# MIS761
# Cyber Security Strategies

**Dept. of Information Systems & Business Analytics**

**Deakin Business School**

## Week 3: Cyber Hygiene: Security Awareness, Training, and Education

AACSB ACCREDITED

DEAKIN BUSINESS SCHOOL

# What is SETA?

- SETA: Ongoing efforts that promote employees' consciousness of security issues and provide them with general security knowledge and skills to combat security threats and risks.
- Security education: Efforts that aim at improving employees' consciousness of security policies, guidelines, and security surroundings to enhance employees' security-related behavior.
  - *Example: Online courses on cybersecurity fundamentals.*
- Security training: Instructional tools and communication tunnels to activate employees' thinking processes, persuade them to act appropriately, and enable them to gain a better understanding of security policies and procedures
  - *Example: Hands-on workshops on recognizing phishing emails.*
- Security awareness: Programs that aim to foster employees' security learning and make employees conscious of the importance of information security protection, and continuous efforts to produce security behavioral changes
  - *Example: Monthly newsletters with security tips and reminders.*

# What's the differences?

| Types of program | Purpose | Delivery method | Target audience | Level of SETA |
|---|---|---|---|---|
| Education program | Enable employees with deep learning on security knowledge and skills, giving employees insights into why security protection is required. | Usually active and engaging mentoring, like cyber attack simulations | Usually IT/security specialists and professionals. | Highest |
| Training program | Builds employees' security knowledge and skills, enabling employees to understand how security protection can be achieved | Usually hands-on approaches, such as formal classes and seminars. | Usually all employees. | Intermediate |
| Awareness program | Draws employees' attention to security and explains to employees what security is. | Poster, banners, reminders, etc. | All employees. | Basic |

# Design Factors of SETA

- **Adapt to Organizational and Employee Needs**
  - Tailor topics to target audience
  - Use real-life examples and employee input
  - Segment employees into small learning groups
- **Effective Delivery Methods**
  - Game-based and hands-on approaches
  - Avoid excessive information or multimedia
  - Use collaborative learning techniques
- **Senior Management Support**
  - Essential for success
  - Champions drive program implementation
- **Communication and Frequency**
  - Frequent, small sessions are more effective
  - Strong, persuasive messages enhance understanding
- **Cultural and Individual Differences**
  - Consider cultural factors and employee personality traits

# Effects on Employees’ security-related behavior

- **Direct Effects of SETA Programs**
  - Increased compliance with security policies
  - Improved overall security performance
  - Reduced instances of misuse or abuse of computer systems
- **Indirect Effects of SETA Programs**
  - Enhanced awareness of security threats
  - Increased sense of responsibility and accountability
  - Greater motivation to follow security practices

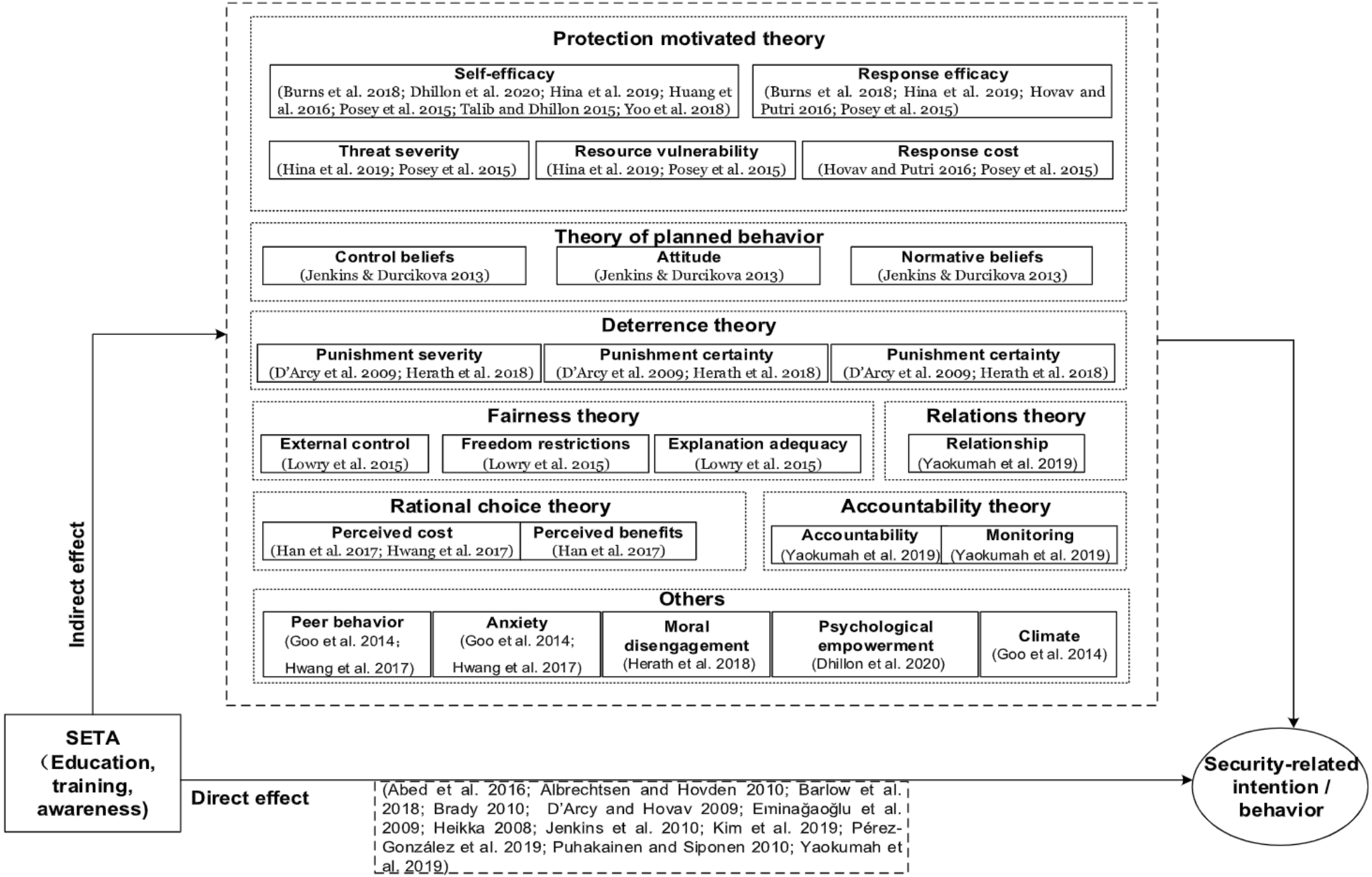
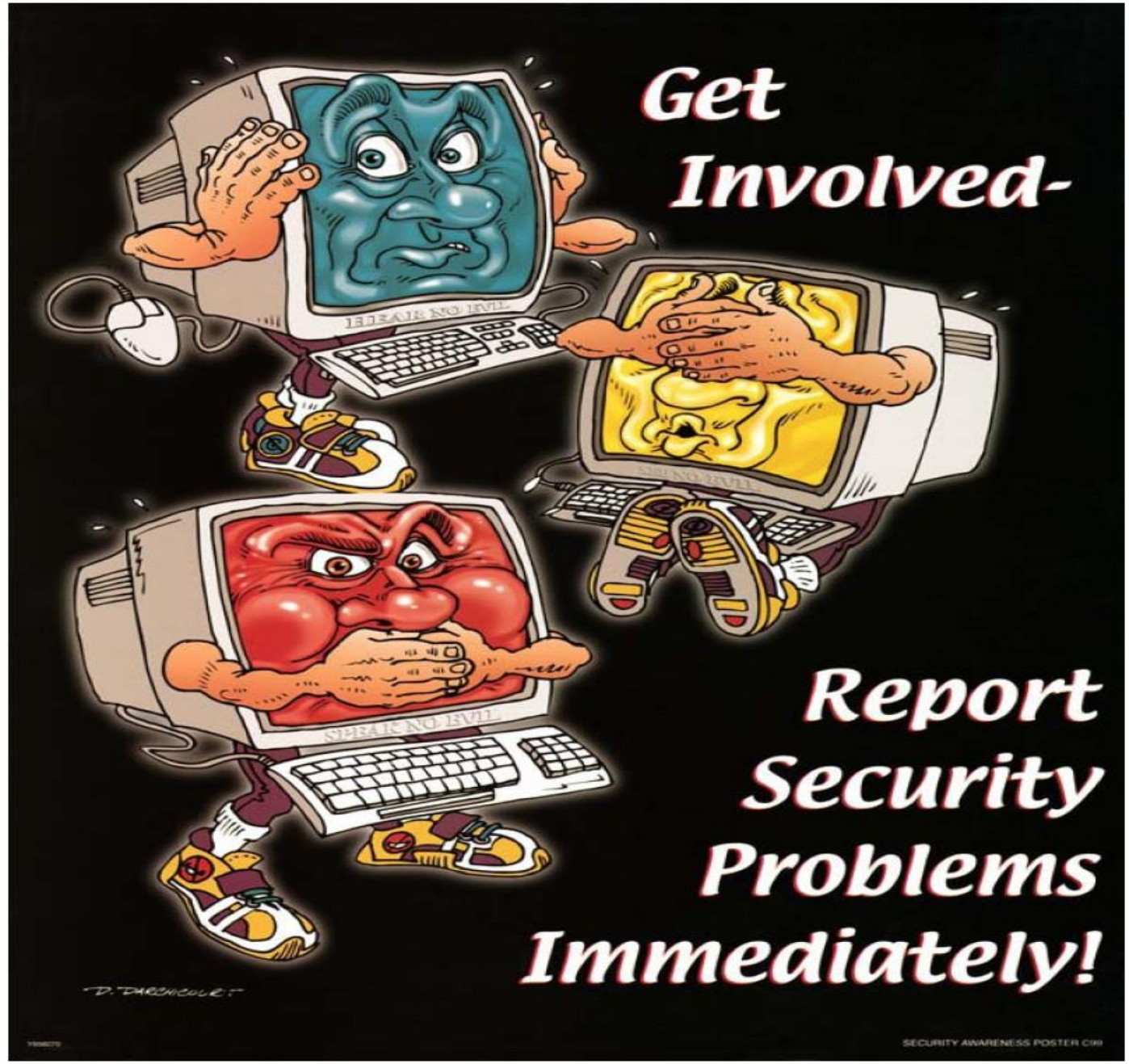



**Figure 2.** SETA and employees' secure behavior.


Get
Involved-
Report
Security
Problems
Immediately!
SECURITY AWARENESS POSTER ©99


Phishing Simulation Email
Report
Congratulations!

# Challenges in Phishing Simulation Campaign

- **Low Participation Rate**
- **Reluctance to Take Training After Failing Simulation**
  - Non-mandatory training.
  - Training hosted on a different system.
  - Training service provider’s language style differs.
  - Challenge in promoting the campaign across branches.
  - Casual staff reluctance and lack of leader support.

Journal of the Association for Information Systems (2024) **25**(4), 1079-1116
**doi:** 10.17705/1jais.00875

RESEARCH ARTICLE

ISSN 1536-9323

# An Empirical Investigation of The Unintended Consequences of Vulnerability Assessments Leading to Betrayal

Daniel Pienta,[1] Jason Bennett Thatcher,[2] Ryan T. Wright,[3] Philip L. Roth[4]

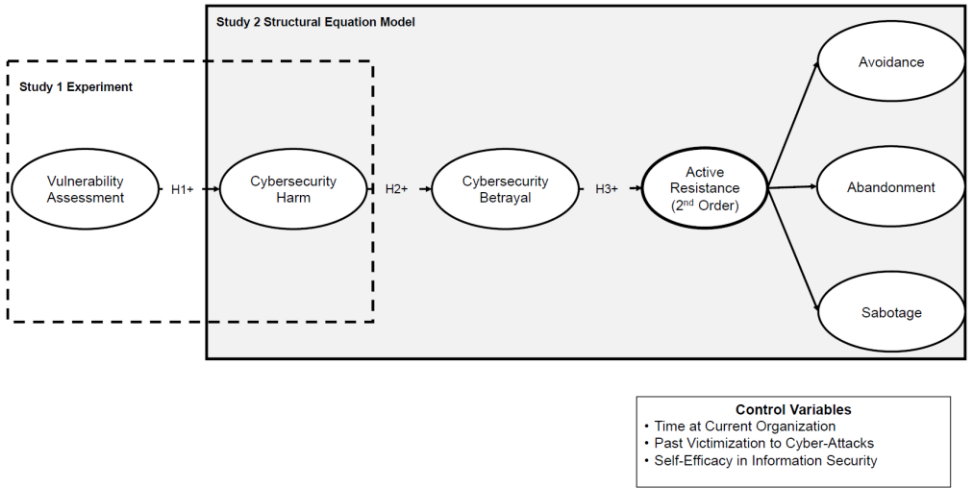



Figure 3. Research Model of Vulnerability Assessments, Harm, and Betrayal

# Trust Matters! Don't Hurt the Employees!

- **Negative Perceptions:**
- Employees view vulnerability assessments, like phishing simulations, as harmful
- Feelings of harm lead to a sense of betrayal and active resistance
- **Balancing Benefits and Costs:**
- Organizations need to weigh the benefits against potential negative impacts
- **Role of SETA:**
- Building trust and transparency can mitigate negative perceptions
- Explain the purpose and benefits of vulnerability assessments
- Provide support and training to reduce feelings of harm and build trust

# Building Trust in Cybersecurity

- **Human-Centric Approach:**
  - Security is a human problem needing human-centric solutions
  - Culture is key to effective cybersecurity
- **Establish the Right Mindset:**
  - Focus on positive actions employees can take
  - Encourage curiosity and vigilance with positive reinforcement
- **Engage with Empathy:**
  - Avoid a blame culture to encourage prompt reporting
  - Focus on collective learning from incidents
- **Effective Communication:**
  - Utilize various communication channels strategically
  - Ensure messages reach employees effectively and consistently
- **Teamwork and Collaboration:**
  - Involve different functions within the business
  - Align goals and show the importance of each team's role in cybersecurity

# Willingness Matters! Don’t Force the Employees!


- **Definition of Cybersecurity Legitimacy:**
  - Employees’ perception of fairness, appropriateness, and suitability of cybersecurity policies
- **Impact on Compliance:**
  - Positive perception of legitimacy leads to higher compliance
  - Negative perception can nullify compliance, even with threat awareness
- **Role of SETA:**
  - SETA programs help build legitimacy by explaining the fairness and necessity of security measures
  - Emphasizing the reasonableness and benefits of security policies enhances acceptance

because it's inconvenient not to

because management says so?

# Practical Insights on Cybersecurity Legitimacy

- **Ongoing Training and Executive Buy-In:**
  - Treat cybersecurity training as ongoing change management.
  - Secure executive support and align with organizational goals.
- **Creating a Program Vision:**
  - Communicate clear objectives and the importance of the program.
  - Regularly update employees through multiple communication channels.
- **Best Practices for Training:**
  - Teach relevant, updated topics tailored to different employee groups.
  - Contextualize training content for various roles.
  - Plan for long-term engagement and regular updates.

Contents lists available at ScienceDirect

Information & Management

journal homepage: www.elsevier.com/locate/im

How "What you think you know about cybersecurity" can help users make more secure decisions

Amir Fard Bahreini [a,*], Hasan Cavusoglu [b], Ronald T. Cenfetelli [b]

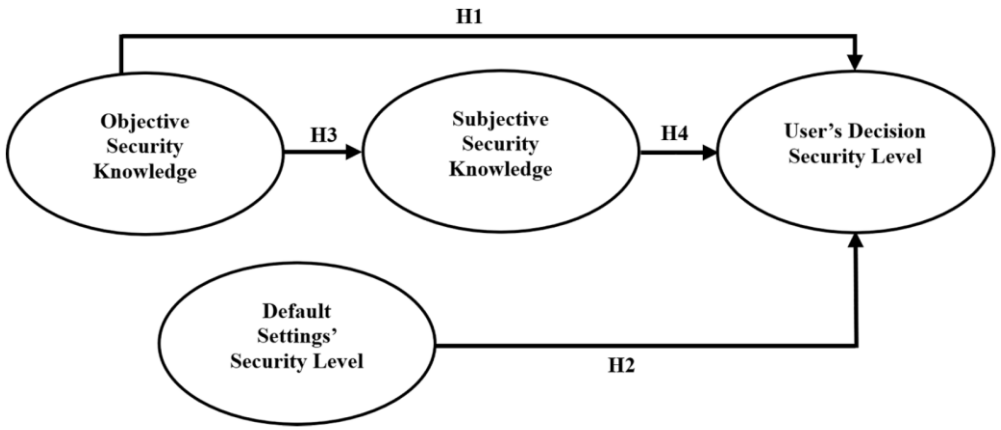



Fig. 1. Theoretical Model.

# Confidence Matters! Empower the Employees!

- **Understanding Security Knowledge:**
  - **Objective Security Knowledge:** Actual knowledge about security
  - (e.g., creating strong passwords, recognizing phishing emails)
  - **Subjective Security Knowledge:** Confidence in one's security knowledge
- **Decision Security Levels:**
  - High actual knowledge paired with high confidence leads to better security decisions
  - Confidence helps prevent reliance on insecure default settings
- **Default Settings:**
  - Default settings are often accepted without changes
  - Confident users are more likely to adjust these settings for better security

# Enhancing User Confidence and Experience

- **Human-Centric Security Approach:**
  - Design security measures that prioritize user experience and reduce friction.
  - *Example: Implementing easy-to-use phishing reporting buttons in email clients.*
- **Secure by Design:**
  - Incorporate security features seamlessly into digital and physical environments.
  - *Example: Default settings should be secure to guide user behavior without additional effort.*
- **Enhancing User Confidence:**
  - Provide clear, consistent, and engaging security training tailored to job roles.
  - *Example: Use colorful pop-ups to remind users about security practices.*

Journal of the Association for Information Systems (2024) **25**(4), 1037-1078
**doi:** 10.17705/1jais.00854

RESEARCH ARTICLE

ISSN 1536-9323

## Roles of Feedback and Phishing Characteristics in Antiphishing Training Performance: Perspectives of Goal Setting and Skill Acquisition

Shihe Pan,[1] Dong-Heon Kwak,[2] Jungwon Kuem,[3] Sung S. Kim[4]

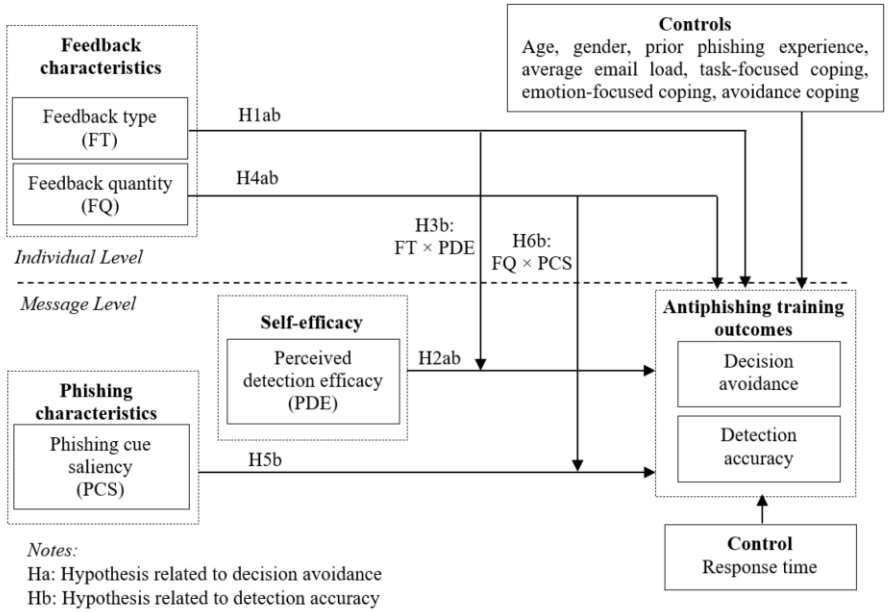



Figure 1. Research Model

# Feedback Matters! Strengthen Employees' Confidence!

- **Types of Feedback:**
- Example-based feedback is more effective than abstract feedback
- Helps employees better identify phishing emails by enhancing procedural knowledge
- **Perceived Detection Efficacy:**
- Confidence in detecting phishing emails improves training outcomes
- Boosting this confidence leads to higher detection accuracy and reduced decision avoidance
- **Quantity of Feedback:**
- More feedback isn't always better; too much can overwhelm trainees
- Start with basic tips before moving to more complex scenarios

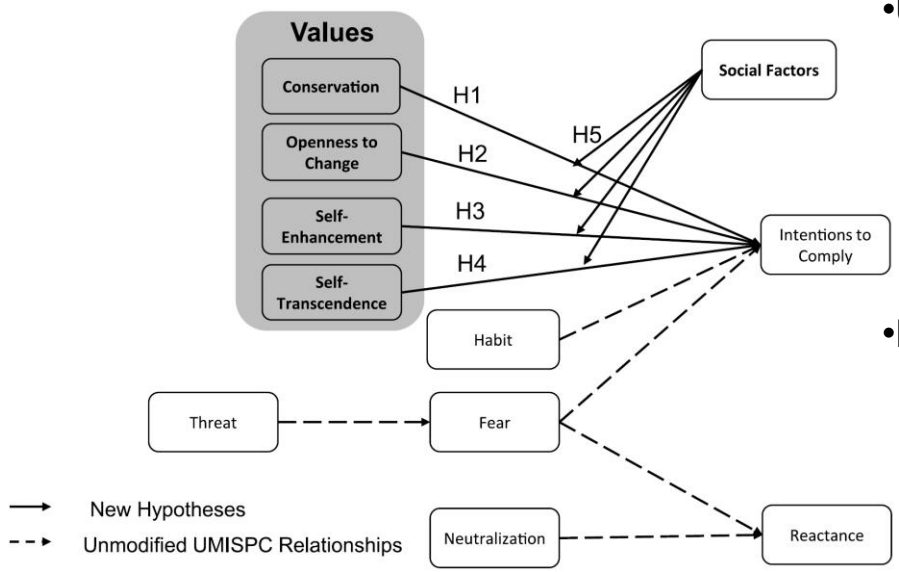
informs
https://pubsonline.informs.org/journal/isre

INFORMATION SYSTEMS RESEARCH
*Articles in Advance*, pp. 1–13
ISSN 1047-7047 (print), ISSN 1526-5536 (online)

**Promoting Security Behaviors in Remote Work Environments: Personal Values Shaping Information Security Policy Compliance**

Carlos I. Torres,[a,*] Robert E. Crossler[b]

**Figure 1.** Proposed Modified UMISPC Research Model




# Customization Matters! Treasure Employees' Personal Values!

- **Understanding Personal Values:**
  - **Conservation:** Valuing tradition and security, may resist change
  - **Openness to Change:** Valuing creativity and innovation, embraces new opportunities
  - **Self-Enhancement:** Valuing personal success and power, seeks personal benefits
- **Implications for SETA Programs:**
  - Tailor training to match these values
  - Highlight organizational stability for those valuing conservation
  - Present security practices as innovative for those valuing openness to change
  - Emphasize personal gains for those focused on self-enhancement

# Tailored Security Training (Adapt to Evolving Threats)

- **Customized Training:**
  - Tailor training based on job function, employee tenure, and work environment.
  - Provide relevant examples specific to each role.
- **Department and Job Function:**
  - Customize training for different departments (e.g., finance, sales).
  - Use real-world examples targeting specific job roles.
- **Employee Tenure:**
  - Focus on vulnerabilities of new employees.
  - Integrate security training into onboarding.
- **Remote or In-Office Work:**
  - Address specific risks for remote, in-office, and hybrid work environments.
- **Human Error:**
  - Implement real-time tools to flag potential mistakes.
  - Provide in-the-moment training to correct behaviors.

# Extending Awareness to Culture (Beyond Training)

- **From Awareness to Culture:**
  - Awareness training is just the first step.
  - Security culture encompasses values, beliefs, and behaviors.
- **Importance of Culture:**
  - Culture fosters shared responsibility and community.
  - Encourages proactive security behaviors.

# Creating a Strong Security Culture (Engagement and Accountability)

- **Employee Engagement:**
  - Gamified training programs.
  - Encourage employees to take pride in security.
- **Shared Responsibility:**
  - Real-time threat reporting and validation.
  - Validates employee contributions to security.

# Building Resilient Security Culture (Evolution and Inclusion)

- **Evolving with Threats:**
  - Continual improvement of the human layer.
  - Learn from failures and fortify against future threats.
- **Inclusion in Security:**
  - Every team owns their security.
  - CISOs as partners, not enforcers.
- **Soft Skills:**
  - Importance of communication and relationship-building.
  - Driving engagement and understanding across the organization.

# Case Study - Yahoo

- **Proactive Engagement:**
  - Combined red team and security awareness efforts.
  - Behavioral engineering to measure and influence security behaviors.
- **Action, Habit, Behavior:**
  - Action: Completing a task, like security training.
  - Habit: Using a password manager.
  - Behavior: Consistently using the password manager when creating or updating accounts.
- **Behavioral Goals:**
  - Define clear goals for specific security actions.
  - Example: Use corporate password manager for new passwords.

# Case Study - Yahoo

Implementing Change and Measuring Success

- **Steps to Change Behavior:**
  - Identify behavioral goals.
  - Measure baseline and adjust actions.
  - Repeat process for continuous improvement.
- **Key Measures:**
  - Susceptibility Rate: Employees falling for phishing.
  - Credential Capture Rate: Credentials entered on fake sites.
  - Reporting Rate: Phishing emails reported accurately.

# Case Study - Yahoo

Creating a Culture of Security (Incentives and Communication)

- **Incentives and Tools:**
  - Encourage use of password manager.
  - Offer rewards like branded merchandise.
- **Communication:**
  - Educate with how-to videos and content.
  - Use dashboards for performance benchmarking.
- **Real-Time Reporting:**
  - Employees report suspicious emails.
  - Immediate feedback provided to employees.