# Behavioral Aspects of Cybersecurity "Decision Making"

Bruce Caulkins, Ph.D.

School of Modeling, Simulation & Training (SMST)
University of Central Florida



# **AGENDA**

- Introduction to Human Factors & Cybersecurity
- Decision Making
  - Individual Differences



It is no longer enough to create a secure infrastructure for information. Organizations must also address the *human* factors of cybersecurity by cultivating an informed and proactive workforce.



### **HUMAN FACTORS & CYBERSECURITY**

1. What has Human Factors got to do with Cybersecurity?

Scientific principles of *perception*, *decision making*, *action selection*, and *training* that have been developed in basic and applied cognitive research can provide a principled basis for analyzing the factors affecting security-related human decisions and choices.

PERCEPTION -> DECISION MAKING -> ACTION SELECTION



## **HUMAN FACTORS & CYBERSECURITY**

### **PERCEPTION**

- Perception of information
- Views on security, risk perception (bias, heuristics)

### **DECISION MAKING**

- Individual Differences
- Expert vs. novice decision making
- Decision making under stress, over/underload, fatigue
- Bias and heuristics that affect decision making
- Factors that contribute to vulnerability (weapons of influence, social engineering etc.)

### **ACTION SELECTION**

Ease of implementing response required

### **TRAINING**

Organizational factors

### **SYSTEM DESIGN**

Features of task, website etc.

### **HUMAN FACTORS & CYBERSECURITY**

### **PERCEPTION**

- Perception of information
- Views on security risk perception (higs heuristics)

### **DECISION MAKING**

- Individual Differences
- Expert vs. novice decision making
- Decision making under stress, over/underload, fatigue
- Bias and heuristics that affect decision making
- Factors that contribute to vulnerability (weapons of influence, social engineering etc.)

### **ACTION SELECTION**

Ease of implementing response required

### **TRAINING**

Organizational factors

### **SYSTEM DESIGN**

Features of task, website etc.

# Decision Making: Introduction

- 1. In the cyber context, decisions are made:
  - Before a cyberattack (i.e., Users deciding whether or not to engage in safe/unsafe behavior)
    - People may be more complacent and prone to thinking heuristically online
    - Principles of persuasion/Weapons of influence
  - When an attack is suspected/during an attack (i.e., System administrators deciding what to do)

# Decision Making: Introduction

### 1. In the cyber context, decisions are made:

- Before a cyberattack (i.e., Users deciding whether or not to engage in safe/unsafe behavior)
  - People may be more complacent and prone to thinking heuristically online
  - Principles of persuasion/Weapons of influence
- When an attack is suspected/during an attack (i.e., System administrators deciding what to do)

### 2. Decision Making and trade-offs

- Safety vs. Potential Gains/Losses
- Safety vs. Convenience/Expediency

# Decision Making: Introduction

### 1. In the cyber context, decisions are made:

- Before a cyberattack (i.e., Users deciding whether or not to engage in safe/unsafe behavior)
  - People may be more complacent and prone to thinking heuristically online
  - Principles of persuasion/Weapons of influence
- When an attack is suspected/during an attack (i.e., System administrators deciding what to do)

### 2. Decision Making and trade-offs

- Safety vs. Potential Gains/Losses
- Safety vs. Convenience/Expediency

### 3. Decision Making under stress

- Workload, fatigue, attentional narrowing
- Hypotheses formulation and testing (when under attack), bias and heuristics
- Role of expertise

 Extraversion: higher sociability and excitement-seeking, may be tend to violate security policies, take risks

- Extraversion: higher sociability and excitement-seeking, may be tend to violate security policies, take risks
- Conscientiousness: higher tendency to follow through with commitments, may be susceptible to continuance commitment tactics

- Extraversion: higher sociability and excitement-seeking, may be tend to violate security policies, take risks
- Conscientiousness: higher tendency to follow through with commitments, may be susceptible to continuance commitment tactics
- Agreeableness: tend to be more trusting, may have increased susceptibility to phishing, share passwords

- Extraversion: higher sociability and excitement-seeking, may be tend to violate security policies, take risks
- Conscientiousness: higher tendency to follow through with commitments, may be susceptible to continuance commitment tactics
- Agreeableness: tend to be more trusting, may have increased susceptibility to phishing, share passwords
- Neuroticism: greater anxiety, more cautious, may be protective, but...
  - Those who were high on neuroticism tend to fall for prize phishing email

- Extraversion: higher sociability and excitement-seeking, may be tend to violate security policies, take risks
- Conscientiousness: higher tendency to follow through with commitments, may be susceptible to continuance commitment tactics
- Agreeableness: tend to be more trusting, may have increased susceptibility to phishing, share passwords
- Neuroticism: greater anxiety, more cautious, may be protective, but...
  - Those who were high on neuroticism tend to fall for prize phishing email
- Openness: tend to seek new experiences, lower concern with privacy settings
  - Those high on openness tend to post more info on Facebook, less strict privacy settings 

    increased phishing vulnerability

# **Decision Making: Authority**

- People are more likely to do something when an authority figure tells them to do it.
  - Authority figures are more credible, have more expertise, have opinions that are more valuable, and are more influential. (i.e., Milgram's expts)
    - Ex. Phishing scam in 2012: emails were sent to US Department of Defense military members and were seemingly from the Defense Finance and Accounting Services



# **Decision Making: Authority**

- People are more likely to do something when an authority figure tells them to do it.
  - Authority figures are more credible, have more expertise, have opinions that are more valuable, and are more influential. (i.e., Milgram's expts)
    - Ex. Phishing scam in 2012: emails were sent to US Department of Defense military members and were seemingly from the Defense Finance and Accounting Services
- Defense: (i) Is this person truly an expert? (ii)
  How truthful would I expect this person to be
  based on his/her position?



# **Decision Making: Authority**

### **Phishing Scam**

The e-mails display a spoofed .mil e-mail address and say that recipients of disability compensation from the Veterans Affairs Department could also be eligible to get money from the IRS, DFAS said. The phishing scam asks recipients to submit their VA award letters, income tax returns, 1099-R forms and other documents to a supposed retired colonel in Florida.



### ACCOUNTING SERVICE



### FIANCE REQUEST FORM

THIS IS A SCAM

The Fiancée is to complete the data below correctly and in capital letter in respective of the military officer:

SECTION A (FIANCEE):

NAME:

SEX:

ADDRESS: ZIP CODE:

PHONE NUMBER:

CITY: STATE:

NOTE: The registration fee (\$350.00)

SECTION B (MILITARY OFFICER):

NAME:

SEX: RANK:

BRANCH:

STATE OF DEPLOYMENT:

DATE:

Once you provide us with the above information you are no longer anonymous to us, you will be registered in our data base as the fiancée and you will be entitled to his entire asset upon death or natural circumstance.

(We) protect your privacy. We do not insist you to provide extra personal information than necessary.

All information collected will not be used for any illegal activity The information is what we are going to use to register you with our service. Remember, the aforementioned fee is refundable

ONLY REGISTERED FIANCEE WILL QUALIFIED TO REQUEST FOR LEAVE ON BEHALF OF HER FIANCE.

Regards,

DFAS.

Feel free to our service (dfasmilitary@aol.com) Information and data collection server Copyright by DFAS. All Rights Reserved



# Decision Making: Social Proof

- When unsure, people are more likely to do something when others are doing it
  - Diffusion of Responsibility
  - When users notice that many of their friends installed an application on Facebook, they are more likely to do so themselves (Goodchild, 2009)
  - Social engineers/computer programmers can encourage certain behaviors by generating fake "likes", and artificially increasing no. of followers on social media to give the impression that others are supporting that behavior (Finkle, 2013)

# Decision Making: Social Proof

- When unsure, people are more likely to do something when others are doing it
  - Diffusion of Responsibility
  - When users notice that many of their friends installed an application on Facebook, they are more likely to do so themselves (Goodchild, 2009)
  - Social engineers/computer programmers can encourage certain behaviors by generating fake "likes", and artificially increasing no. of followers on social media to give the impression that others are supporting that behavior (Finkle, 2013)
- Defense: Remind yourself that just because others are doing it, doesn't mean you have to follow. Recognize and isolate the influence from others' behaviors

# Decision Making: Likability & Similarity

- People are more likely to do something when someone likeable asks them to do it
  - Likeable people are more influential. They tend to be more familiar, similar to us, and are perceived as being more trustworthy.
  - Decision heuristic: "Likeable = Good source of information"
  - Deception tactic by using someone likeable or making oneself likeable to the victim (i.e., befriend and build rapport over time), to influence the victim to do something
    - E.g., People are more likely to open email simply because it is from a friend (person they like and probably trust)
    - Phishing scam "Stranded Traveler"

# Decision Making: Likability & Similarity

- People are more likely to do something when someone likeable asks them to do it
  - Likeable people are more influential. They tend to be more familiar, similar to us, and are perceived as being more trustworthy.
  - Decision heuristic: "Likeable = Good source of information"
  - Deception tactic by using someone likeable or making oneself likeable to the victim (i.e., befriend and build rapport over time), to influence the victim to do something
    - E.g., People are more likely to open email simply because it is from a friend (person they like and probably trust)
    - Phishing scam "Stranded Traveler"
- Defense: Separate the likeable person from the request would you still comply if someone else asked it?



### Arnie Arnesen

Sent: Monday, November 11, 2013 12:01 PM

To:

You forwarded this message on 11/11/13 12:15 PM.

You replied to this message on 11/11/13 1:20 PM.

Hello,

Hope you're OK?. I'm writing to let you know that I am currently in London, United Kingdom for a Radio Presentation.

At the moment, I have a little problem that i hope you can help me with.

The favor is a loan till I return home in a few days time.

Please let me know if you are able to assist so i can tell you the amount i need.

Hope to Hear from you soon.

Best regards, ARNIE.

--

KEEPING THE POT STIRRED SO SCUM DOESN'T RISE TO THE TOP - Anonymous

### D. ARNIE ARNESEN

15 Rumford Street Concord NH 03301 politicalchowder@gmail.com (C) 603-321-7654

### Arnie on the air?

The Attitude with Arnie Arnesen 94.7 FM WNHN Concord NH (M-F/ 11am to 1pm EST) streaming live at: <a href="www.nhnewsviewsblues.org">www.nhnewsviewsblues.org</a>
<a href="www.nhnewsviewsblue

### Arnie in print?

<u>www.insideriowa.com</u> - The Intersection of Big Ideas and News (check out Politics - Red and Blue) Silver winner in 2010 W3 Awards News Category Concord Monitor - regular contributor

# Decision Making: Commitment & Consistency

- When an individual agrees to an initial request, s/he will tend to comply with subsequent requests
  - In general, people want to be consistent and appear (to themselves and others) to have integrity. So they will tend to try to follow through with their commitments.
  - Ask for something small first, then the subsequent larger request will be more likely to be fulfilled (Foot-in-the-door technique).
    - E.g., "Please provide your email address.....and your mailing address and DOB"
    - E.g., After giving in to the "Stranded Traveler" the 1<sup>st</sup> time, people are more likely to give in the 2<sup>nd</sup> time etc.

# Decision Making: Commitment & Consistency

- When an individual agrees to an initial request, s/he will tend to comply with subsequent requests
  - In general, people want to be consistent and appear (to themselves and others) to have integrity. So they will tend to try to follow through with their commitments.
  - Ask for something small first, then the subsequent larger request will be more likely to be fulfilled (Foot-in-the-door technique).
    - E.g., "Please provide your email address.....and your mailing address and DOB"
    - E.g., After giving in to the "Stranded Traveler" the 1<sup>st</sup> time, people are more likely to give in the 2<sup>nd</sup> time etc.
- Defense: Recognize that you may be influenced to do something that you don't want to do. Think about whether you will regret later if you complied

# **Decision Making: Scarcity**

- People will tend to take action when they perceive that they may be missing out on something valuable
  - Scarce or difficult-to-come-by objects or opportunities are perceived as more valuable.
  - When people are overloaded with information, they may tend to transit to a "mentally passive" social state and "absorb information rather than evaluating it" (Burtner, 1991)
  - Applying time pressure (e.g., K-mart's Blue light specials) gives victims less time to think rationally and they rely on heuristics and bias more.
    - E.g., The Koobface malware (virus) was engineered to contain a link to "secret" or hard to find media (Goodchild, 2009a). By making access to this media appear to be limited, it encourages users to click on the link because this makes it suddenly seem more desirable.
    - E.g., "Limited time only" offers. In 2011, links were sent out via emails and Facebook purporting to offer \$100 Walmart gift cards "for a limited time only" (Spilewsky & Healy, 2012).

# **Decision Making: Scarcity**

- People will tend to take action when they perceive that they may be missing out on something valuable
  - Scarce or difficult-to-come-by objects or opportunities are perceived as more valuable.
  - When people are overloaded with information, they may tend to transit to a "mentally passive" social state and "absorb information rather than evaluating it" (Burtner, 1991)
  - Applying time pressure (e.g., K-mart's Blue light specials) gives victims less time to think rationally and they rely on heuristics and bias more.
    - E.g., The Koobface malware (virus) was engineered to contain a link to "secret" or hard to find media (Goodchild, 2009a). By making access to this media appear to be limited, it encourages users to click on the link because this makes it suddenly seem more desirable.
    - E.g., "Limited time only" offers. In 2011, links were sent out via emails and Facebook purporting to offer \$100 Walmart gift cards "for a limited time only" (Spilewsky & Healy, 2012).
- Defense: Recognize the increase in anxiety/arousal that resulted from knowing how scarce the opportunity is. Calm down and think more carefully. Scarce may not = good



### ATTENTION U.S. CITIZEN:

### RECEIVE A STIMULUS CHECK BASED ON YOUR INCOME LEVEL.

PARTICIPATION REQUIRED CLICK HERE FOR DETAILS.

### SELECT YOUR ANNUAL SALARY INCOME:

TEARLY SALARY		CHECK AMOUNT	
0	\$0-35,000	\$709	
0	\$35,000-70,000	\$615	
0	\$70,000+	\$504	

### PLEASE ENTER YOUR EMAIL ADDRESS:

CLICK HERE TO CONTINUE

| Control that I am a U.S. Resident over the age of 18, and I agree to the Privacy Policy and Terms & Conditions.

### Why are we offering this?

The United States is facing its worst economy since the Great Depression. Americans are losing their homes, struggling to put food on the table and cutting back on everyday living expenses.

But help is available! Make getting through the tough times easier and let GiftHouse extend a helping hand.

### How is this possible?

Since Giff-louse's sponsors pay to be part of this program, it allows us to give our participants incredible gifts. You'll receive your stimulus check once you complete the gift eligibility requirements.







THANK YOU.

PLEASE TELL US WHERE TO SEND YOUR STIMULUS CHECK.

Zgc	
First Name	
Last Name:	
Address	
Address 2	
City	
State:	Please Select X
Date of Birth	✓ 1991 ✓
Phone.	
Gender:	O Maje O Female

# Decision Making: Reciprocity

- People are more likely to do something if they are first given something
  - People's desires (needs and greed) make them more vulnerable.
    - E.g., Attacker disables victim's Ethernet port, and then contacts the victim posing as help-desk technician. Attacker restores the connection that the victim <u>needs</u> and asks victim to download a 'patch' (actually a Trojan virus) to prevent the problem in future (Mitnick, 2002).
  - Variation: Door-in-the-face technique. Ask for a large favor which will be invariably turned down, then ask for a small favor. The victim will be more likely to agree this time.

# Decision Making: Reciprocity

- People are more likely to do something if they are first given something
  - People's desires (needs and greed) make them more vulnerable.
    - E.g., Attacker disables victim's Ethernet port, and then contacts the victim posing as help-desk technician. Attacker restores the connection that the victim <u>needs</u> and asks victim to download a 'patch' (actually a Trojan virus) to prevent the problem in future (Mitnick, 2002).
  - Variation: Door-in-the-face technique. Ask for a large favor which will be invariably turned down, then ask for a small favor. The victim will be more likely to agree this time.
- Defense: Reject the initial offer. Think about whether the person truly wants to offer something to benefit you

# Decision Making: Strong Affect - Distraction

- People are more likely not to evaluate information carefully when they are distracted (e.g., by strong emotions)
  - When in a heightened emotional state or when preoccupied with other tasks/priorities, people tend not to carefully evaluate information and situations. May be more inclined to use heuristics and show bias.
    - E.g., Email about close relative in need of major surgery who requires help with medical bills.
    - E.g., Company preoccupied with trying to avert the "Y2K" bug (distracter), hires a team of inexpensive programmers from India without doing proper background checks on them (Abagnale, 1999).

# Decision Making: Strong Affect - Distraction

- People are more likely not to evaluate information carefully when they are distracted (e.g., by strong emotions)
  - When in a heightened emotional state or when preoccupied with other tasks/priorities, people tend not to carefully evaluate information and situations. May be more inclined to use heuristics and show bias.
    - E.g., Email about close relative in need of major surgery who requires help with medical bills.
    - E.g., Company preoccupied with trying to avert the "Y2K" bug (distracter), hires a team of inexpensive programmers from India without doing proper background checks on them (Abagnale, 1999).
- Defense: Recognize when you are experiencing strong emotions and avoid making any important decisions until you can refocus (try taking a short walk etc.)

# Individual Differences Recap

Human error affects the success of many cyber operations. Individual differences such as personality traits, skills and abilities play a large role in predicting how both cybersecurity experts and users react to given cyber situations. Knowing more about the individual human can help prevent errors.





Causes









# Next Week

- Decision Making: Human Error
  - Decision making under stress, over/underload, fatigue
  - Bias and heuristics that affect decision making
  - Factors that contribute to vulnerability (weapons of influence, social engineering etc.)



# Behavioral Aspects of Cybersecurity "Decision Making"

Bruce Caulkins, Ph.D.

School of Modeling, Simulation & Training (SMST)
University of Central Florida

