SOCIAL ENGINEERING - HOW NOT TO BE A VICTIM!

BHUSHAN GUPTA

GUPTA CONSULTING, LLC.

WWW.BGUPTA.COM

WHAT IS YOUR PASSWORD?

Jimmy Kimmel Live

JIMMY KIMMEL LIVE - OBSERVATIONS

Most Common Password – password123

- No hesitation to answer password specific questions
- Only one person realized that he was being asked to reveal his password
- Only one person realized that he has given away his password.

Twitter Hack on June 9, 2016

120,000 Users opted for password - 123456

Its fair to assume that these people work somewhere and can be victims of serious social engineering attacks.

1987 - AT&T 3B2 with UNIX

SOCIAL ENGINEERING INGREDIENT

Human Persuasion!!

WHAT IS SOCIAL ENGINEERING?

Social engineering is an attack vector that relies heavily on human interaction and often involves tricking people in breaking normal security procedures.

(WhatIs.com)

WHAT IS SOCIAL ENGINEERING?

Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information.

(Wikipedia)

UBIQUITI NETWORKS ATTACK

- Ubiquiti Network Inc.
  San Jose, CA (Hong Kong Subsidiary)
  - June 5, 2015 (after 7 months)
  - CEO Fraud/BEC Attack
  - Cost $46.7M

- 2015 FBI Warning - $215M

BEC – Business Email Compromise

SOCIAL ENGINEERING - TROJAN HORSE (GREECE & TROY WAR)

an ancient art

THE BIGGEST THREAT

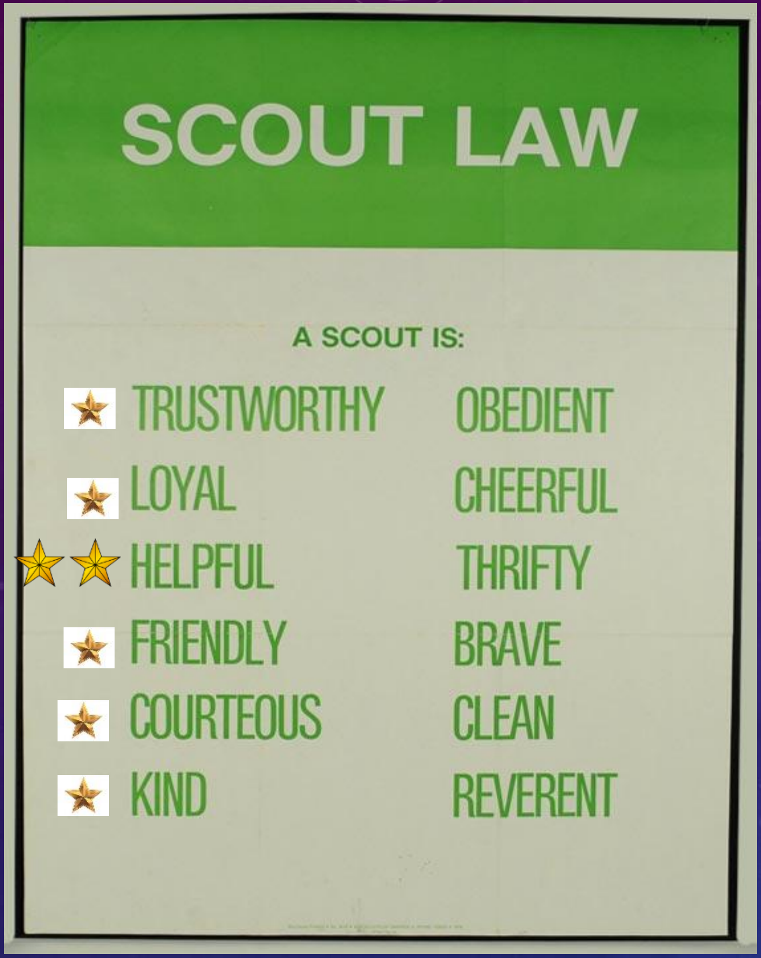
Image courtesy: Mikhail Romanenko

“The biggest threat to the security of a company is not a computer virus, an unpatched hole in a key program or a badly installed firewall. In fact, **the biggest threat could be you**.”

- Kevin Mitnick – Computer Security Consultant, Author

Why Me?

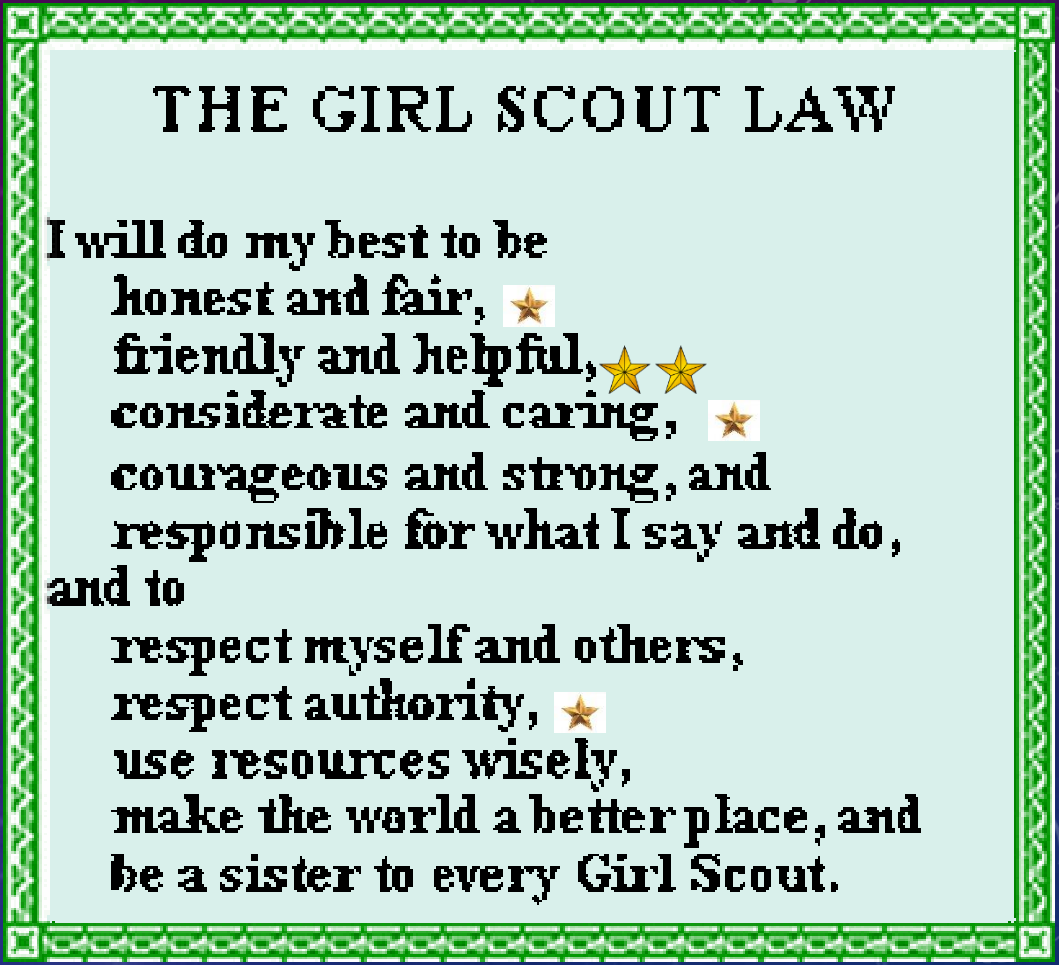
WE GROW UP WITH SOME CORE VALUES!



SCOUT LAW

A SCOUT IS:

- ★ TRUSTWORTHY
- ★ LOYAL
- ★★ HELPFUL
- ★ FRIENDLY
- ★ COURTEOUS
- ★ KIND
- OBEDIENT
- CHEERFUL
- THRIFTY
- BRAVE
- CLEAN
- REVERENT



THE GIRL SCOUT LAW

I will do my best to be
honest and fair, ★
friendly and helpful, ★★
considerate and caring, ★
courageous and strong, and
responsible for what I say and do,
and to
respect myself and others,
respect authority, ★
use resources wisely,
make the world a better place, and
be a sister to every Girl Scout.

OUR FOUNDATION – TEACHINGS FROM CHILDHOOD

REWARDED BASED UPON - TEAM WORK, WIN-WIN, HELPFUL, LOYALTY, OBEDIENCE!

Exercise Good Judgement

ATTACK VECTORS AND LURES

ATTACK VECTORS - TACTICS

Physical Vectors

- Shoulder Surfing
- Baiting – promise of goods to entice victim

  Infected USBs, CD

- Quid Pro Quo – service

  IT Impersonator trying to fix your system, obtaining a password and convincing you to load a utility (malware) on your system

ATTACK VECTORS - TACTICS

Physical Vectors Cont..

- Tailgating – impersonation as a courier/messenger/friend of an employee
- Impersonating as an authority - Ubiquity
- Dumpster Diving
- Pretexting – scammer creating false trust

ATTACK VECTORS - TACTICS

Digital Vectors:

- Social Media – Obtaining information from Facebook or Instagram and create fake profiles

  Admiral James Stavridis (NATO Supreme Allied Commander Europe) Facebook Profile

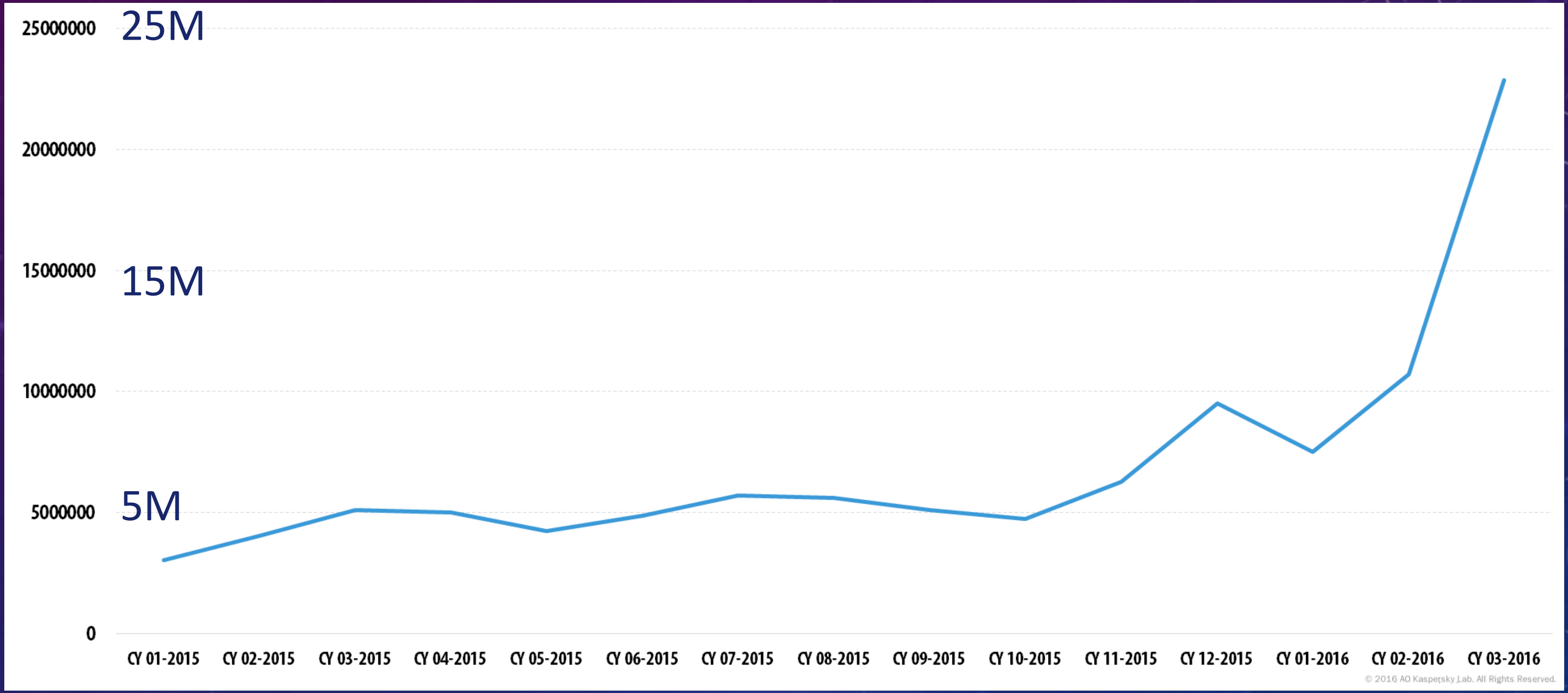
WHAT IS PHISHING?

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

While Phishing, an attacker casts a wider net hoping that someone will be tricked.

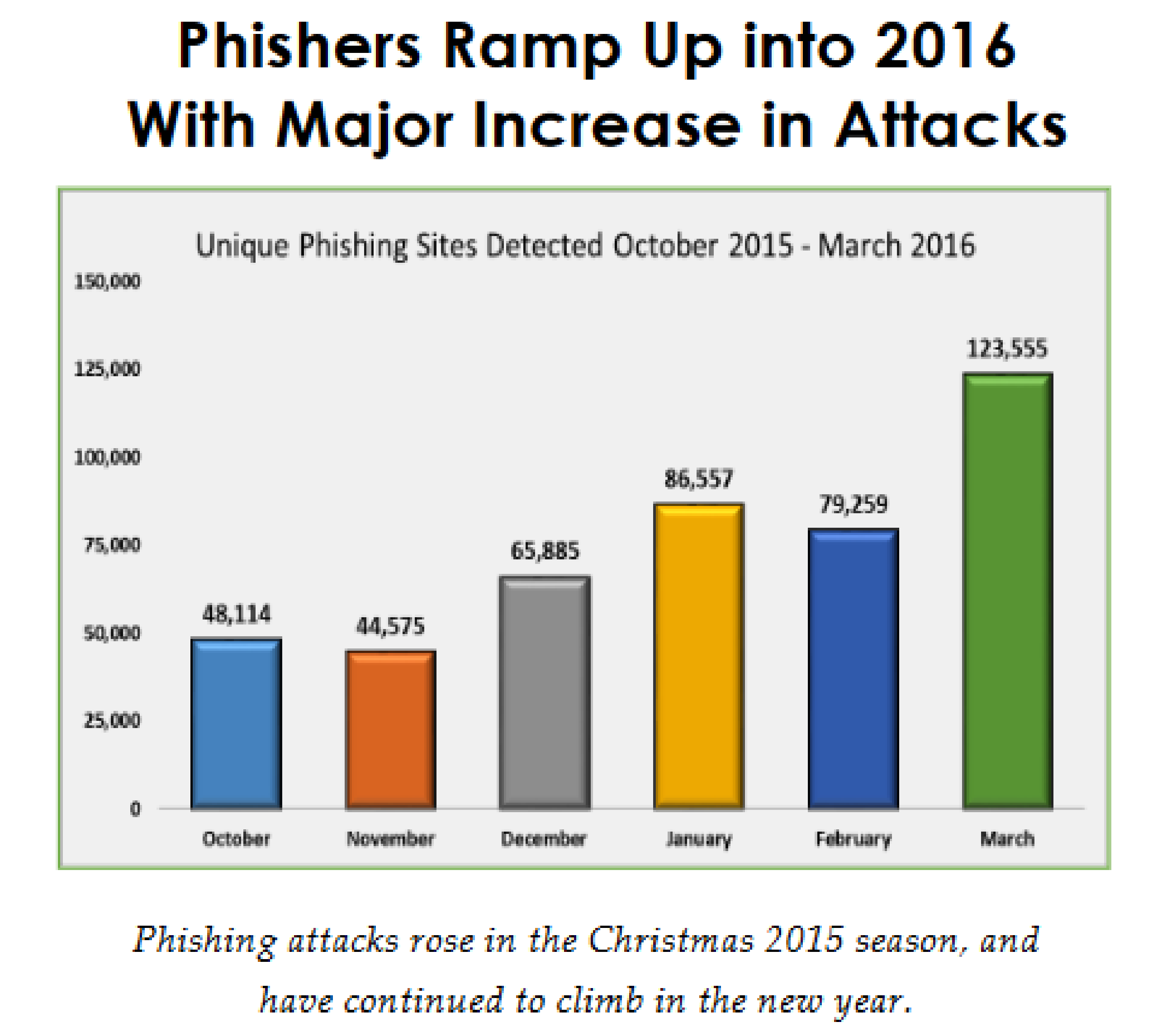
Source: Wikipedia

PHISHING TREND – JANUARY 2015 TO MARCH 2016



Source: Securitylist.com

INCREASE IN PHISHING WEB SITES



Phishers Ramp Up into 2016 With Major Increase in Attacks

Phishing attacks rose in the Christmas 2015 season, and have continued to climb in the new year.

ATTACK VECTORS - PHISHING

Types of phishing:

- Phishing – attacker casts a broad net
- Spear Phishing – somewhat more specific to one person
- Whaling – phishing targeted at a person with specific valuable information

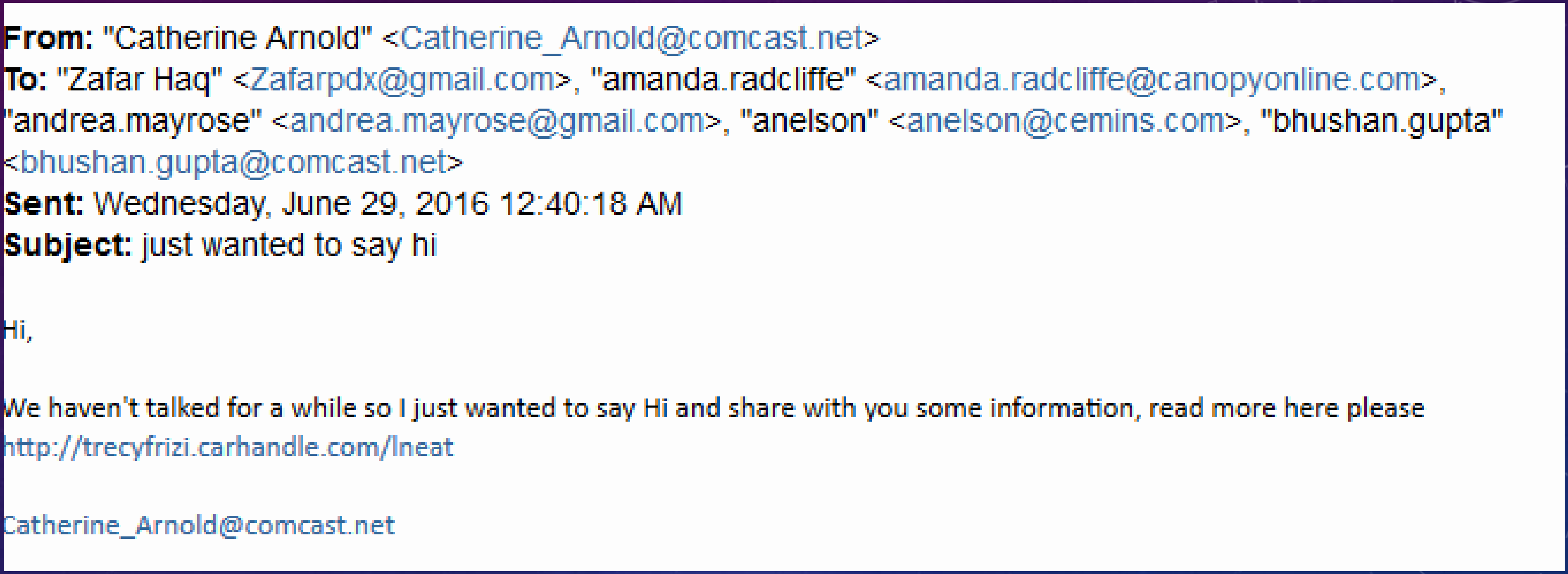
PHISHING TARGETS - ALMOST ANYONE

- Individuals (elderly, common people, security experts)
- Influential people
- Corporations

MECHANICS OF A PHISHING ATTACK

- Attacker sends out an email that appears to be legitimate
- Email either directs the receiver to click on a link or perform an action
- When sent to the linked site, the attacker intends to:
  - Gather personal and confidential information
  - Install malware to get access to the system
- If the email requires an action it is either to collect confidential information or take an action (such as transferring money) to benefit the attacker
- The email often has threats - harmful consequences

A PHISHING EXAMPLE



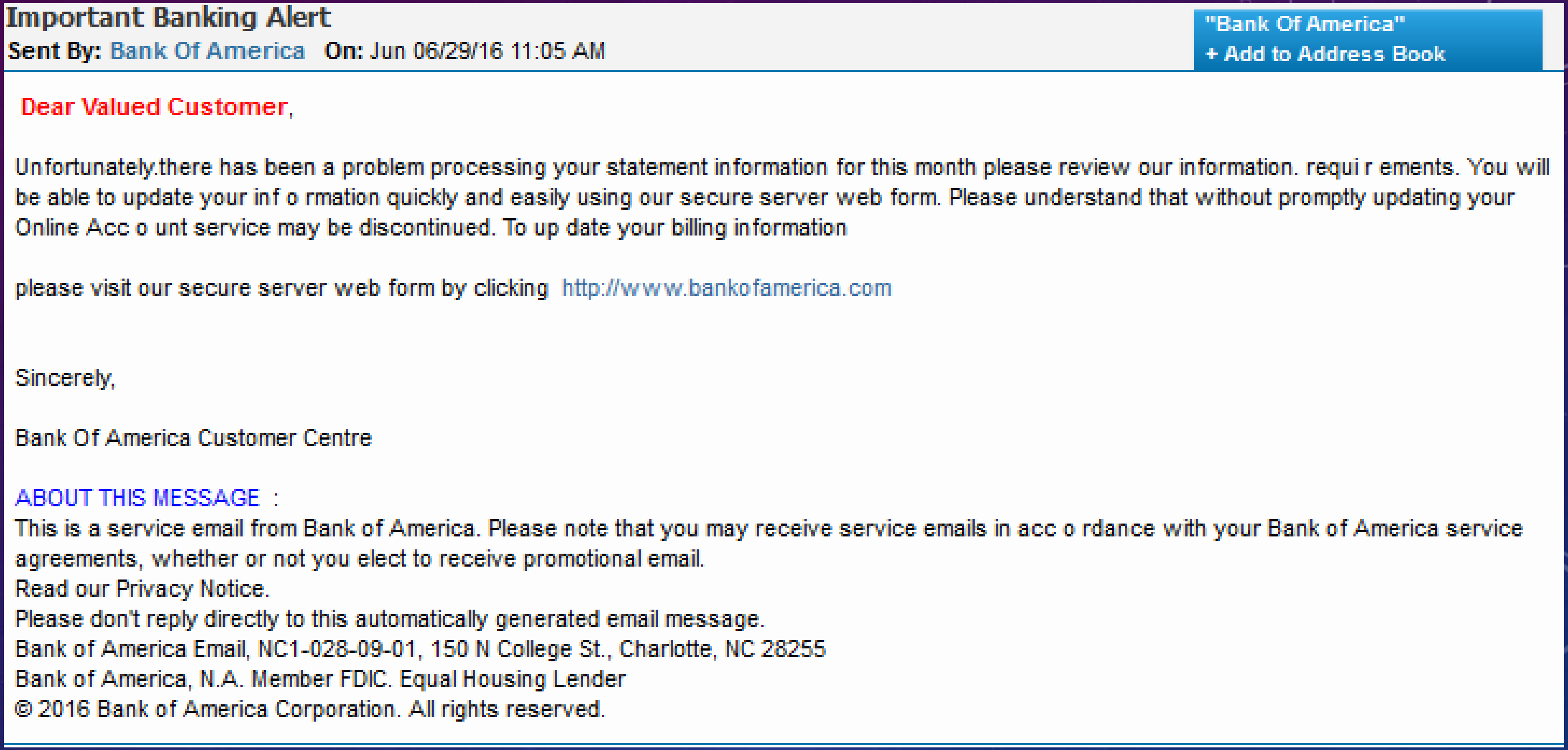
From: "Catherine Arnold" <Catherine_Arnold@comcast.net>
To: "Zafar Haq" <Zafarpdx@gmail.com>, "amanda.radcliffe" <amanda.radcliffe@canopyonline.com>, "andrea.mayrose" <andrea.mayrose@gmail.com>, "anelson" <anelson@cemins.com>, "bhushan.gupta" <bhushan.gupta@comcast.net>
Sent: Wednesday, June 29, 2016 12:40:18 AM
Subject: just wanted to say hi

Hi,

We haven't talked for a while so I just wanted to say Hi and share with you some information, read more here please
http://trecyfrizi.carhandle.com/lneat

Catherine_Arnold@comcast.net

A SPEAR PHISHING EXAMPLE



Important Banking Alert

Sent By: Bank Of America **On:** Jun 06/29/16 11:05 AM

Dear Valued Customer,

Unfortunately.there has been a problem processing your statement information for this month please review our information. requi r ements. You will be able to update your inf o rmation quickly and easily using our secure server web form. Please understand that without promptly updating your Online Acc o unt service may be discontinued. To up date your billing information

please visit our secure server web form by clicking http://www.bankofamerica.com

Sincerely,

Bank Of America Customer Centre

ABOUT THIS MESSAGE :
This is a service email from Bank of America. Please note that you may receive service emails in acc o rdance with your Bank of America service agreements, whether or not you elect to receive promotional email.
Read our Privacy Notice.
Please don't reply directly to this automatically generated email message.
Bank of America Email, NC1-028-09-01, 150 N College St., Charlotte, NC 28255
Bank of America, N.A. Member FDIC. Equal Housing Lender
© 2016 Bank of America Corporation. All rights reserved.

Bank of America Email, 8th Floor-NC1-002-08-25, 101 South Tryon St., Charlotte, NC 28255-0001

WHALING ATTACK

Focused on an individual who has highly valuable information – C Levels

For a successful whaling attack

- Attacker performs significant research ahead of attack
- Takes place when the C-Level executive admin forwards an email to the finance department

CHARACTERISTICS OF A PHISHING EMAIL

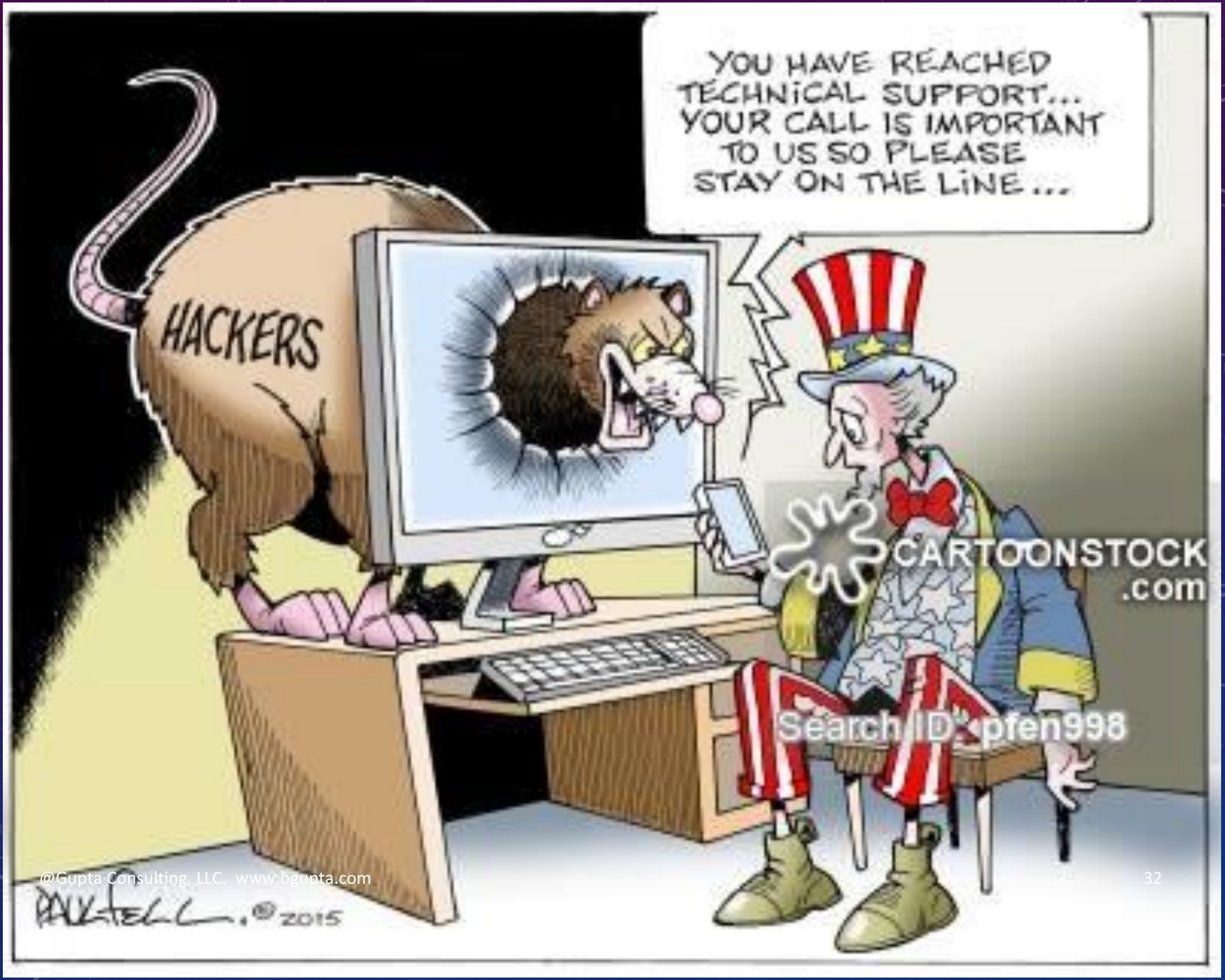
Not as polished as a legitimate email

- Grammar
- Salutation (generic)
- Wrong Information

ATTACK LURES – MOST POPULAR IN 2014

- Big News – Malaysian Airline Flight 370
- Celebrity Gossip – Death of Robin Williams in 2012
  - Link to site to view the video, WORM_GAMARUE.WSTQ
- Movies – Annie, Hobbit: Battle of the five armies
  - Malicious links, Adware
- Tech Games – Flappy Bird
- Social Media Scams – LinkedIn
- Scare Tactics – Ebola Outbreak

PHISHING - HOW TO PROTECT YOURSELF?



YOU HAVE REACHED TECHNICAL SUPPORT... YOUR CALL IS IMPORTANT TO US SO PLEASE STAY ON THE LINE...
HACKERS
CARTOONSTOCK .com
Search ID: pfen998
©2015

THE BIGGEST THREAT

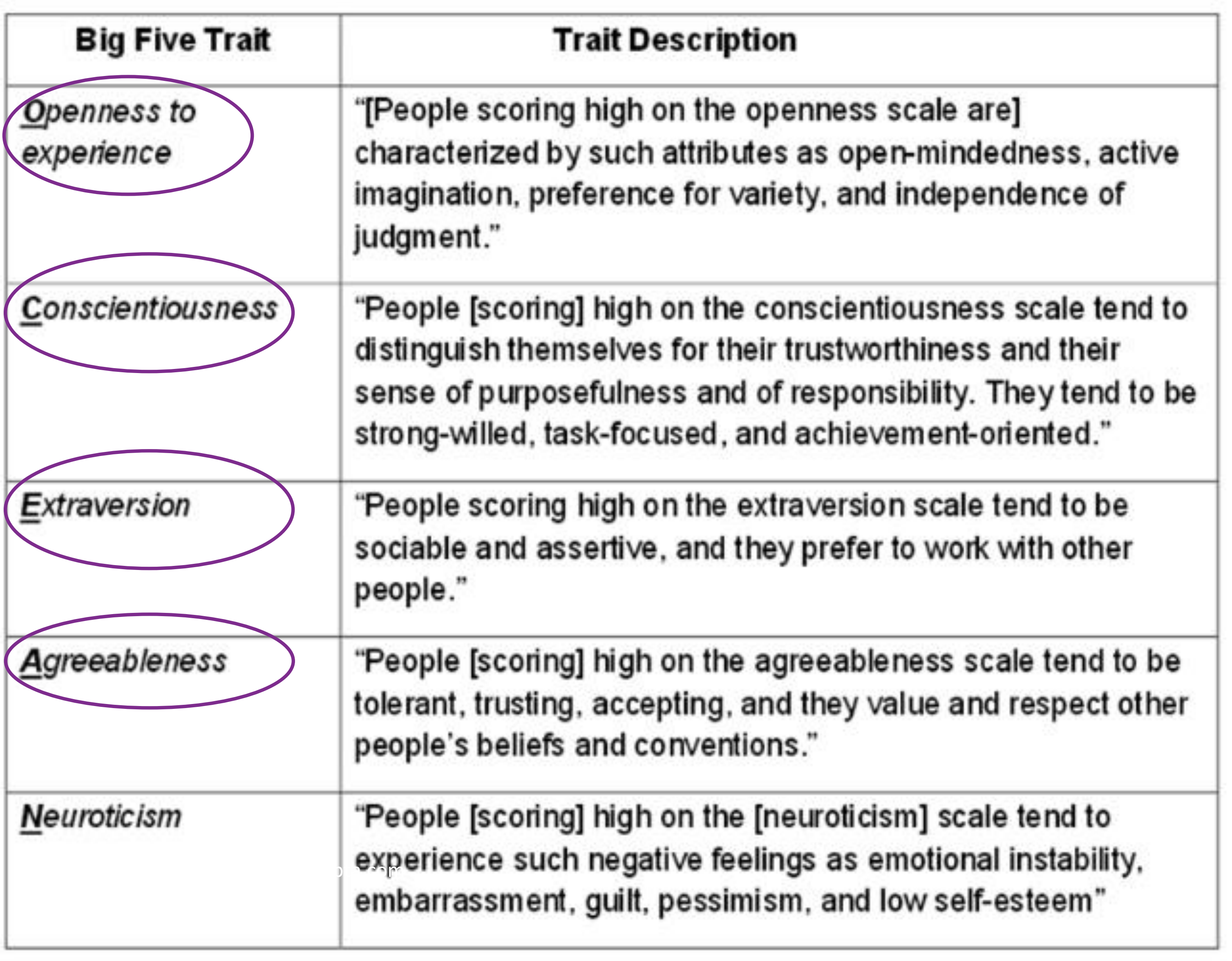
Image courtesy: Mikhail Romanenko

Educate/
Train

“The l y of a company is not a compu ole in a key program or a badly installed firew , the biggest threat could be you.”

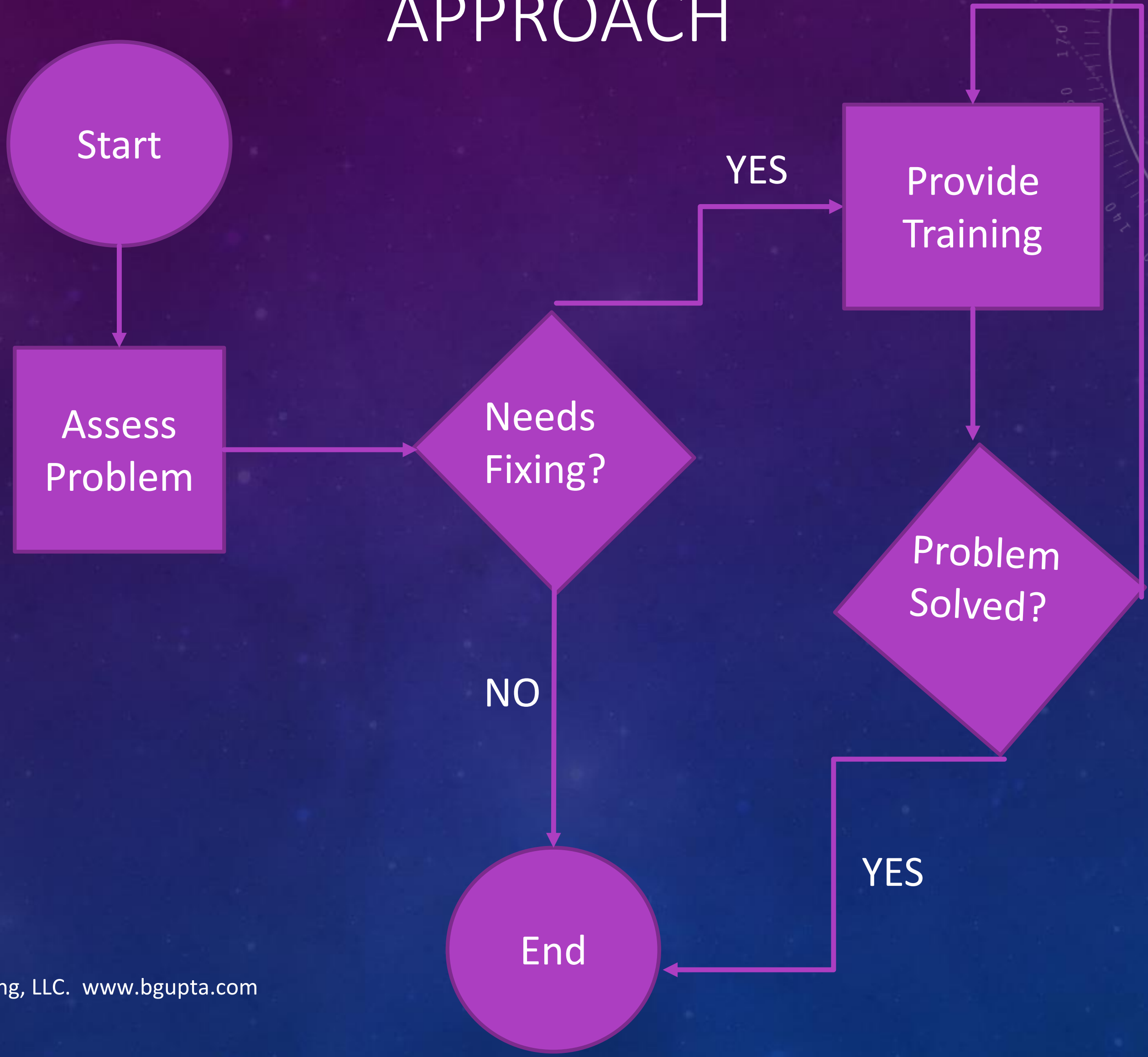
- Kevin Mitnick – Computer Security Consultant, Author

HUMAN TRAITS



Big Five Trait	Trait Description
Openness to experience	"[People scoring high on the openness scale are] characterized by such attributes as open-mindedness, active imagination, preference for variety, and independence of judgment."
Conscientiousness	"People [scoring] high on the conscientiousness scale tend to distinguish themselves for their trustworthiness and their sense of purposefulness and of responsibility. They tend to be strong-willed, task-focused, and achievement-oriented."
Extraversion	"People scoring high on the extraversion scale tend to be sociable and assertive, and they prefer to work with other people."
Agreeableness	"People [scoring] high on the agreeableness scale tend to be tolerant, trusting, accepting, and they value and respect other people's beliefs and conventions."
Neuroticism	"People [scoring] high on the [neuroticism] scale tend to experience such negative feelings as emotional instability, embarrassment, guilt, pessimism, and low self-esteem"

APPROACH


Start
Assess Problem
Needs Fixing?
YES
Provide Training
NO
Problem Solved?
NO
YES
End

ASSESS YOUR VULNERABILITY

Assess your vulnerability by simulating controlled experiments:

- Baiting – promise of goods to entice victim
- Quid Pro Quo – service
- Tailgating

  impersonation as a courier/messenger/friend of an employee

  Impersonating as an authority
- Dumpster Diving

Phishing, spear phishing, whaling

SIMULATING A PHISHING EXPERIMENT

Considerations

- Support
- Experiment Logistics
- Metrics
- Outcome

SIMULATE A PHISHING EXPERIMENT – SUPPORT

Build Support

- Company ethics
- Championship form upper management
- Support from participating managers

PHISHING EXPERIMENT – SAMPLE

Characteristics

- Statistically viable Sample size - 20 to 30% of population
- Appropriate representation – high value targets
  - System Administrators – Level of Privilege
  - C-Levels (CEO, CFO, CTO)- Decision Makers
  - Finance – Revenue
  - Sales/Marketing - Extroverts
  - Human Resources – Access to personal information
  - Design Groups – seeking new ideas

SIMULATE PHISHING EXPERIMENT - LOGISTICS

Crafting a Phishing Email

- Appear to come from a legitimate source
- Compelling reason or enticing element to take an action
  - Incentive
  - Threat / consequence
  - Entice user to read and take action multiple times
  - Address interest of entire population

SIMULATE PHISHING EXPERIMENT - LOGISTICS

Data collection – time period

- Optimal time
- Follow the schedule

Resources – Security operations + QA

- Account for tools – price and training
- Creation of experiments
- Data analysis

SIMULATE PHISHING EXPERIMENT - ASSESS PROBLEM MAGNITUDE

Metrics:

- Percentage of population fell victim
- Victim Rate by Time: % by time – 24, 48, 72 hours, beyond
- Percentage of people falling victim multiple times
- Group affinity - # of victims by Group(s)
- Rate of Proactive Reporting

SIMULATE PHISHING EXPERIMENT - OUTCOME

Analysis Outcome:

- Is it a problem that needs attention based upon security policy?
- How wide spread the problem is?
  - Particular group(s) - HR, Finance, Marketing
  - Entire Organization

COMBAT THE PROBLEM

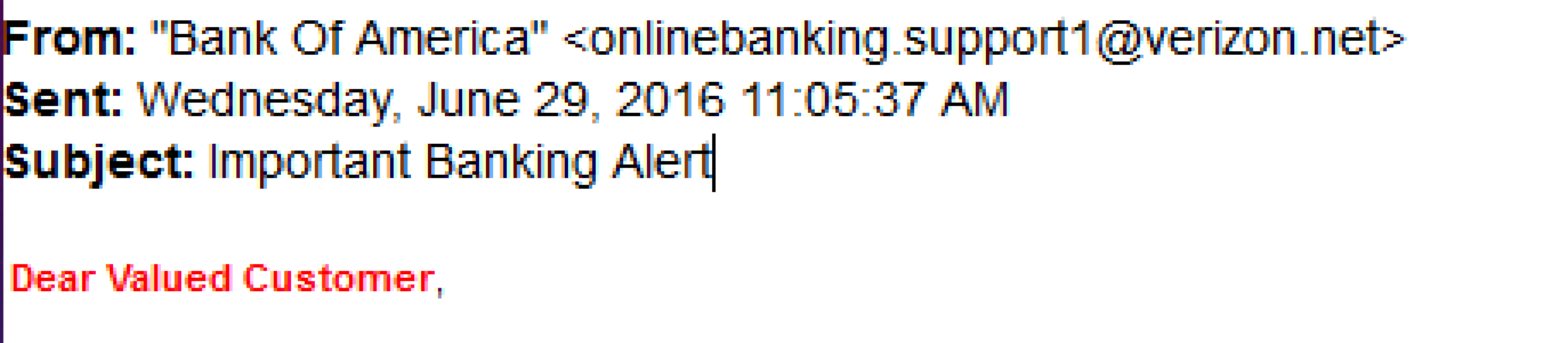
- Assess problem magnitude
- Validate against your organization security objectives
- Set goals for social engineering vulnerability
  - Overall Victims Rate <10% in next 6 months
  - X Group victim Rate < 5% in next 6 months
- Design and provide Training
- Assess impact and follow up

PROVIDING EDUCATION/TRAINING

TRAINING – DESIGN/CONTENT

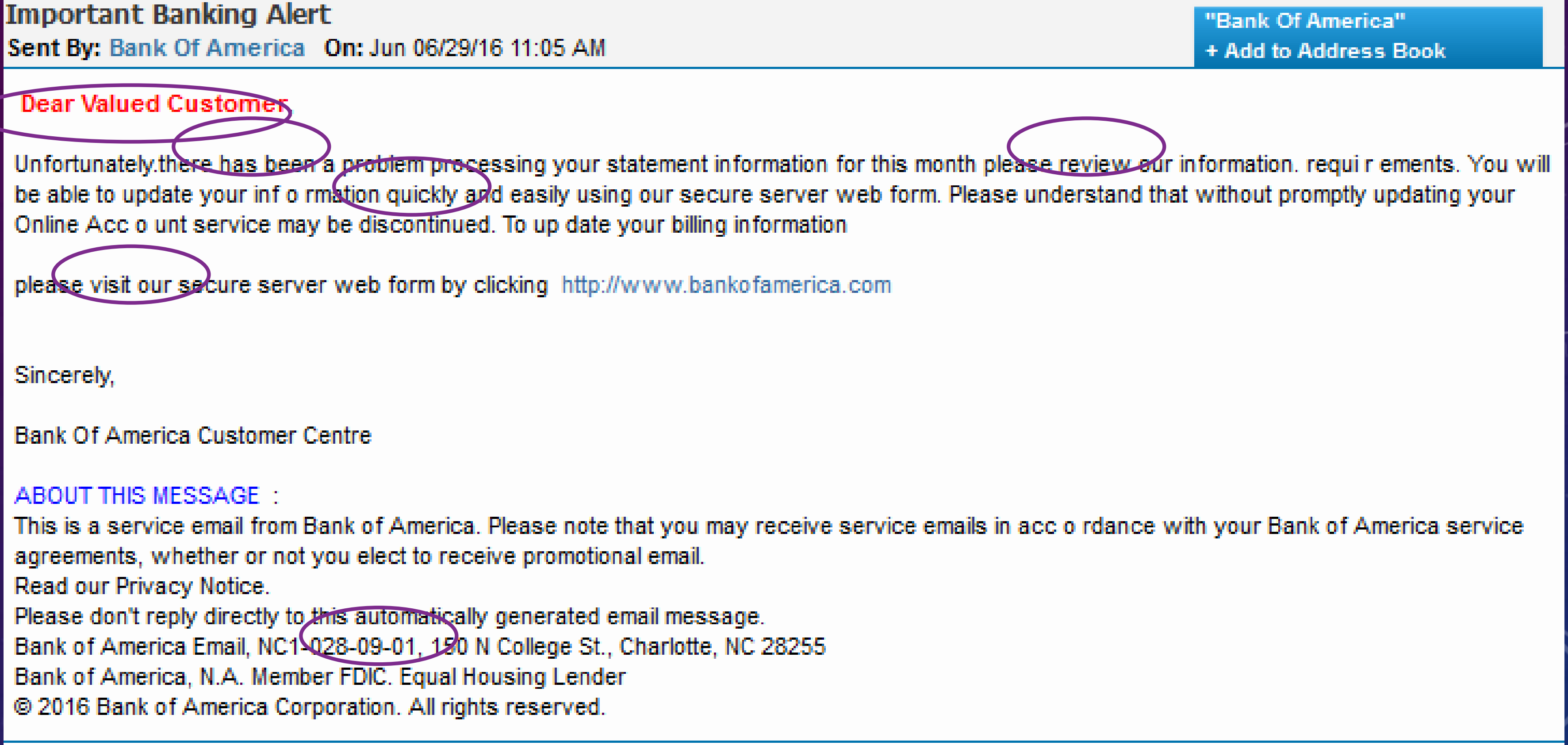
Identification of email legitimacy:

- Source validation
- Evaluation of email content
  - Grammatical Errors
  - Professional vs. crude email
  - Source of origin
  - Disclaimers if any
  - Getting basic link information – IP Address



From: "Bank Of America" <onlinebanking.support1@verizon.net>
Sent: Wednesday, June 29, 2016 11:05:37 AM
Subject: Important Banking Alert

Dear Valued Customer,



Important Banking Alert

Sent By: Bank Of America **On:** Jun 06/29/16 11:05 AM

Dear Valued Customer

Unfortunately.there has been a problem processing your statement information for this month please review our information. requi r ements. You will be able to update your inf o rmation quickly and easily using our secure server web form. Please understand that without promptly updating your Online Acc o unt service may be discontinued. To up date your billing information

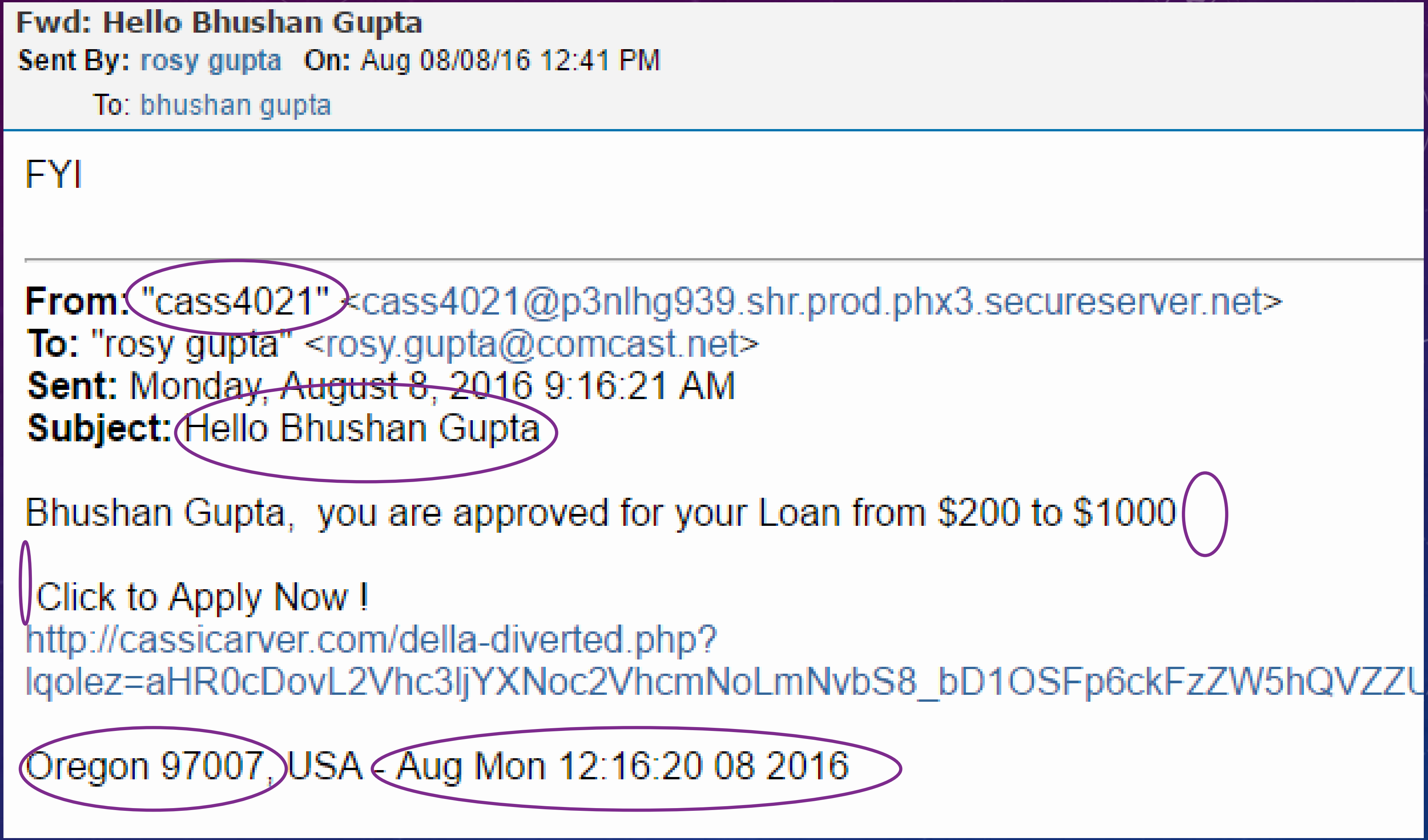
please visit our secure server web form by clicking http://www.bankofamerica.com

Sincerely,

Bank Of America Customer Centre

ABOUT THIS MESSAGE :
This is a service email from Bank of America. Please note that you may receive service emails in acc o rdance with your Bank of America service agreements, whether or not you elect to receive promotional email.
Read our Privacy Notice.
Please don't reply directly to this automatically generated email message.
Bank of America Email, NC1-028-09-01, 150 N College St., Charlotte, NC 28255
Bank of America, N.A. Member FDIC. Equal Housing Lender
© 2016 Bank of America Corporation. All rights reserved.

Bank of America Email, 8th Floor-NC1-002-08-25, 101 South Tryon St., Charlotte, NC 28255-0001



Fwd: Hello Bhushan Gupta

Sent By: rosy gupta **On:** Aug 08/08/16 12:41 PM

To: bhushan gupta

FYI

From: "cass4021" <cass4021@p3nlhg939.shr.prod.phx3.secureserver.net>
To: "rosy gupta" <rosy.gupta@comcast.net>
Sent: Monday, August 8, 2016 9:16:21 AM
Subject: Hello Bhushan Gupta

Bhushan Gupta, you are approved for your Loan from $200 to $1000

Click to Apply Now !
http://cassicarver.com/della-diverted.php?
lqolez=aHR0cDovL2Vhc3ljYXNoc2VhcmNoLmNvbS8_bD1OSFp6ckFzZW5hQVZZ

Oregon 97007, USA - Aug Mon 12:16:20 08 2016

TRAINING – DESIGN/CONTENT

Importance of not deleting the email

- Forensics
- Build threat data
- Example for future training

WHAT TO DO IF:

A phishing email has been identified: Provide Documented process for :

- Contact Person – phone and email
- Safe ways to deal with the email - forward to security group

The link has been followed

- Capturing the web site
- Basic system monitoring techniques

POST-TRAINING ACTIVITIES

- Monitor phishing email rate
- Run another experiment to measure the impact
- Train new employees on a regular basis
- Offer supplemental training as necessary

ASSESS YOUR OVERALL VULNERABILITY

Other vectors:

- Tailgating – impersonation as a courier/messenger/friend of an employee
- Dumpster Diving
- Baiting – promise of goods to entice victim
- Quid Pro Quo – service
- Impersonating as an authority

SIMULATE PHISHING EXPERIMENT - TOOLS

Industry Tools:

- Wombat Security Technologies – wide range of utilities
- phishingbox (phisingbox.com)
    - Capability to execute an attack and gather results
- Kali Linux – Social Engineering Module – Open Source

HUMAN HARDWARE BUGS

- High level of trust
- Believing in simplicity
  - Password
- Losing passion of something important
- Failure to take a timely action
  - Apply patches
  - Provide documentation
  - Review requests for action

BEST PRACTICES

- Develop an enterprise security plan
- Put right team in place
- Deploy defenses
- Perform threat analysis
- Continued training and awareness
- Respond to incidence

CYBERSECURITY IS A BUSINESS ISSUE!!

- Support from Management
- Appropriate Budget
- Multiple forms of protection

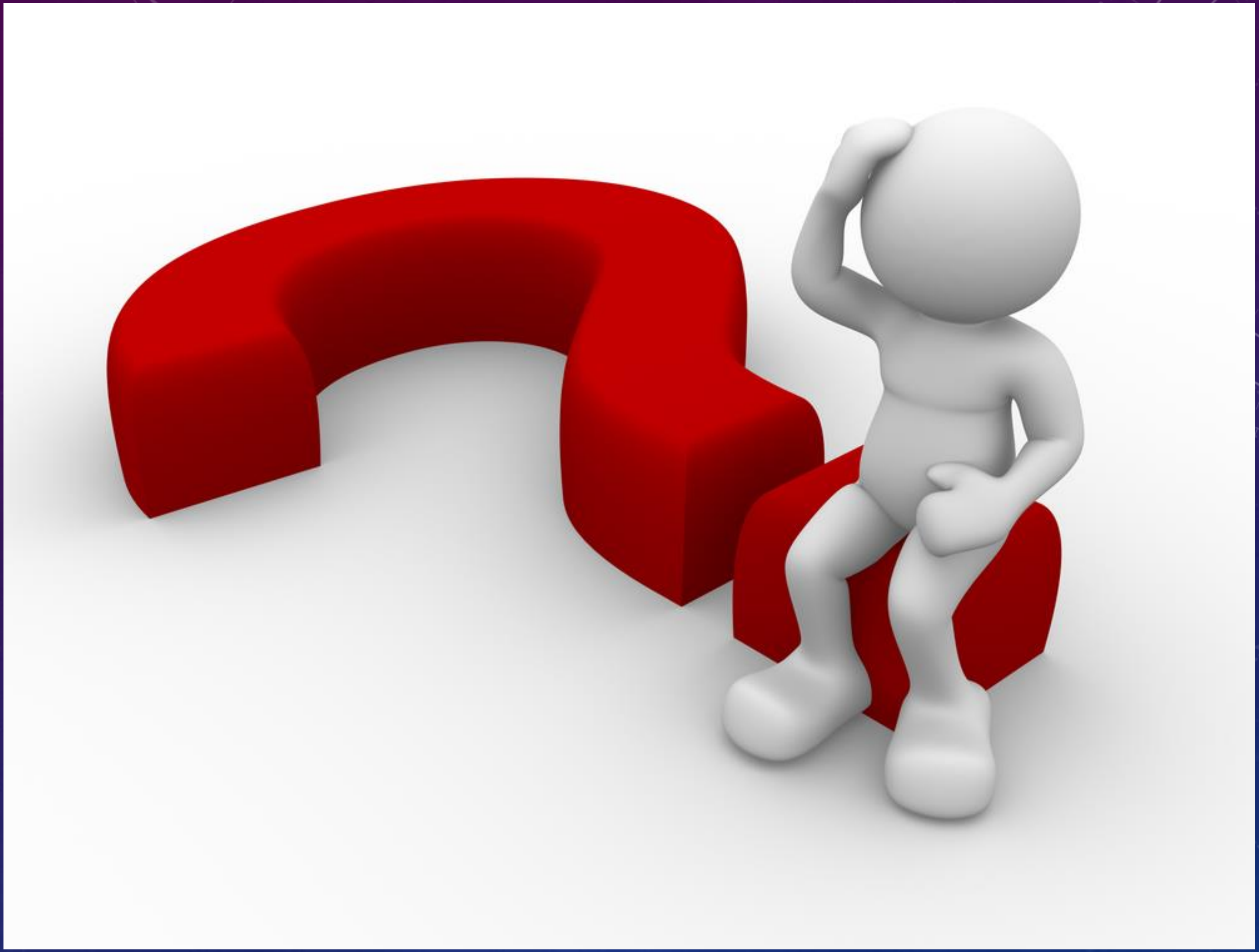
WANT TO KNOW MORE?

White Paper from SANS

https://www.sans.org/reading-room/whitepapers/engineering/methods-understanding-reducing-social-engineering-attacks-36972

"Instead of waiting for someone to steal my identity, I'm going to auction it on eBay!"

OH MY GOD! WE'VE BEEN THE VICTIMS OF CYBER-CRIME...SOMEONE ON THE OTHER SIDE OF THE WORLD HAS PAID ALL OUR BILLS!
CARTOONSTOCK .com
Search ID: mlyn1542
LYNCH



Thank
you