Northern New England School of Banking

Fraud and Cybercrime

Threats / Recognizing Fraud / Staying Safe

Presented by:
John H. Rogers, CISSP
Director of Advisory Services
john.rogers@tylertech.com

sage DATA SECURITY

tyler technologies

Agenda

- The Internet Environment
- Threat Update
- Breach Update
- Recognizing Fraud
- Social Engineering : The Human Factor
- Defenses
- Questions & Answers

sage DATA SECURITY

Foundational Principle

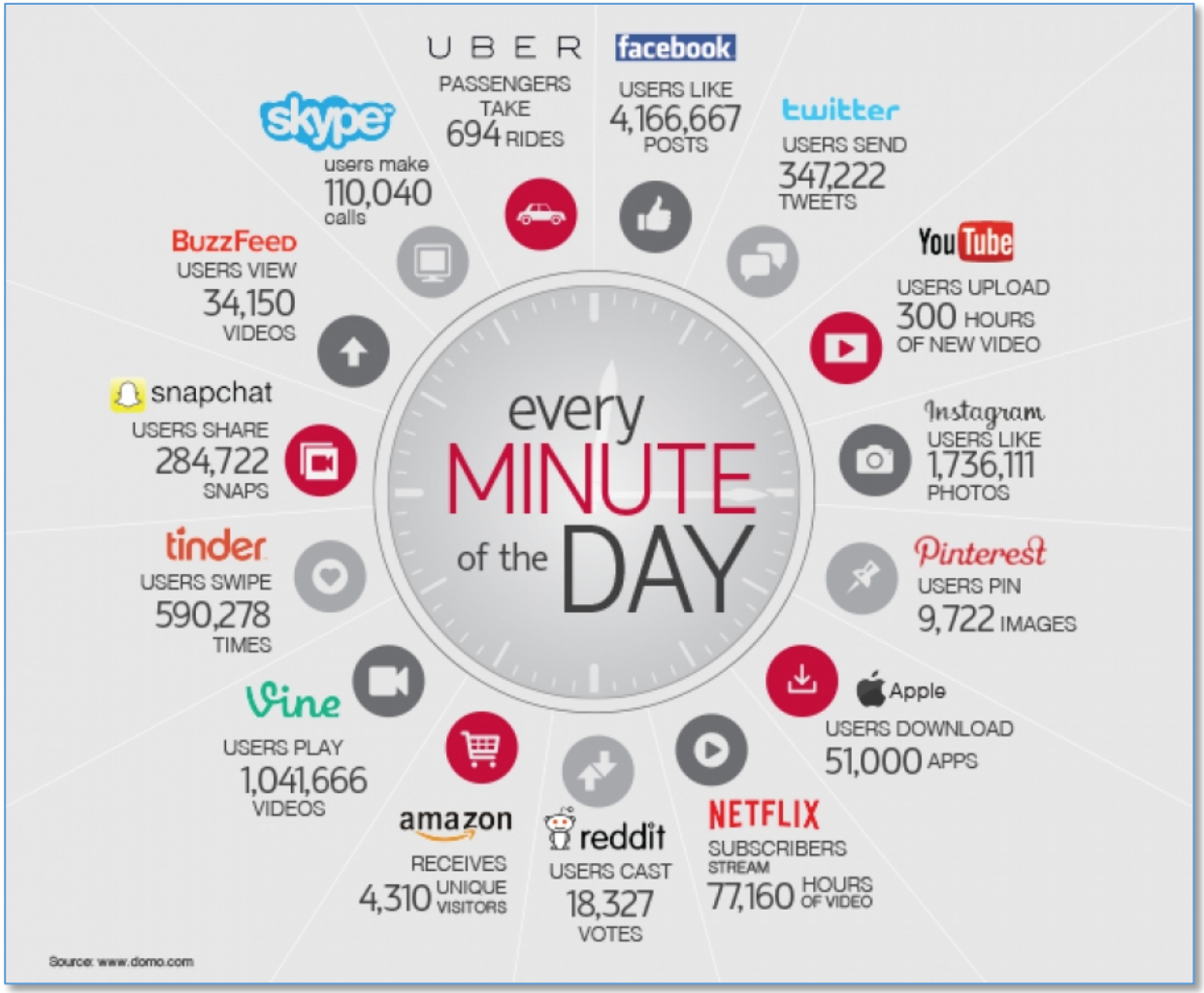
- The Internet is a shared resource and securing it is

~ Our Shared Responsibility ~

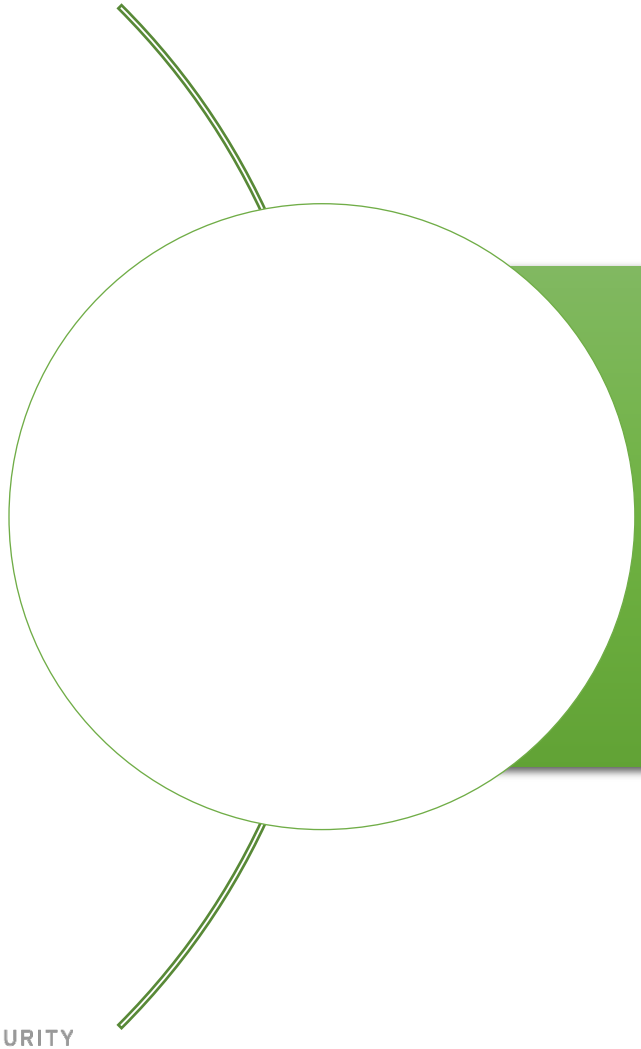
- No individual, business or government entity is solely responsible for securing the Internet. Everyone has a role in securing their part of cyberspace, including the devices and networks they use.
- Individual actions have a collective impact and when we use the Internet safely we make it more secure for everyone.

Background: The Real Internet

Every two days now we create as much information as we did from the dawn of civilization up until 2003, according to Eric Schmidt of Google.

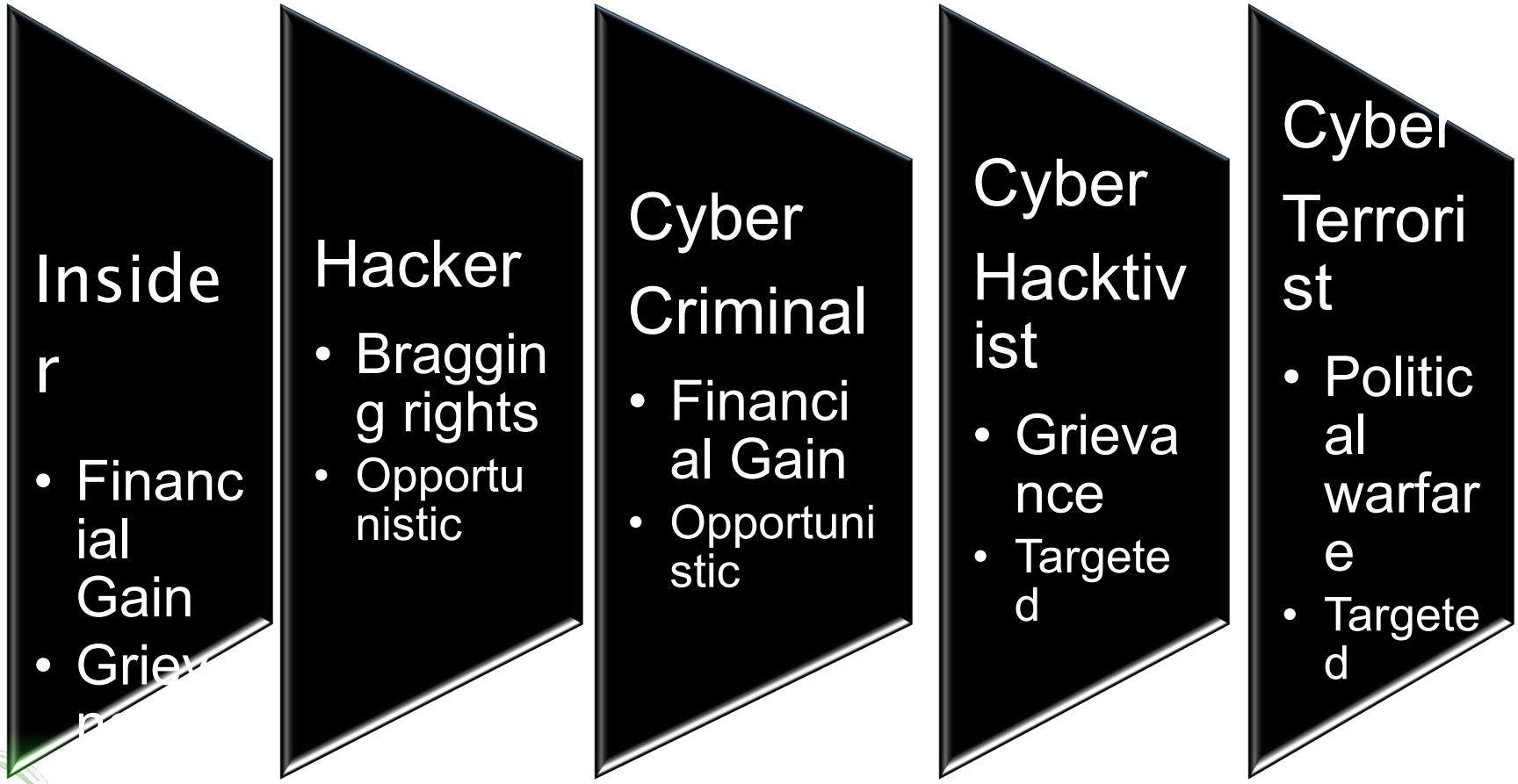


Threat Update

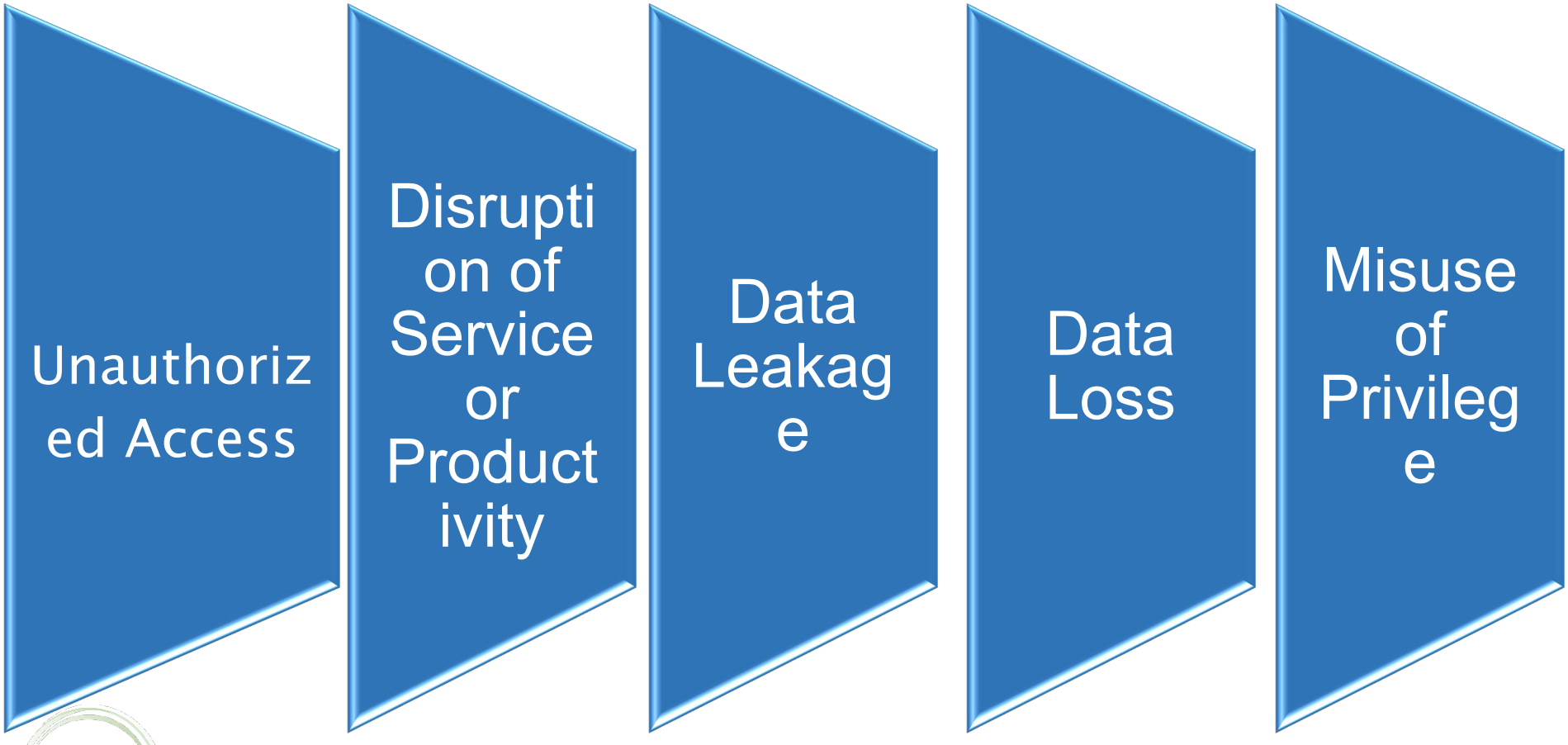


sage DATA SECURITY

Adversaries



Threats


Unauthorized Access
Disruption of Service or Productivity
Data Leakage
Data Loss
Misuse of Privilege

Today's Hacker – Media Fantasy

Today's Hacker - Reality

sage DATA SECURITY

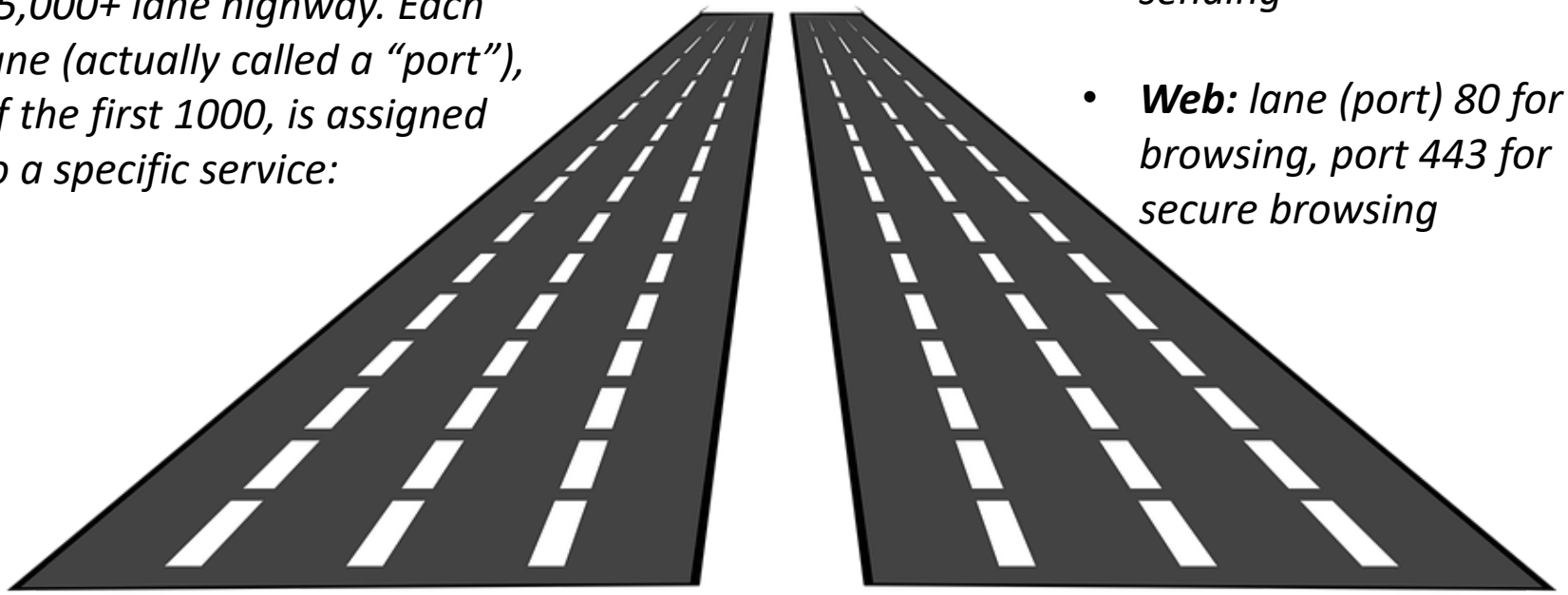
Breach Update

sage DATA SECURITY

Internet Analogies

US Highway System

Think of the Internet as a 65,000+ lane highway. Each lane (actually called a "port"), of the first 1000, is assigned to a specific service:



- ***Email**: lane (port) 110 receiving, port 25 for sending*
- ***Web:** lane (port) 80 for browsing, port 443 for secure browsing*

Internet Analogies

US Postal Service

Data moves through the Internet like regular mail:

- *Sender address*
- *Recipient address*
- *Datagrams*
  - *Packets of information travel across thousands of routes to arrive at their destination and/or connection point.*

Internet Analogies

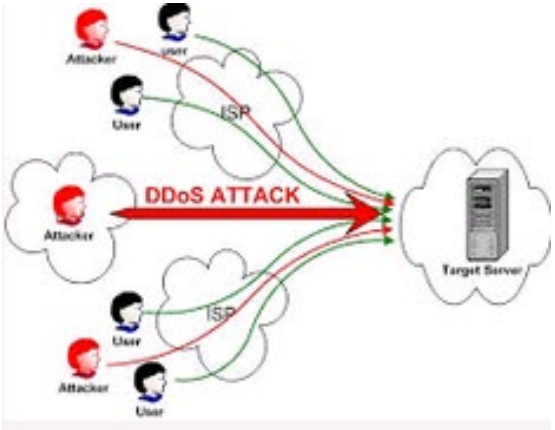
The Phone Book

Domain Name Service
(DNS, Port 53)

- *First, your browser asks DNS to find the website you want to visit.*
- *You type a name, e.g., www.amazon.com,*
- *DNS knows the website's IP Address, and tells your browser, e.g., 44.248.2.125 (IP Address)*
- *"That website is at this address…"*

Threat Landscape

DDoS Attack



Zero Day Vulnerability Exploit

Ransomware

Remote Access Exploits

sage DATA SECURITY

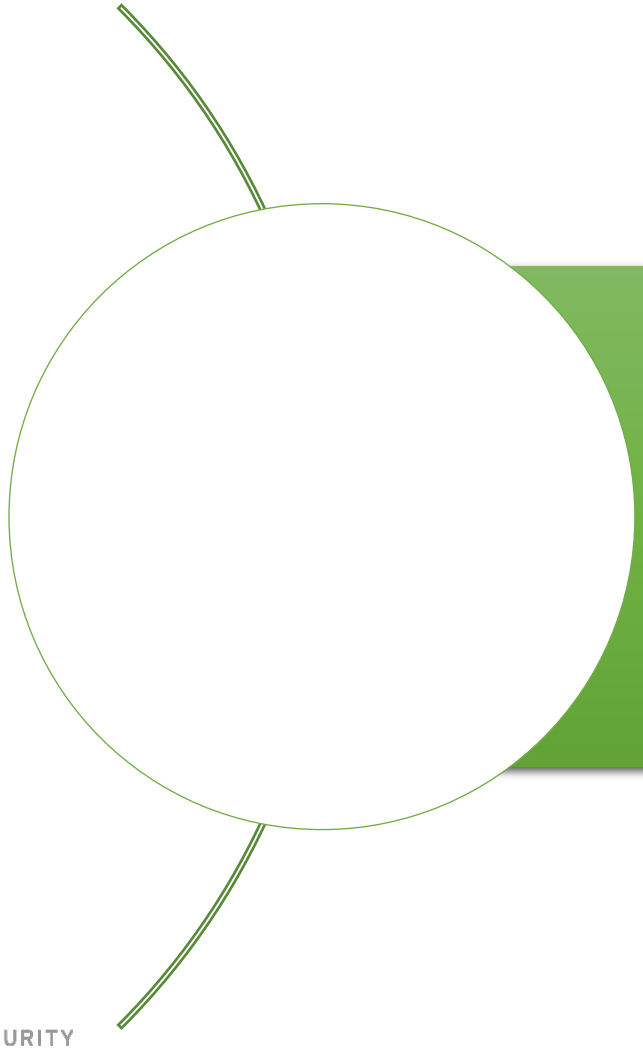
Email Fraud

- Client Email Fraud, theft of severance package
  - Wire Fraud attempt for $30K
  - Procedures were successful in stopping the transfer
- Real Estate Closing
  - Profit on sale stolen from attorneys, $100K loss
- In Maine, 2017
  - HELOC Fraud via wire transfer request
  - $232K Loss, 2 wires
  - Fraudster phished the couple, forwarded their phone to his cell phone, compromised email account, issued wire requests, and knew enough to answer all authentication questions.

sage DATA SECURITY

*FinCEN Advisory FIN-2016-A003 Financial Crimes Enforcement Network

Recognizing Fraud



sage DATA SECURITY

Email Fraud

E-mail Compromise Fraud: Schemes in which criminals compromise the e-mail accounts of victims to send fraudulent wire transfer instructions to financial institutions in order to misappropriate funds. The main types of e-mail compromise fraud include:

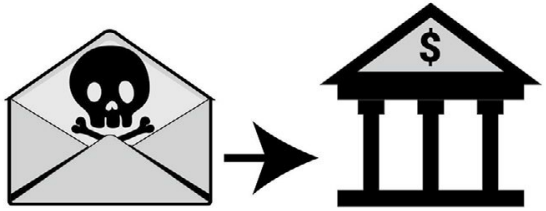
- Business Email Compromise
  - Targets a financial institution's commercial customers
- E-mail Account Compromise
  - Targets personal accounts

*FinCEN Advisory FIN-2016-A003 Financial Crimes Enforcement Network

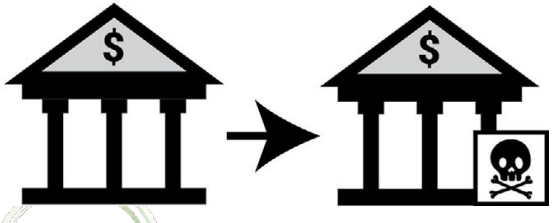
Email Fraud

Stage 1 – Compromising Victim Information and E-mail Accounts: Criminals first unlawfully access a victim's e-mail account through social engineering[3] or computer intrusion techniques. Criminals subsequently exploit the victim's e-mail account to obtain information on the victim's financial institutions, account details, contacts, and related information.

Stage 2 – Transmitting Fraudulent Transaction Instructions: Criminals then use the victim's stolen information to e-mail fraudulent wire transfer instructions to the financial institution in a manner appearing to be from the victim. To this end, criminals will use either the victim's actual e-mail account they now control or create a fake e-mail account resembling the victim's e-mail.



Stage 3 – Executing Unauthorized Transactions: Criminals trick the victim's employee or financial institution into conducting wire transfers that appear legitimate but are, in fact, unauthorized. The fraudulent transaction instructions direct the wire transfers to the criminals' domestic or foreign bank accounts. Banks in Asia—particularly in China and Hong Kong—are common destinations for these fraudulent transactions.



*FinCEN Advisory FIN-2016-A003 Financial Crimes Enforcement Network

Email Fraud - Email Account Compromise

Scenario 1 – Lending/Brokerage Services: A criminal hacks into and uses the e-mail account of a financial services professional (such as a broker or accountant) to e-mail fraudulent instructions, allegedly on behalf of a client, to the client's bank or brokerage to wire-transfer client's funds to an account controlled by the criminal.

Scenario 2 – Real Estate Services: A criminal compromises the e-mail account of a realtor or of an individual purchasing or selling real estate, for the purposes of altering payment instructions and diverting funds of a real estate transaction (such as sale proceeds, loan disbursements, or fees). Alternately, a criminal hacks into and uses a realtor's e-mail address to contact an escrow company, instructing it to redirect commission proceeds to an account controlled by the criminal.

Scenario 3 – Legal Services: A criminal compromises an attorney's e-mail account to access client information and related transactions. The criminal then e-mails fraudulent transaction payment instructions to the attorney's financial institution. Alternatively, the criminal may compromise a client's e-mail account to request wire transfers from trust and escrow accounts the client's attorney manages.

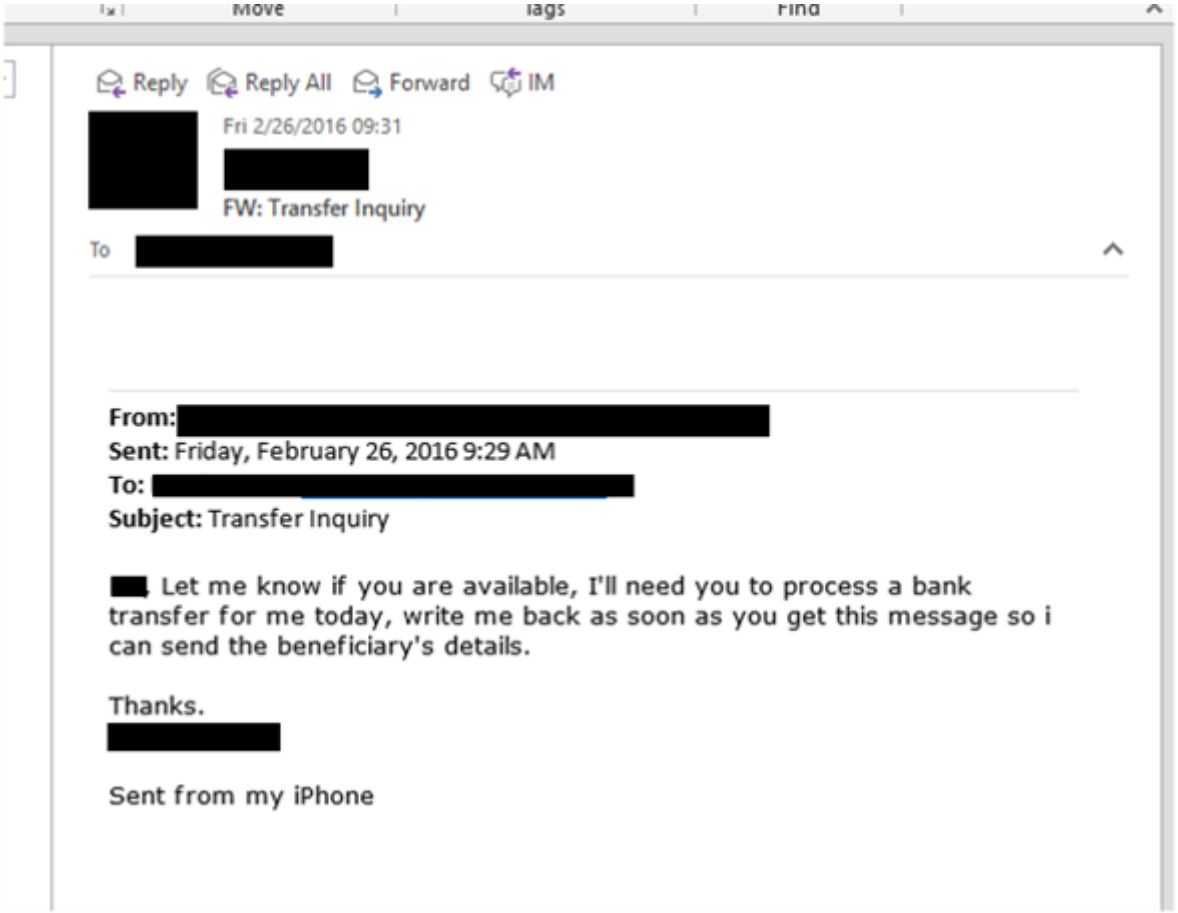
*FinCEN Advisory FIN-2016-A003 Financial Crimes Enforcement Network

Email Fraud: Whale Phishing

A phishing attack that targets significant and/or leadership personnel.

- Attacker impersonates leadership
- Sends instructions for transactions
- Tone is demanding, “must be handled quickly.”
- Chance of bigger pay-off for criminals

Email Fraud: Whale Phishing



Email Fraud: Whale Phishing

From: Greg Oler [mailto: @udel.edu]
Sent: Wednesday, November 09, 2016 7:38 AM
To: @udel.edu>
Subject: Payment Request.....

Hello

Hope your day is going on well. Are you at your desk to process a payment to a new Vendor today?

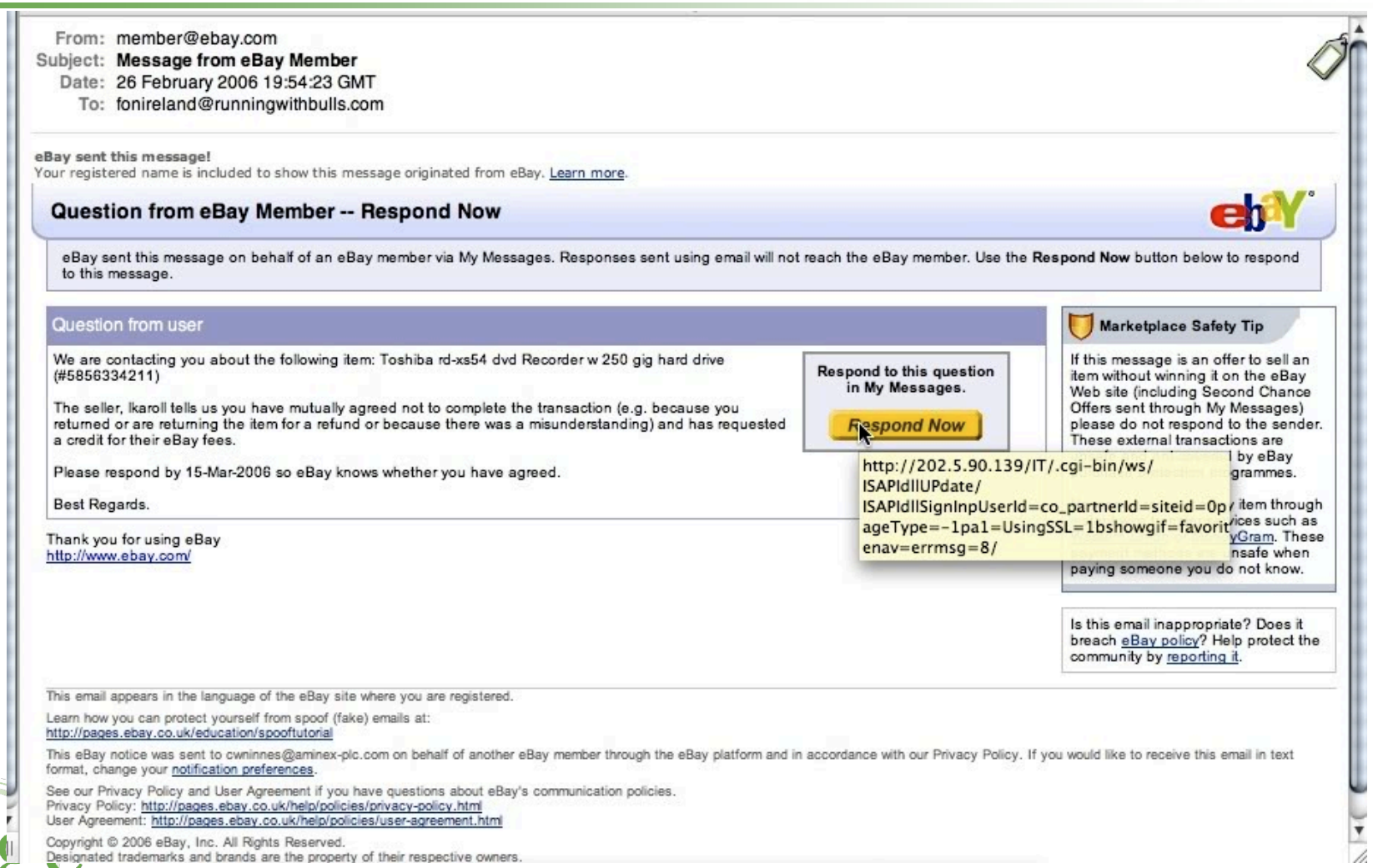
I will appreciate a swift responds and wants the payment to be completed before the end of the day.

Thanks!

Regards,

Greg

Email Fraud – Other Examples of Email Fraud



From: member@ebay.com
Subject: **Message from eBay Member**
Date: 26 February 2006 19:54:23 GMT
To: fonireland@runningwithbulls.com

eBay sent this message!
Your registered name is included to show this message originated from eBay. Learn more.

Question from eBay Member -- Respond Now

eBay sent this message on behalf of an eBay member via My Messages. Responses sent using email will not reach the eBay member. Use the **Respond Now** button below to respond to this message.

Question from user

We are contacting you about the following item: Toshiba rd-xs54 dvd Recorder w 250 gig hard drive (#5856334211)

The seller, lkaroll tells us you have mutually agreed not to complete the transaction (e.g. because you returned or are returning the item for a refund or because there was a misunderstanding) and has requested a credit for their eBay fees.

Please respond by 15-Mar-2006 so eBay knows whether you have agreed.

Best Regards.

Thank you for using eBay
http://www.ebay.com/

Respond to this question in My Messages.

Respond Now

http://202.5.90.139/IT/.cgi-bin/ws/
ISAPIdllUPdate/
ISAPIdllSignInpUserId=co_partnerId=siteid=0p
ageType=-1pa1=UsingSSL=1bshowgif=favorit
enav=errmsg=8/

Marketplace Safety Tip

If this message is an offer to sell an item without winning it on the eBay Web site (including Second Chance Offers sent through My Messages) please do not respond to the sender. These external transactions are
by eBay
grammes.
item through
ices such as
yGram. These
nsafe when
paying someone you do not know.

Is this email inappropriate? Does it breach eBay policy? Help protect the community by reporting it.

This email appears in the language of the eBay site where you are registered.

Learn how you can protect yourself from spoof (fake) emails at:
http://pages.ebay.co.uk/education/spooftutorial

This eBay notice was sent to cwinnes@aminex-plc.com on behalf of another eBay member through the eBay platform and in accordance with our Privacy Policy. If you would like to receive this email in text format, change your notification preferences.

See our Privacy Policy and User Agreement if you have questions about eBay's communication policies.
Privacy Policy: http://pages.ebay.co.uk/help/policies/privacy-policy.html
User Agreement: http://pages.ebay.co.uk/help/policies/user-agreement.html

Copyright © 2006 eBay, Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.

*FinCEN Advisory FIN-2016-A003 Financial Crimes Enforcement Network

Email Fraud – Other Examples of Email Fraud

From: anthem@healthcare-net.com
To: Henry, Garrett
Cc:
Subject: You have not registered for All Clear ID protection service.
Sent: Fri 4/10/2015 12:39

This email did not come from Anthem. The source address is from healthcare-net.com

Anthem

Note: Since the email was not expected, it should immediately be considered suspicious. You can call Anthem or visit their website to verify the legitimacy of the email.

How to Access & Sign Up For Identity Theft Repair & Credit Monitoring Services

http://anthem.healthcare-net.com/anthem/mainf5bp81wqt.html
Click to follow link

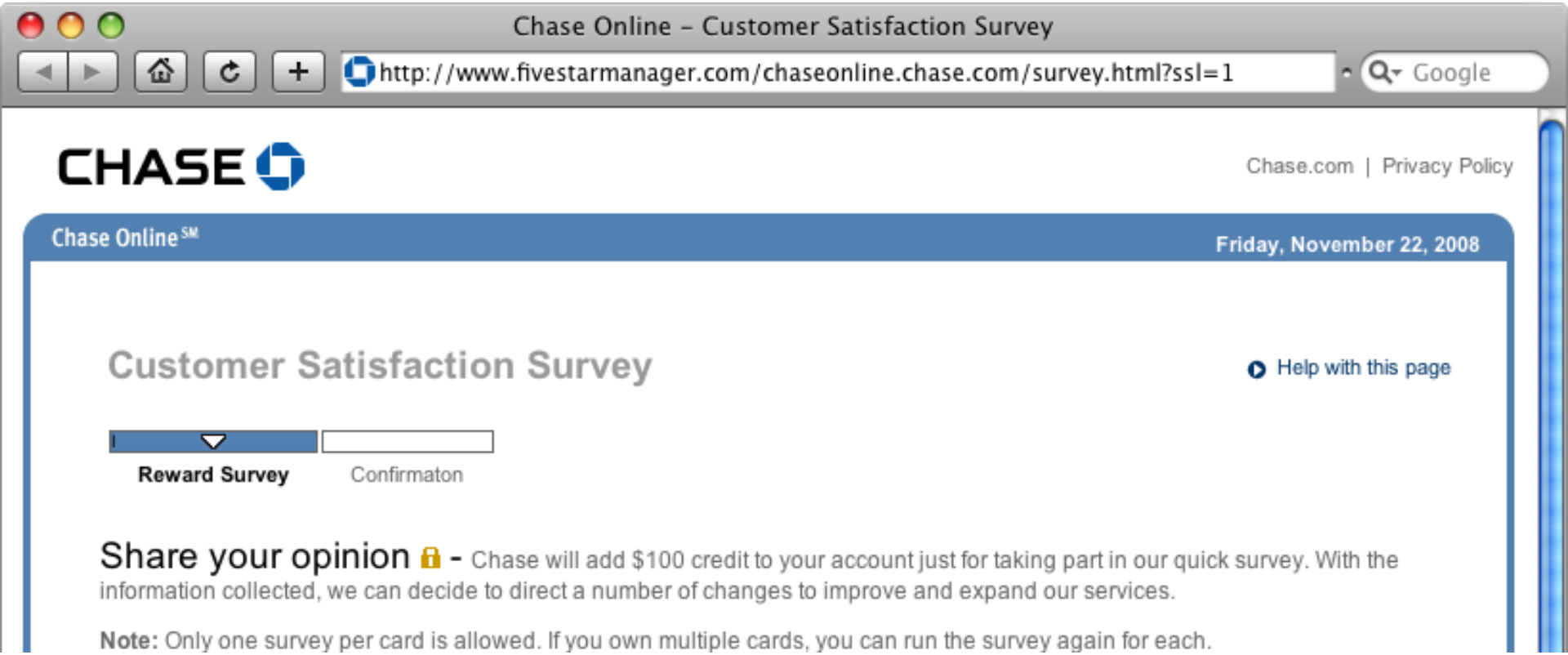
If I hover over the link, I notice that the web address does not point to allclearid.com!

For the fastest & easiest service, enroll online at:https://anthem.allclearid.com/

Anthem is working with All Clear ID, a leading and trusted identity protection provider, to offer 24 months of identity theft repair and credit monitoring services to current or former members of an affected Anthem plan dating back to 2004.

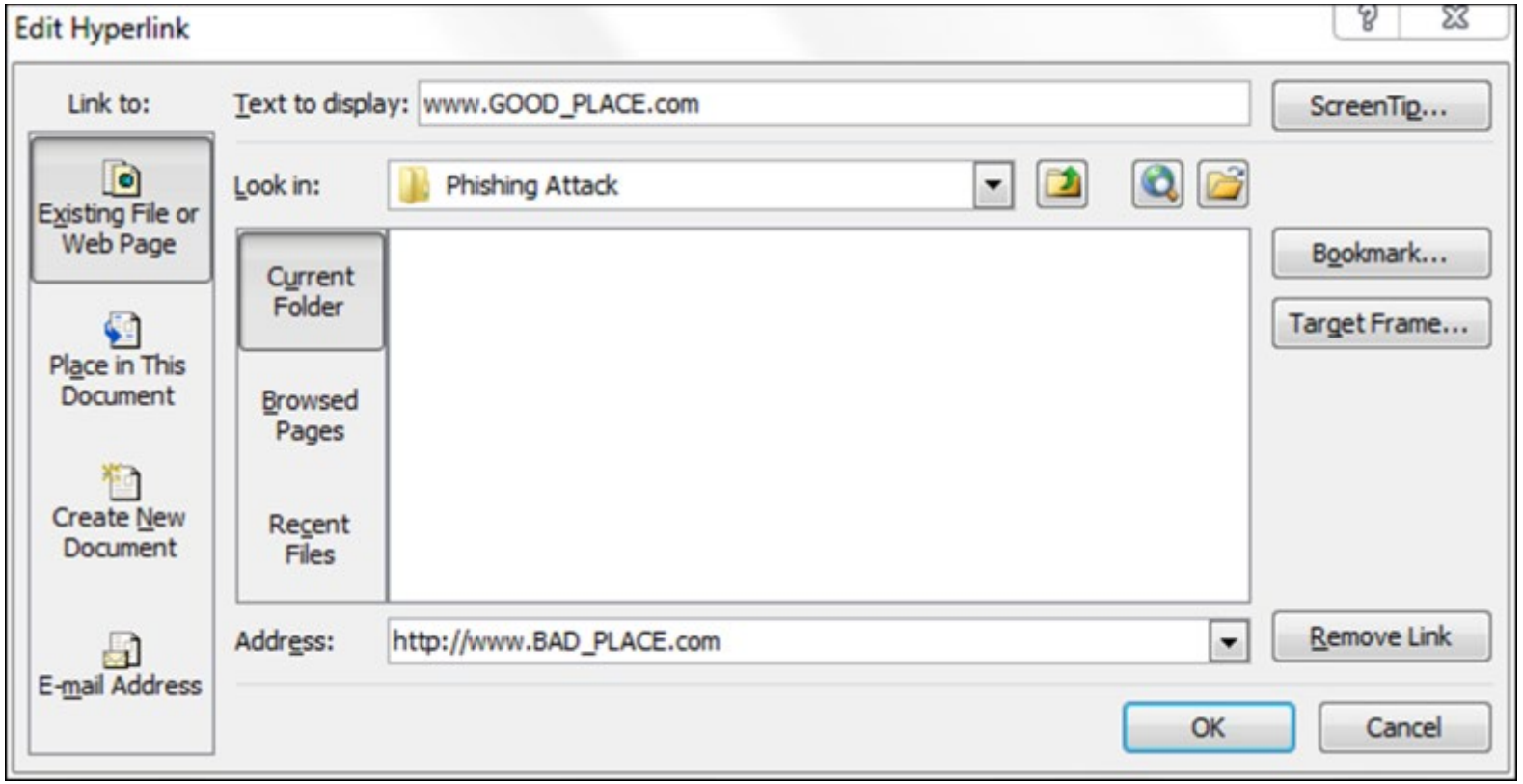
*FinCEN Advisory FIN-2016-A003 Financial Crimes Enforcement Network

Website Fraud – Other Examples of Fraud

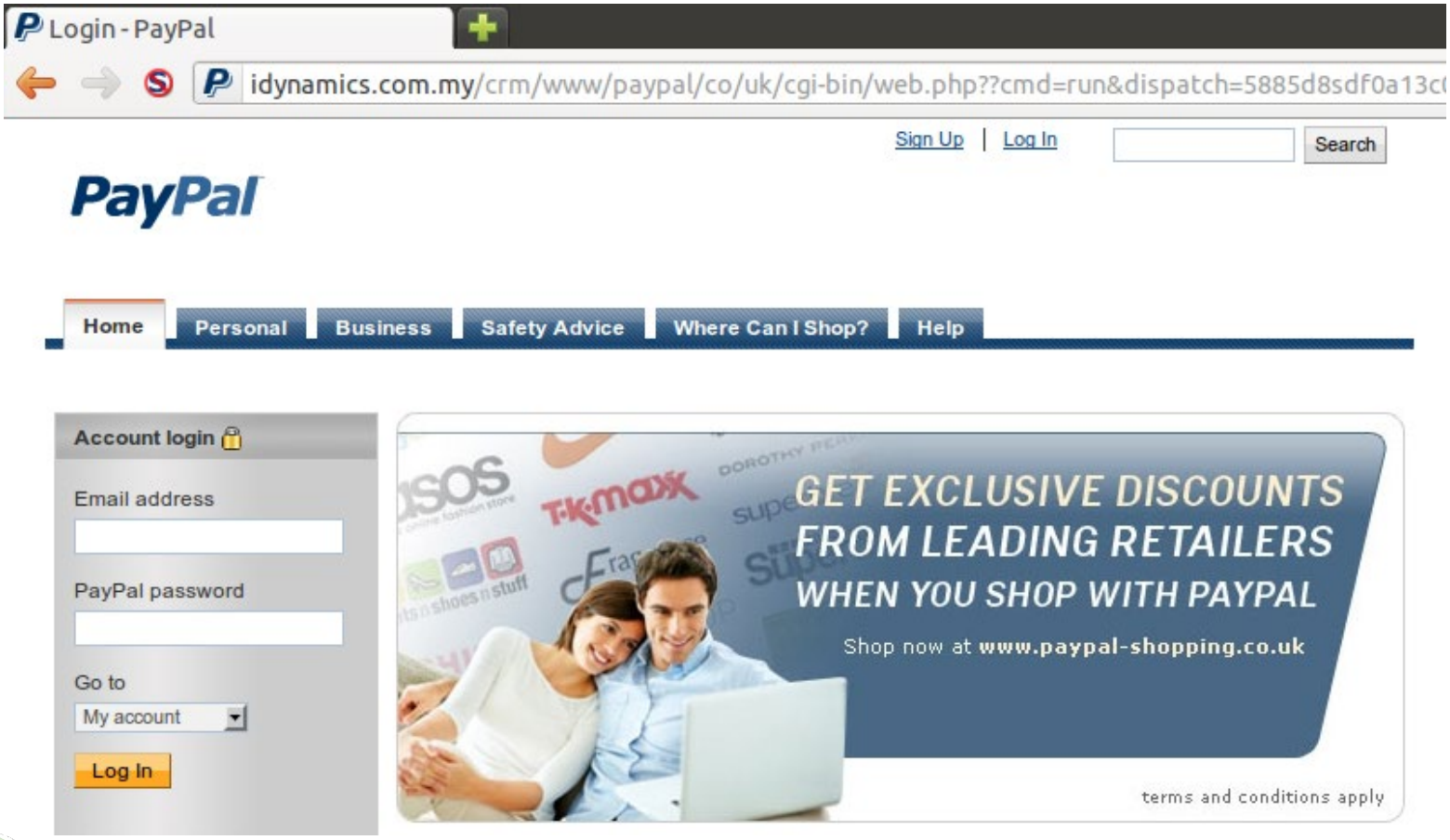


*FinCEN Advisory FIN-2016-A003 Financial Crimes Enforcement Network

Delivery Channels : Phishing Emails



Website Fraud – Other Examples of Fraud



*FinCEN Advisory FIN-2016-A003 Financial Crimes Enforcement Network

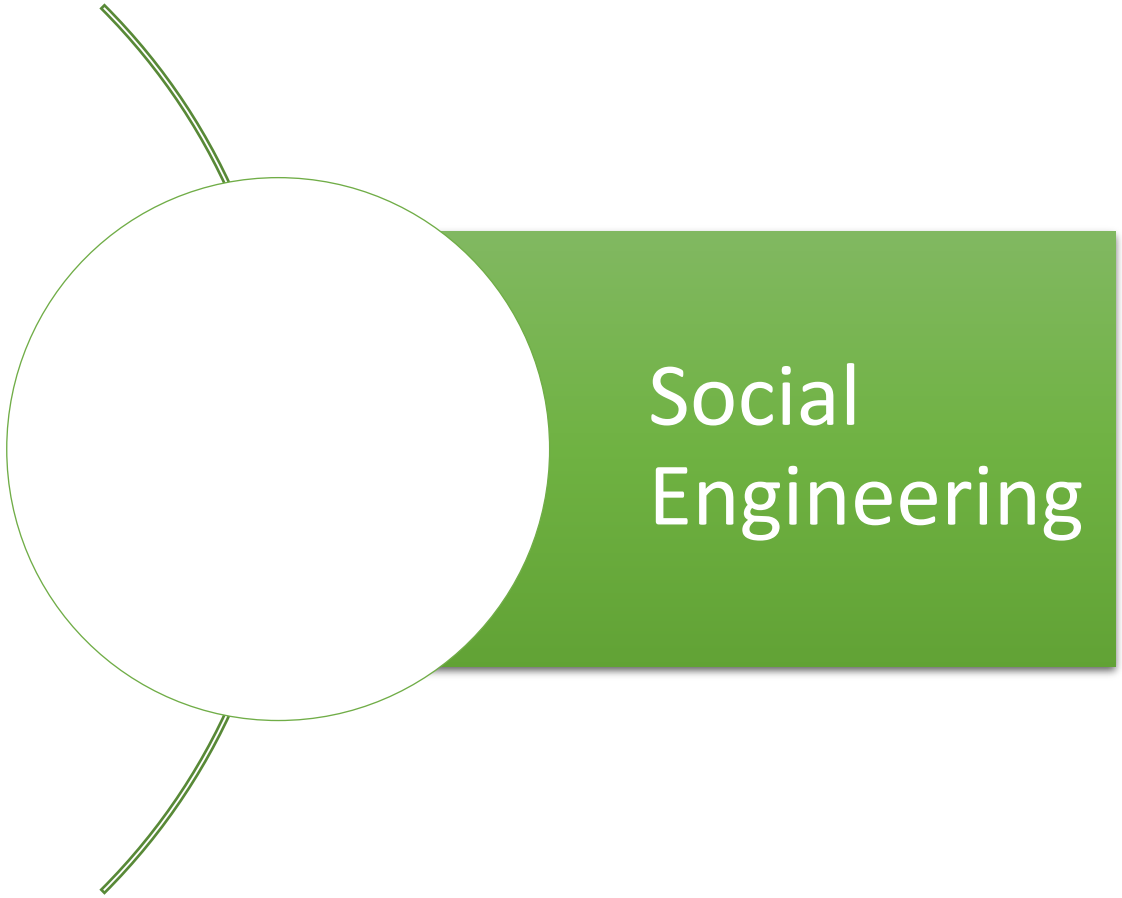
Text Message Fraud- Smishing

- SMS Text Message Fraud
  - Three instances in the last month
  - Text messages are sent to an area code claiming problems with a debit/credit card type
  - Phone number is included
  - No specific financial institution is named
  - Callers are asked for:
    - Name on card
    - Debit/Credit Card number
    - Expiration date
    - 3-digit security code

Device Fraud - Skimmers

- **What is a Skimmer?**
  - A set of physical devices applied to a Point of Sale Terminal (POS) or an ATM
  - Devices allow the bad actors to capture both the electronic information from a card and the keyed in PIN / Access code the customer may use
  - The devices have become so good they are very hard to distinguish from the authorized equipment and in some cases may not be visible at all

Agenda



The Human Factor

Why We're All Vulnerable

Goal of Social Engineering is the acquisition of sensitive information or inappropriate access privileges by an outsider based upon the building of trusted or intimidating relationship with insiders.

Social Engineering preys on qualities of human nature:

- the desire to be helpful.
- the tendency to trust people.
- the fear of getting into trouble.

The sign of a truly successful social engineer is that they receive information without raising any suspicion as to what they were doing.

SpoofCard

sage DATA SECURITY

The Human Factor

- Common Attacks | Delivery Channels
  - Email Phishing: Posing as a legitimate business/service
  - Vendor Spoofing: Posing as a vendor on a service call
  - IT/IS Spoofing: Posing as internal IT or IS department staff
  - Website Spoofing: Creating phony websites that appear to be legitimate
  - Phone Spoofing: Caller ID

Defenses

Defense = Situational Awareness

sage DATA SECURITY

Defense: Tips & Tricks

- **Can I call you back?**
  - Simple phrase ends most telephone pretexting attacks
  - If caller provides number, google the number to ensure it is a legitimate organization
  - Should be standard procedure for all IT Helpdesk communication
  - There is no such thing as “innocuous” information

Defense: Tips & Tricks

- **Did I initiate this communication?**
  - If the answer is yes, go ahead and click, go ahead and answer the question.
  - If the answer is no, don't click, and don't answer.
  - Examples:
    - IRS calls you and asks for your social security #
      - Did you initiate? NO!
    - You call IRS and they ask for your social security #
      - Did you initiate? YES!
    - You sign-up for mobile banking on your bank's website, the bank immediately sends an email to verify your email address.
      - Did you initiate? YES!
    - You receive an email from your bank that there is a problem with your account
      - Did you initiate? NO!

Defense: Tips & Tricks

- **Forward Slash and Two Dots Back**
  - This is the formula to determine the actual URL you are visiting.
  - Fraudsters use many types of URL constructions to deceive:
    - http://www.jetblue.**seetssavers.com/**row/usa/....
    - http://www.yourbank.**com.mx/**communicate/tweet/current...
    - http://login.**auction.info/**www.ebay.com/buyer/seller/....
    - http://www.**amazone.com/**043094/abc/....

*Important to remember, this is not 100% rule, but does apply to most situations.

Defense: Tips & Tricks

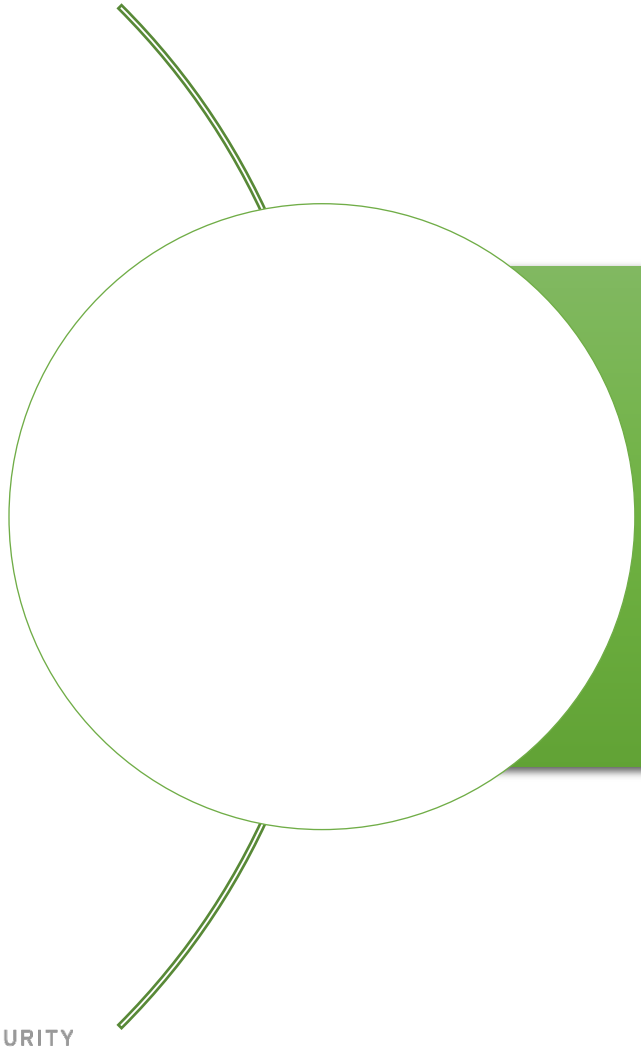
- **Am I expecting this?**
  - Attachments that are unexpected should be treated with suspicion.
  - If your role requires you open unexpected attachments, scan the attachment with anti-virus software –usually found on the “right click” menu.
  - If your role does not require, never open unexpected attachments.

Defense: Situational Awareness

- **Mindful Use**
  - We are called to develop new habits, and we know how to do that:
    - Seatbelts
    - Diet/Exercise
    - Smoking
  - Mindful Use habits carry from work to home to anywhere you use Internet-connected resources.
  - Situational awareness is increased by mindful use habits.

Can You Spot the Fraud?

https://www.opendns.com/phishing-quiz/?__utma=5277664.1308558171.1462993826.1463062975.1463062975.1&__utmb=5277664.0.10.1463062975&__utmc=5277664&__utmx=-&__utmz=5277664.1463062975.1.1.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided)&__utmv=-&__utmk=227333017



Questions & Answers

sage DATA SECURITY

Thank you for attending!

Presented by:
John H. Rogers, CISSP
Director of Advisory Services
john.rogers@sagedatasecurity.com

Copyright Sage Data Security 2018© All Rights Reserved