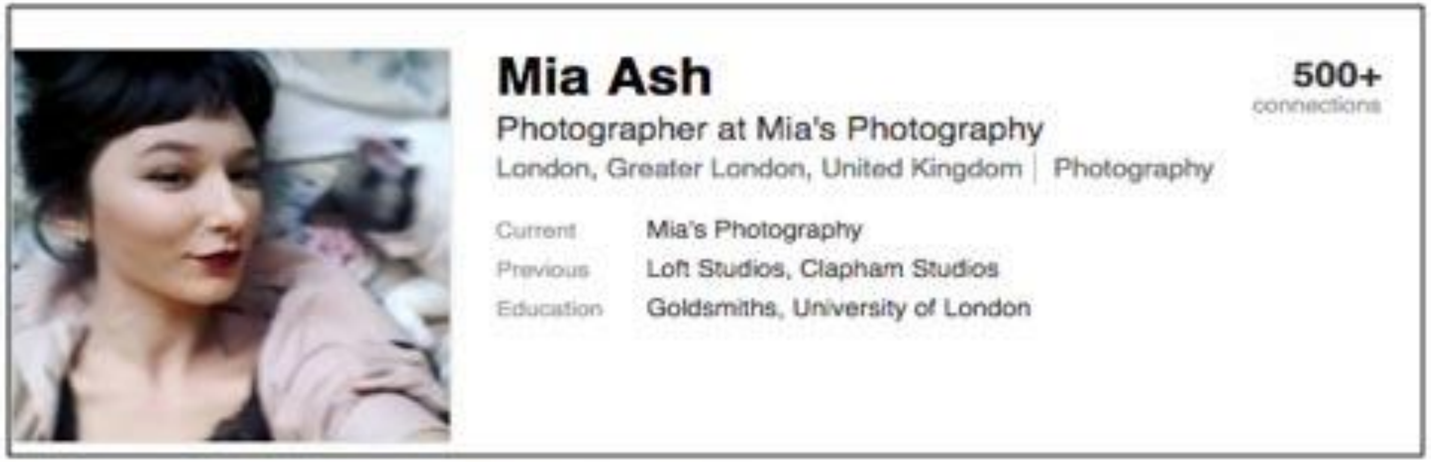
Lockheed Martin

- In 2011 Lockheed Martin was hacked
- F35 design plans were stolen
- The attackers initially hacked RSA security
- Sent phishing emails to 2 groups
- Subject line “2011 Recruitment Plan”
- One employee retrieved the mail from the junk folder and opened the Excel file
- The Excel file contained a malware that exploited a zero-day vulnerability in Adobe Flash to install a backdoor

https://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/

Mia Ash

- 30-year-old British woman
- Two art school degrees
- Successful career as a photographer
- 500+ friends on LinkedIn (many known photographers)
- Active Instagram/Facebook accounts
- Relationship status: ‘It's complicated’



Mia Ash

Photographer at Mia's Photography

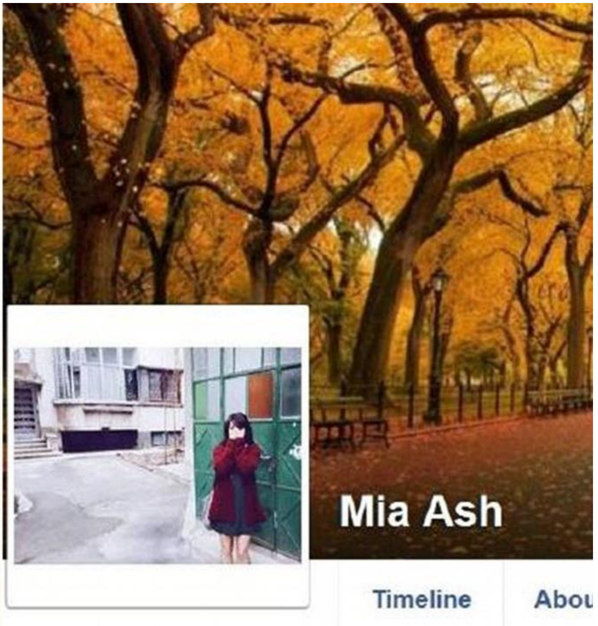
London, Greater London, United Kingdom | Photography

500+ connections

Current Mia's Photography

Previous Loft Studios, Clapham Studios

Education Goldsmiths, University of London

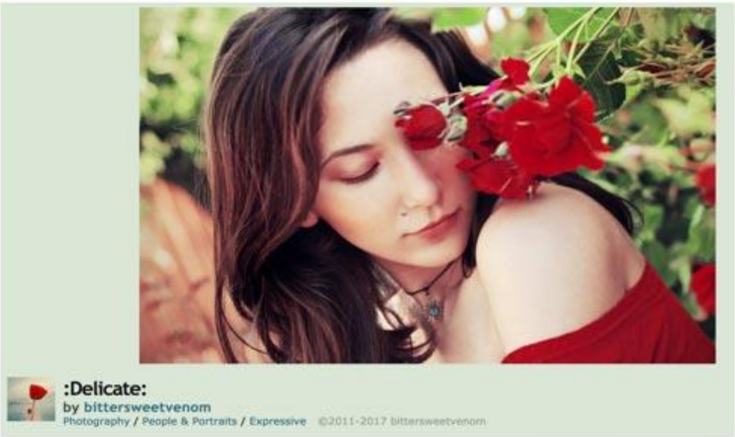


Mia Ash

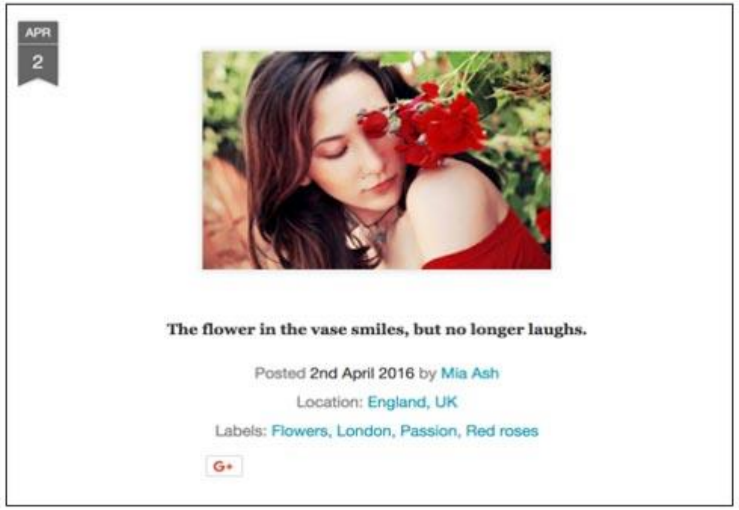
- In Dec 2016 – Jan 2017 there were phishing attacks targeting Middle East companies
- Trying to inject PupyRAT (Remote Access Trojan)
- The phishing attack was unsuccessful
- Iranian hackers (Cobalt Gypsy) created a fake virtual entity: Mia Ash
- Jan 13, Mia Ash contacted an employee via LinkedIn
- Jan 21, Mia asked to continue Facebook
- Correspondence continues via email/WhatsApp/Facebook
- Feb 12 Mia emailed ‘Copy of Photography Survey.xlsm’
- Mia encouraged to open the email at work using corporate email account
- The Excel file contained a macro that downloaded PupyRAT

Mia Ash

- Most content taken from other accounts



:Delicate:
by bittersweetvenom
Photography / People & Portraits / Expressive ©2011-2017 bittersweetvenom



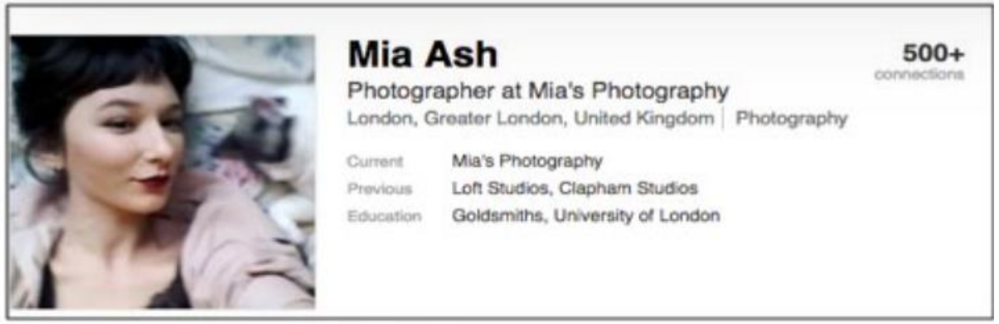
APR
2

The flower in the vase smiles, but no longer laughs.

Posted 2nd April 2016 by Mia Ash

Location: England, UK

Labels: Flowers, London, Passion, Red roses



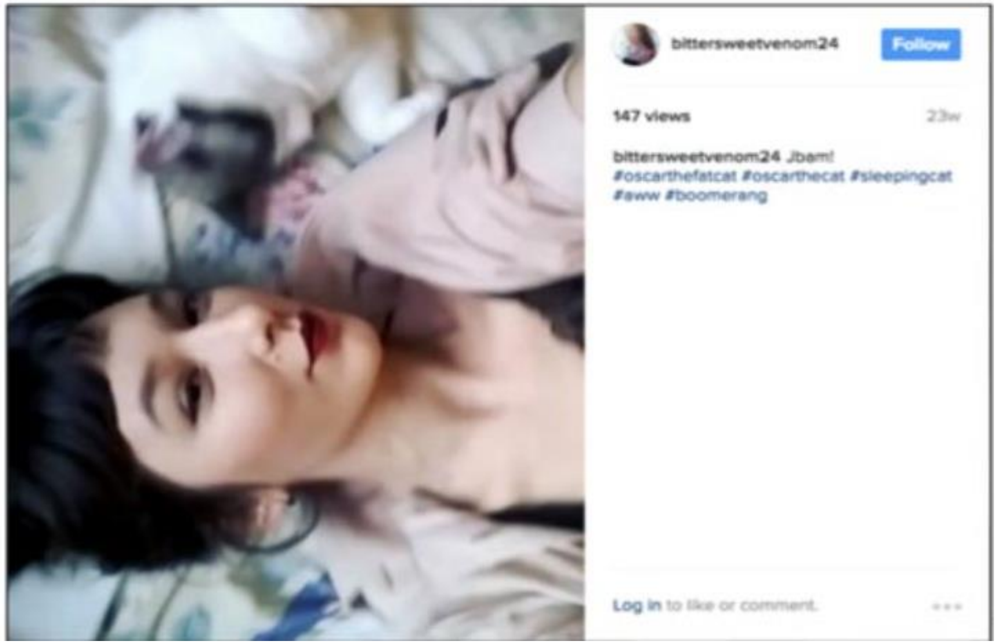
Mia Ash

500+ connections

Photographer at Mia's Photography

London, Greater London, United Kingdom | Photography

Current: Mia's Photography
Previous: Loft Studios, Clapham Studios
Education: Goldsmiths, University of London



bittersweetvenom24

147 views 23w

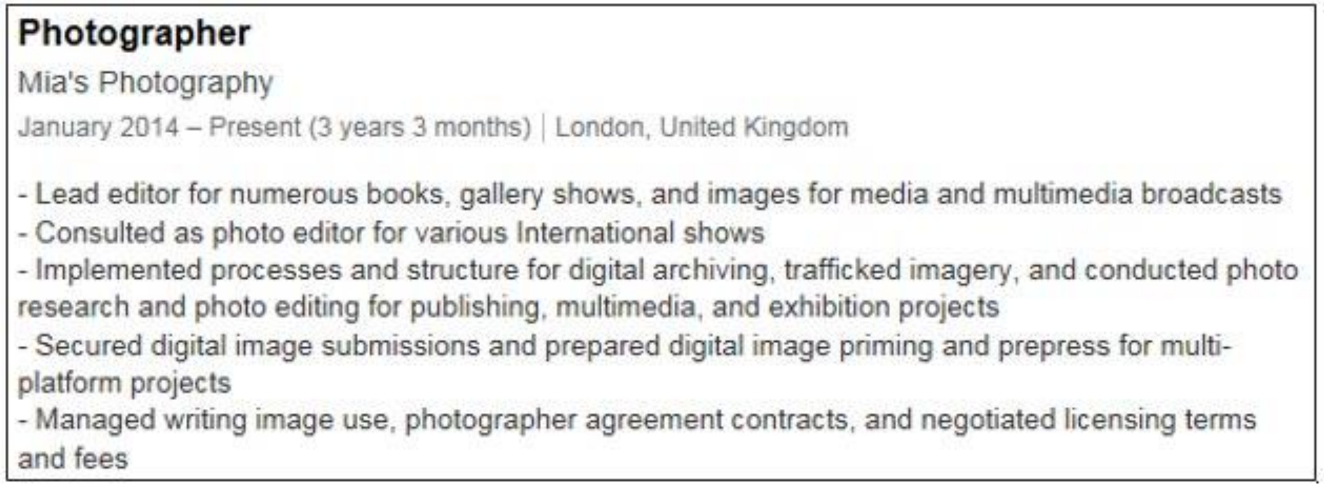
bittersweetvenom24 Jbam!
#oscarthefatcat #oscarthecat #sleepingcat
#aww #boomerang

Log in to like or comment.

https://www.instagram.com/bittersweetvenom24/

Mia Ash

- Mia’s job description is almost identical to an account of a U.S.-based photographer

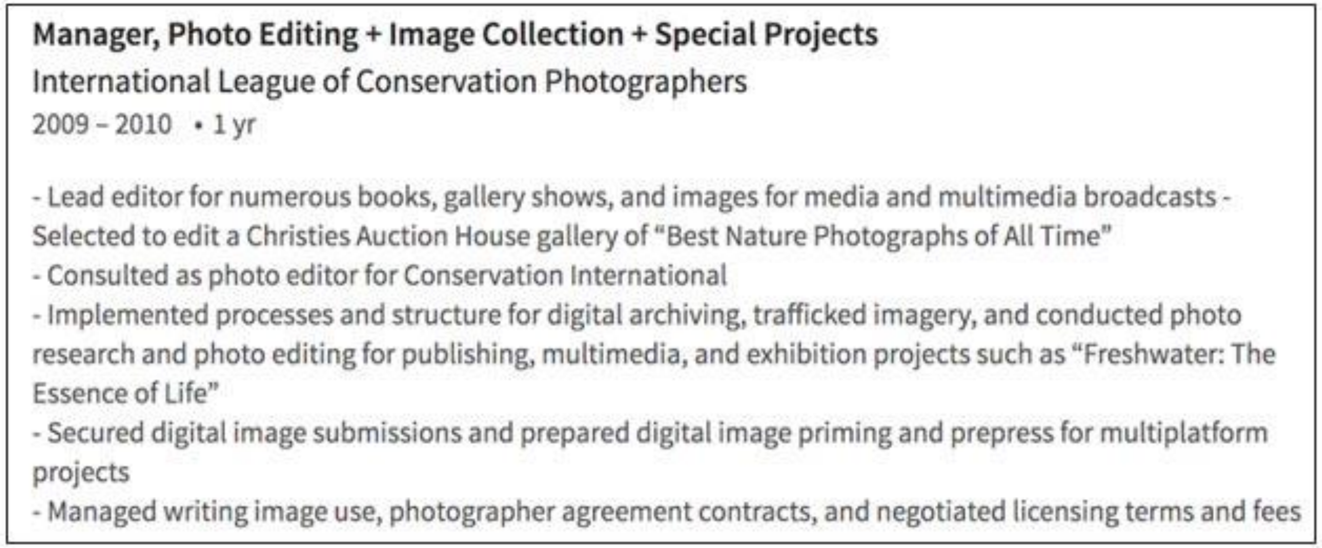


Photographer

Mia's Photography

January 2014 – Present (3 years 3 months) | London, United Kingdom

- Lead editor for numerous books, gallery shows, and images for media and multimedia broadcasts
- Consulted as photo editor for various International shows
- Implemented processes and structure for digital archiving, trafficked imagery, and conducted photo research and photo editing for publishing, multimedia, and exhibition projects
- Secured digital image submissions and prepared digital image priming and prepress for multi-platform projects
- Managed writing image use, photographer agreement contracts, and negotiated licensing terms and fees



Manager, Photo Editing + Image Collection + Special Projects

International League of Conservation Photographers

2009 – 2010 • 1 yr

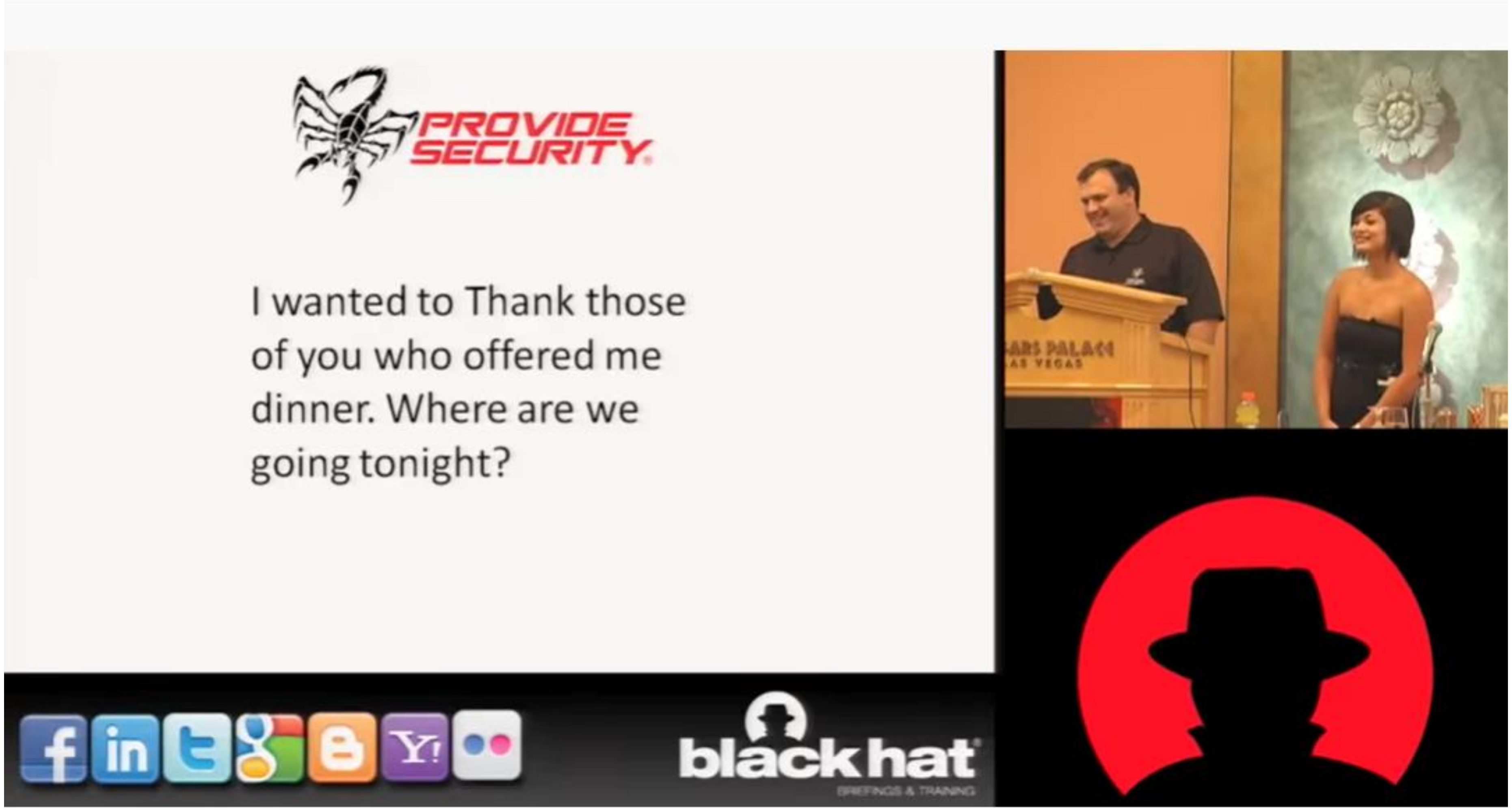
- Lead editor for numerous books, gallery shows, and images for media and multimedia broadcasts - Selected to edit a Christies Auction House gallery of “Best Nature Photographs of All Time”
- Consulted as photo editor for Conservation International
- Implemented processes and structure for digital archiving, trafficked imagery, and conducted photo research and photo editing for publishing, multimedia, and exhibition projects such as “Freshwater: The Essence of Life”
- Secured digital image submissions and prepared digital image priming and prepress for multiplatform projects
- Managed writing image use, photographer agreement contracts, and negotiated licensing terms and fees

https://www.secureworks.com/research/the-curious-case-of-mia-ash

Robin Sage

- A virtual entity created in 2009 by Robin Casey and Thomas Ryan (Black Hat 2010)
- 25-year-old ‘cyber threat analyst’
- MIT graduate
- Works at Naval Network Warfare Command in Norfolk, Virginia
- Has 10 years of work experience
- Facebook/LinkedIn/Twitter accounts
- Offered consulting work with Google and Lockheed Martin
- Received dinner invitations from several male contacts

Robin Sage



I wanted to Thank those of you who offered me dinner. Where are we going tonight?

https://www.youtube.com/watch?v=4pnKbibi6QY