IDC6601: BEHAVIORAL IMPERATIVES

BRUCE D. CAULKINS, PH.D.

ROLE OF HUMANS IN CYBERSECURITY

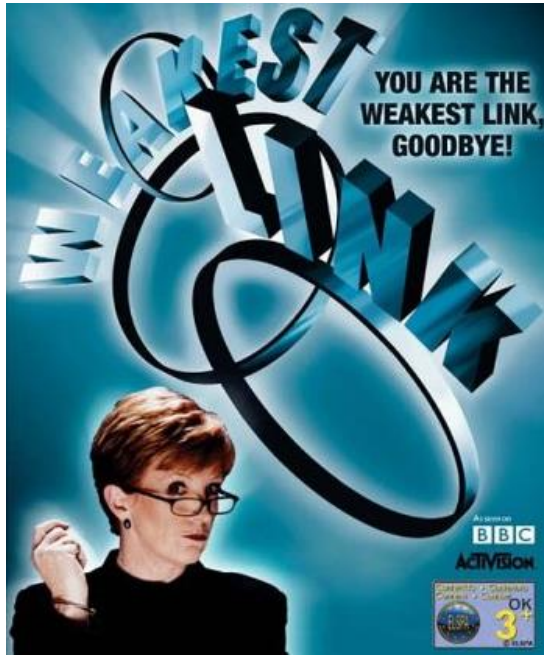
- Humans as system ***developers and designers***
- Humans as ***users and consumers***
- Humans as ***defenders and practitioners*** (i.e., IT dept, network administrators)
- Humans as ***perpetrators and adversaries***

WHAT IS HUMAN FACTORS PSYCHOLOGY?

- Psychology is the study of behavior and the mind
- Human Factors *(excerpt from American Psychological Association, APA)*
  - Human Factors, a.k.a. Ergonomics
  - Study mental processes , i.e., perception, attention, cognition, decision making, action selection etc.
  - Use psychological science to guide the design of products, equipment, devices, hard/software, systems, applications etc.
  - Study of humans and technology at the level of individuals, teams. How humans interact with machines, technology and each other.
  - Focus on performance and safety.
  - Macroergonomics HF (organizational level, intersection with I/O psych)

WHAT HAS HUMAN FACTORS GOT TO DO WITH CYBERSECURITY?

- "The common denominator across the top four [incident] patterns – accounting for nearly 90% of all incidents – is people." (Verizon Data Breach Investigation, 2015)
- "The human factor remains security's weakest link in cyberspace" (Wiederhold, 2014)
- "The application of information security technologies do not always result in improved security" (Parsons et al., 2010)
- "The first level of vulnerability is an organic one – people" (Business Reporter, 2015)
- "Amateurs hack systems, professionals target people" (Schneier, 2000)



STAGES OF A CYBERATTACK

1. **Reconnaissance**: Harvest information (social media etc.), port scans
2. **Weaponization**: Scan for point of access, develop exploit, decoys, "lures"

3. **Delivery**: Gain access, insert malicious software
4. **Exploitation**: Execute malicious code on victim system
5. **Installation/proliferation**: Malware installed, spreads, escalate privileges

6. **Command and control**: Steal/modify/delete data etc.
7. **Take action on objectives** (e.g., demand ransom) or hide tracks (e.g., remove traces of the data theft)

STAGES OF A CYBERATTACK

1. **Reconnaissance**: Harvest information (social media etc.), port scans
2. **Weaponization**: Scan for point of access, develop exploit, decoys, "lures"

3. **Delivery**: Gain access, insert malicious software
4. **Exploitation**: Execute malicious code on victim system
5. **Installation/proliferation**: Malware installed, spreads, escalate privileges

6. **Command and control**: Steal/modify/delete data etc.
7. **Take action on objectives** (e.g., demand ransom) or hide tracks (e.g., remove traces of the data theft)

ACCESS POINTS (TO INSTALL MALWARE)

Access points	Cyberattacks/threats
Passwords	Password attack, Spoofing, Keyloggers
Email	Malware, Social engineering, Phishing, Eavesdropping, Spoofing, Information disclosure
Websites (incl. social media sites)	Social engineering, Man in the middle (impersonate you to the bank, impersonate bank to you), Spoofing
Downloads	Drive-by downloads, Spoofing

ATTACK PATTERNS

Attack Scenarios	Motivation	By whom?
1. Inside jobs: exploit position in company	Sabotage, retaliation	Organized crime, end-users
2. Social Engineering: usually through low-tech, or non-technical methods	Obtain valuable info. through impersonation, deception, persuasion to commit unsafe acts (e.g., to reveal sensitive info.)	Internal actors: cashiers, finance personnel, end-users
3. Exploitation malware	Obtain valuable info., data theft	Organized crime, nation states
4. Extortion and blackmail	Ransomware	Opportunistic external actors

COMMON ATTACK PATTERNS

Attack Pattern	% of cyber incidents	By whom?
1. Web Applications	9.4%	Organized crime, end-users
2. Privilege Misuse	10.6%	Internal actors: cashiers, finance personnel, end-users
3. Cyber Espionage	18%	Organized crime, nation states
4. Crimeware/malware	18.8%	Opportunistic external actors
5. Point-of-sale	28.5%	External and internal actors in hospitality, entertainment, retail sectors

http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-5-most-common-attack-patterns-of-2014/

TYPES OF CYBER ATTACKS/THREATS

- Examples of cyber attacks/threats
  - Backdoors
  - Denial-of-Service attack
  - Direct-access attack
  - Eavesdropping
  - Spoofing
  - Tampering
  - Password attack
  - Information disclosure
  - Zero day exploitation
  - Drive-by downloads
  - Man in the middle (impersonate you to the bank, impersonate bank to you)
  - Privilege Escalation attack
  - Exploits
  - Social engineering
  - Indirect attack
  - Computer crime
  - Malware (rogue security software, adware, bots, ransomware, rootkits, spyware, scareware, Trojan horses, virus, worm, phishing, identity theft, intellectual property theft, password attacks, bluesnarfing, bluejacking, DDoS, keyloggers)

STAGES OF A CYBERATTACK

1. **Reconnaissance**: Harvest information (social media etc.), port scans
2. **Weaponization**: Scan for point of access, develop exploit, decoys, "lures"

3. **Delivery**: Gain access, insert malicious software
4. **Exploitation**: Execute malicious code on victim system
5. **Installation/proliferation**: Malware installed, spreads, escalate privileges

6. **Command and control**: Steal/modify/delete data etc.
7. **Take action on objectives** (e.g., demand ransom) or hide tracks (e.g., remove traces of the data theft)

WHEN AN ATTACK IS SUSPECTED

- Forensics and investigation
  - What questions are you trying to answer?
  - What data do you need to answer that question?
  - How do you extract and analyze that data?
  - What does that data tell you?
  - “Every contact leaves a trace…” (log files, timeline analysis)
  - Use deductive reasoning

WHEN AN ATTACK IS SUSPECTED & WHAT CAN GO WRONG IN TAKING CORRECTIVE ACTION

- What question are you trying to answer?
  - Hypothesis generation based on incorrect assumptions about system
  - Perceptual errors in reading system state (e.g., misread IP address)
- What data do you need to answer that question?
  - Make wrong assumptions about certain data
- How do you extract and analyze that data?
  - Perceptual errors in extracting data (e.g., misread data source)
  - Obtain inappropriate/incomplete/incorrect data (e.g., outdated data, compromised data)
- What does/would that data tell you?
  - Errors in interpretation of data, drawing wrong conclusions, leading to wrong action

E.g., Three Mile Island nuclear incident:

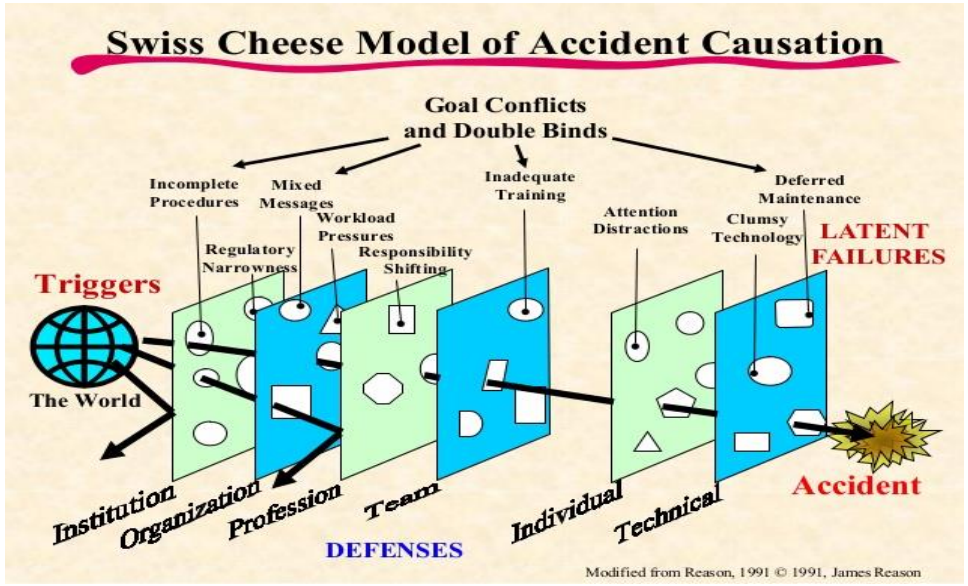
1) Valve was open, but indicator light showed "shut".
2) But indicator lightbulb did not directly reflect valve position, it was connected to a valve solenoid, i.e., driven by another mechanism) →DESIGN FLAW, INADEQUATE TRAINING
3) Operators did not have accurate info. about system state. They thought valve was shut. →MISPERCEPTION OF SYSTEM STATE
4) Other evidence that contradicted the valve shut state caused confusion instead of clarifying the system state because operators could not break out of their wrong thinking. →ERRONEOUS THOUGHT PROCESSES
5) Operators took wrong action, shutting down the cooling system, the very system that was needed in an emergency. →POOR DECISIONS

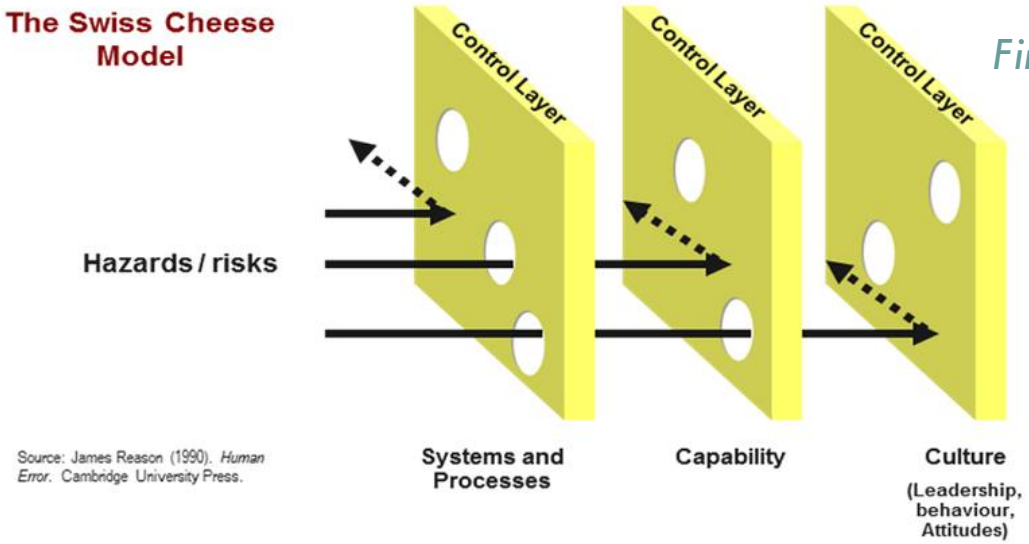
HUMAN FACTORS & CYBERSECURITY

- Most successful cyberattacks are due to an error/failure.
- The extent to which an initial attack is allowed to proliferate can also a result of error/failure.
- There are many levels at which these errors/failures can occur.
  - Individual level – erroneously opened a bad email attachment
  - Technical level – IT support forgot to update virus def's
  - Team level – poor comms between team members on file access
  - Organizational level – poor safety culture; no anti-phishing campaigns

HUMAN FACTORS & CYBERSECURITY

- Reason's (1990) Swiss Cheese model





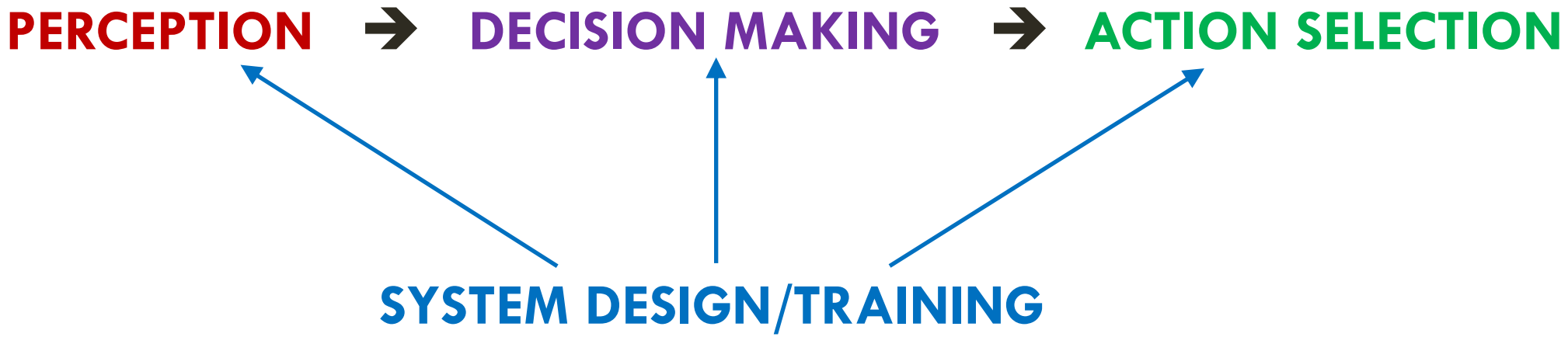
HUMAN FACTORS & CYBERSECURITY

- E.g., "Herald of Free Enterprise" disaster
  - A roll-on/roll-off ferry carrying a cargo of cars.
  - Sank in March 6, 1987, killing 200.
  - Inner and outer bow doors were left open on sailing.
  - Failures ("holes") at Management level/"cheese"
    - Mgmt pressured crew to sail early. To speed up, chief officer would be on bridge earlier, and was not on car loading deck.
    - "Negative reporting" culture, so if nothing was reported, all officers assumed everything was OK.
  - Failures ("holes ") at Supervisory & Organizational level/"cheese"
    - Assistant. boson, whose job was to close the doors, was asleep after a cleaning shift. Boson did not check that the assistant was doing his job. Lack of supervision and poor rostering/monitoring of staff.
  - Failures ("holes") at the System Design level/"cheese"
    - Shipmasters had requested for bow door warning indicators (≈ £400) to be installed on the bridge, but mgmt. did not act on requests.
    - Top-heavy design of ferry did not help the situation, and there was inadequate equipment on board to remove water from flooded deck.

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" (Proctor & Chen, 2015, pp. 722)



HUMAN FACTORS & CYBERSECURITY

PERCEPTION

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

DECISION MAKING

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

ACTION SELECTION

- Ease of implementing response required

SYSTEM DESIGN

- Features of task, website etc.

TRAINING

- Organizational factors

HUMAN FACTORS & CYBERSECURITY

PERCEPTION

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

DECISION MAKING

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

ACTION SELECTION

- Ease of implementing response required

SYSTEM DESIGN

- Features of task, website etc.

TRAINING

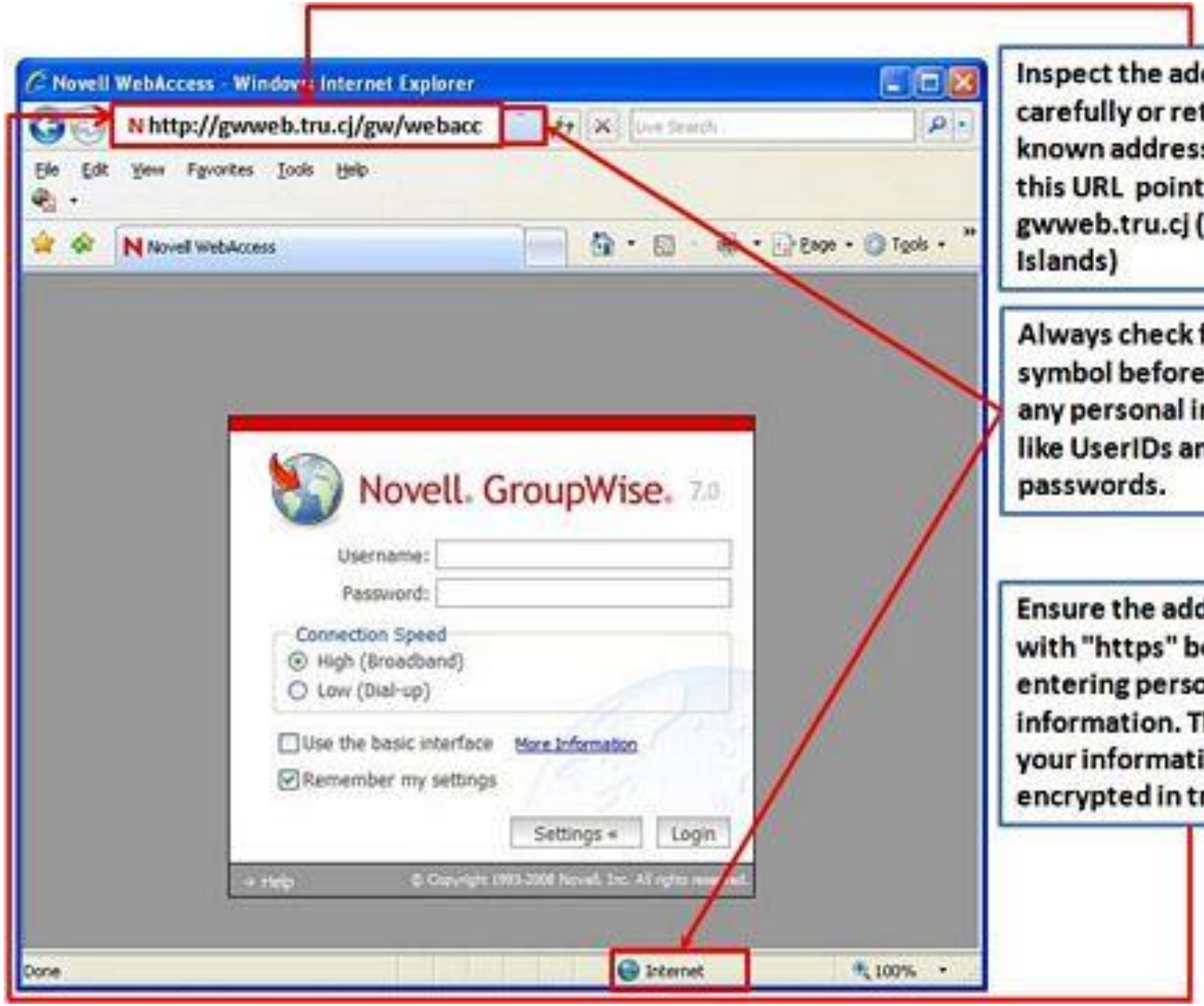
- Organizational factors

PERCEPTION

2 levels of perception:

1. Perception of information on websites/emails/system state (visual perception, legibility of displayed information)
   - Effects of time pressure, workload, fatigue, familiarity
2. Risk perception
   - Views/Attitudes on cybersecurity, security policies and procedures
   - Effects of bias and heuristics

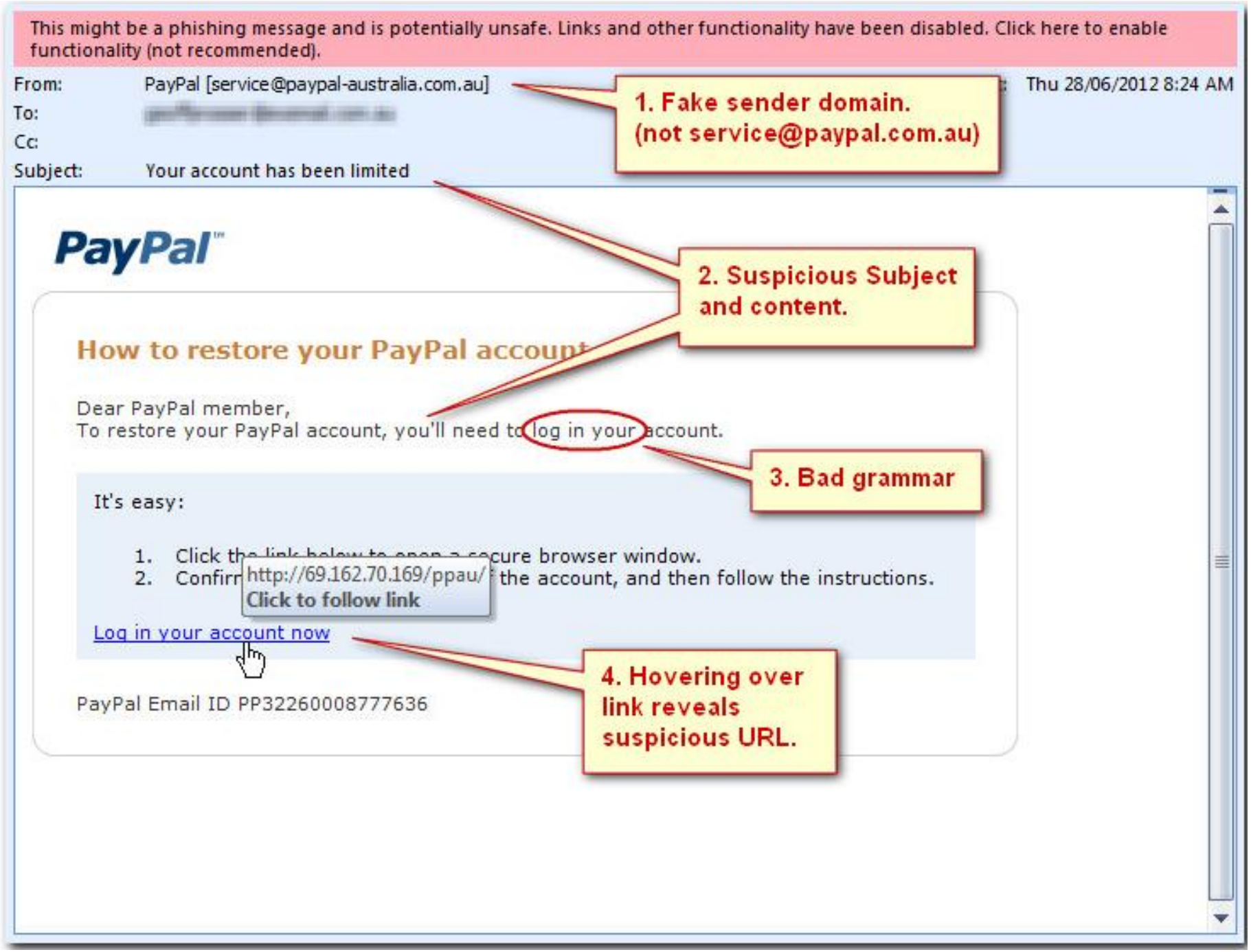

zyngafacebook.x10.mx
Google
Zynga
NEW: Wildfire launc...
facebook
Email
Password
Log In
Keep me logged in
Forgot your password?
Facebook helps you connect and share with the people in your life.
Sign Up
It's free and always will be.
First Name:
Last Name:
Your Email:
Re-enter Email:
New Password:
I am:
Select Sex:
Birthday:
Month:
Day:
Year:
Why do I need to provide my birthday?
Sign Up
Create a Page for a celebrity, band or business.
Filipino English (US) Espa◆ol Portugu◆s (Brasil) Fran◆ais (France) Deutsch Italiano ??????? ?????? ??(??) ◆
Facebook ◆ 2011 ◆ English (US)
Mobile ◆ Find Friends ◆ Badges ◆ People ◆ Pages ◆ About ◆ Advertising ◆ Create a Page ◆ Developers ◆ Careers ◆ Privacy ◆ Terms ◆ Help



Inspect the address carefully or retype the known address. Note that this URL points to gwweb.tru.cj (Cayman Islands)

Always check for the lock symbol before you enter any personal information like UserIDs and passwords.

Ensure the address begins with "https" before entering personal information. That means your information is being encrypted in transit.


This might be a phishing message and is potentially unsafe. Links and other functionality have been disabled. Click here to enable functionality (not recommended).
From: PayPal [service@paypal-australia.com.au]
To:
Cc:
Subject: Your account has been limited
Thu 28/06/2012 8:24 AM
1. Fake sender domain. (not service@paypal.com.au)
PayPal
2. Suspicious Subject and content.
How to restore your PayPal account
Dear PayPal member,
To restore your PayPal account, you'll need to log in your account.
3. Bad grammar
It's easy:
1. Click the link below to open a secure browser window.
2. Confirm your identity in the account, and then follow the instructions.
http://69.162.70.169/ppau/
Click to follow link
Log in your account now
4. Hovering over link reveals suspicious URL.
PayPal Email ID PP32260008777636

PERCEPTION IN THE USER & DEFENDER ROLES

- Perception (Attitudes) of cybersecurity by users in general
  - Security is rarely the primary task/goal.
  - Security precautions and procedures seen as an inconvenience, obstacle, interruption to achieving a goal. (e.g., scanning/quarantining emails and attachments)
- Perception of system state by defenders
  - Expert (i.e., system admin.) vs. Novice (i.e., users) perception (Ross et al., 2005)
    - Experts are better at pattern recognition
    - Experts tend to spend more time understanding/analyzing situation, rather than focus on fixes
    - Experts are better at monitoring their own performance
    - Experts are better at detecting problems as situation progresses

RISK PERCEPTION

- Risk perception affected by:
  - High workload and stress - need to make important decisions under pressure (Intuitive process vs. Rational process: Klein's model of adaptive Decision-Making)
  - Decisions made under conditions of uncertainty, incomplete information
  - Automated aspects of the security system (e.g., spam filters, antivirus scans)
  - Attitudes and beliefs about system security
  - Level of trust in security systems and policies
  - Similar issues affecting trust and reliance in automation
    - Workload, fatigue, attitudes and past experience with automation/system etc.
    - Misuse: Overreliance on automation (monitoring or decision bias)
    - Disuse: Underutilization, neglect, failure to activate automation
    - Abuse: Designing system without regard for consequences on performance

RISK PERCEPTION

- We are constantly bombarded by information and stimuli. To help filter out and reduce the amount information to a manageable level, we use shortcuts (heuristics), which can result in biases.
- Cognitive bias = tendency to think in a certain way that *can* lead to errors.
- Heuristics = shortcuts, rule-of-thumb used in thinking. Most of the time helpful, but in other times, can lead to errors.

RISK PERCEPTION

- Cognitive bias.
  - *Availability heuristic*
    - People tend to judge frequency or likelihood of event happening based on how easily an example can be brought to mind (Slovic, Fischhoff & Lichtenstein, 1979; Tversky & Kahneman, 1979)
    - But memory is very selective
      - Highly publicized/sensationalized events more memorable their likelihood of occurring may be overestimated)
      - Can't recall all events or types equally well.
      - Recall affected by Imaginability – If no memory of specific event, people will imagine possible instances and then evaluate probability of event based on their imagination. But some things easier to ima gine than others.
    - Security breaches are relatively rare. More likely to recall breaches that didn't result in accidents, so estimate of a risk of breach likely to be underestimated (Slovic et al., 1976).

RISK PERCEPTION

- Cognitive bias.
  - *Optimism bias*
    - People tend to believe that negative outcomes are more likely to occur to others (Gray & Ropeik, 2002)
      - Study showed that people rated likelihood of risks occurring to themselves/their family differently from how they rated the risks occurring to the general public (Sjoberg, 2000)
      - Most users don't think that hackers would value the information they have and don't tend to see themselves as potential targets (McIlwraith, 2006)
      - Most users believe that if they do not see any warning signs of an attack, then they are exempt from future risks (Weinstein, 1987).
    - This underestimation of risk may result in risky behavior (e.g., failure to keep up to date with security patches, follow security procedures). They underestimate likelihood that their inactions/actions can result in a security breach.
    - Organizations and individuals tend to think that cyberattacks happen to others, not to them.

RISK PERCEPTION

- Cognitive bias.
  - *Level of control*
    - People tend to think that they have more control over risks than they actually do (Kreuter & Strecher, 1995). E.g., people view actions on their personal computer to be under their control, so threats seem less likely.
    - More likely to underestimate the chance that their non-compliance to security policies on their computers will result in adverse consequences.
    - Related to the *Expert's Bias* – those more competent in information security can be overconfident and overestimate their ability to control the threat and so may engage in more risky behavior.

RISK PERCEPTION

- Cognitive bias.
  - *Level of Knowledge*
    - People who are not as knowledgeable about information security may not understand the risks involved because they lack knowledge of the potential implications of potential security breaches
    - Difficult to perceive risk accurately and make effective decisions without the adequate knowledge of the underlying technology (Fischhoff, 2002; Lacohee, Phippen & Furnell, 2006). E.g., Users may not know what constitutes a secure password if they do not know how passwords can be cracked (Adam & Sasse, 1999).

RISK PERCEPTION

- Cognitive bias.
  - *Risk homeostasis or risk compensation*
    - People will accept a level of risk, and when the situation changes, their behavior will change to maintain the same level of risk (Wilde, 2001). People who are aware of security procedures may actually engage in riskier security behaviors.
      - E.g., if system is in a highly controlled access-area, people may perceive the risk of a breach to be lower and will be less diligent about protecting the computer (Mitnick & Simon, 2005).

RISK PERCEPTION

- Cognitive bias.
  - *Cumulative Risk*
    - The risks involved in information security are cumulative (Fischhoff, 2002).
      - E.g., chance of an insecure password being exploited on a particular day is low, but over a months, this risk is a lot greater.
      - Risks from one individual user not following security procedures may be low, but if a number of people do not comply and create different vulnerabilities, then the cumulative risk is substantial.
      - People do not understand this idea of cumulative risk well, and so do not think much about the small risks they tend to take (Slovic, 2000).

RISK PERCEPTION

- Cognitive bias.
  - *Omission Bias*
    - People tend to consider an omission (failure to act) as more acceptable and less serious than a commission (Ritov & Baron, 2002).
      - Security non-compliance from omissions (e.g., failure to change passwords regularly) seen as less risky than non-compliance from acts of commission (e.g., writing the password down).
      - Users whose inactions result in security breaches may be seen as less morally culpable than users whose actions led to security breaches. (e.g., Post-completion error, which is the failure to complete the final 'clean up' task, leaving the system open to a possible security breach).

RISK PERCEPTION

- Cognitive bias.
  - *Effects of Familiarity*
    - The more familiar a risk is, the more people feel comfortable with living with it, and the more complacent they are because they underestimate it. Novel and unfamiliar risks are less likely to be underestimated.
      - E.g., Locking up an unattended computer is a familiar task. Risk associated with not locking up computer may be underestimated.
    - However, increased familiarity with risk may also increase compliance especially if the user has knowledge and understands the reason for the policies.
      - E.g., People more likely to follow precautions when using products which they are more familiar with and understand better (Ortiz, Resnick & Kengskool, 2000).

RISK PERCEPTION

- Cognitive bias.
  - *Effects of Framing*
    - Prospect theory (Kahneman & Tversky, 1979; Schneier, 2003) – risk perception is influenced by how the risk is framed. Risk-taking higher when framed as losses. Risk-aversion higher when framed as gains.
      - When framed as a 32% chance of dying, more people opted for the risky procedure. When framed as 64% chance of surviving, fewer people opted for the risky procedure (McNeil, Pauker, Sox & Tversky, 1982)
      - People may be more likely to comply with security policies (i.e., be more risk averse) if outcomes are framed in terms of gains.
      - People may to take more risks if the risk is expressed in terms of a loss (e.g., if you don't click on this link, your data worth $10000 will be wiped out) compared to if risk was expressed in terms of a gain (e.g., if you don't click on this link, you will not gain the prize money worth $10000).

RISK PERCEPTION

- Cognitive bias
  - *Representativeness bias*
    - Insensitivity to prior probability – People will guess that a quiet type is a librarian not salesman, even though there are far fewer librarians than salesmen (base-rate ignored).
    - Illusion of validity – overly confident about their guesses (e.g., confident about the librarian guess even though not much basis for that)
    - Can lead to false parallels drawn between unrelated situations/attacks.

RISK PERCEPTION

- Cognitive bias
  - *Confirmatory bias* (Plous, 1993; Lewicke, 1998)
    - People tend to look for or interpret information in a way that confirms their perception/hypotheses.
    - Ambiguous data/situations tend to be interpreted in ways that confirm hypotheses.
    - Security analysts may only look for signs that confirm their hypotheses and not be as open to contradictory information. This can result in inaccurate understanding of system state.
  - *Status quo bias* (Samuelson & Zackhauser, 1988)
    - Tendency to prefer things to stay the same
  - *Sunk cost effect*
    - Tendency to continue investing time and effort into something, or sticking with a particular strategy just because much has already been put into it.

RISK PERCEPTION

- Cognitive bias
  - *Adjustment and Anchoring*
    - When estimating quantity, we usually start with initial guess then adjust this to get the final estimate. Different starting points result in different estimates. (Kahneman et al.'s Anchoring)
    - Tendency to give more weight to some pieces of information, especially the first pieces of information obtained.
  - *Expert's bias*
    - Experts' estimates can be affected by overconfidence. At times, over credit outcomes from small samples.

RISK PERCEPTION

- Personality and Cognitive style.
  - Risk takers/sensation seekers vs. Risk avoiders/rule-conscious
- Social factors
  - Group norms about security behavior – if group considers information security to be important, then individuals in the group are likely to feel the same and follow security procedures.
  - Group behavior and trust – e.g., sharing passwords can be seen as sign of trust among co-workers and friends (McIlwraith, 2006)
  - Bystander effect – The more people there are responsible for something, the less responsible each individual feels – e.g., individual users in large organizations with large security teams may feel less personal responsibility for maintaining security.

DIMENSIONS OF RISK

- Voluntariness: how willing are people to take the risk?
- Controllability: how controllable is the risk?
- Immediateness: how immediate/delayed are the consequences?
- How far-reaching are the consequences? :Global or local consequences? Will consequence persist to future generations?
- Etc.

"Most of the time, when assessing risk, we deal not in calculations of probabilities, but [in] gut feelings" - Slovic

ONE POSSIBLE WAY TO ASSESS CYBER RISK

1. Identify information assets
2. Locate information assets
3. Classify information assets
   - Public info
   - Internal, not secret
   - Sensitive internal info
   - Compartmentalized internal info
   - Regulated info

ONE POSSIBLE WAY TO ASSESS CYBER RISK

4. Conduct threat modeling exercise on the diff types of threats:

   Microsoft's STRIDE for categorization of threats

   - *S*poofing of identity
   - *T*ampering with data
   - *R*epudiation of transactions – transaction not recognized or denied.
   - *I*nfo disclosure
   - *D*enial of service
   - *E*levation of privileges.

5. Finalize data and start planning when scores showing threat per category are obtained

IDC6601: BEHAVIORAL IMPERATIVES

BRUCE D. CAULKINS, PH.D.