

Thursday, 22 February 2018

Psybersecurity: Human Behaviour and Network Security

Paul Corballis
School of Psychology



SCIENCE



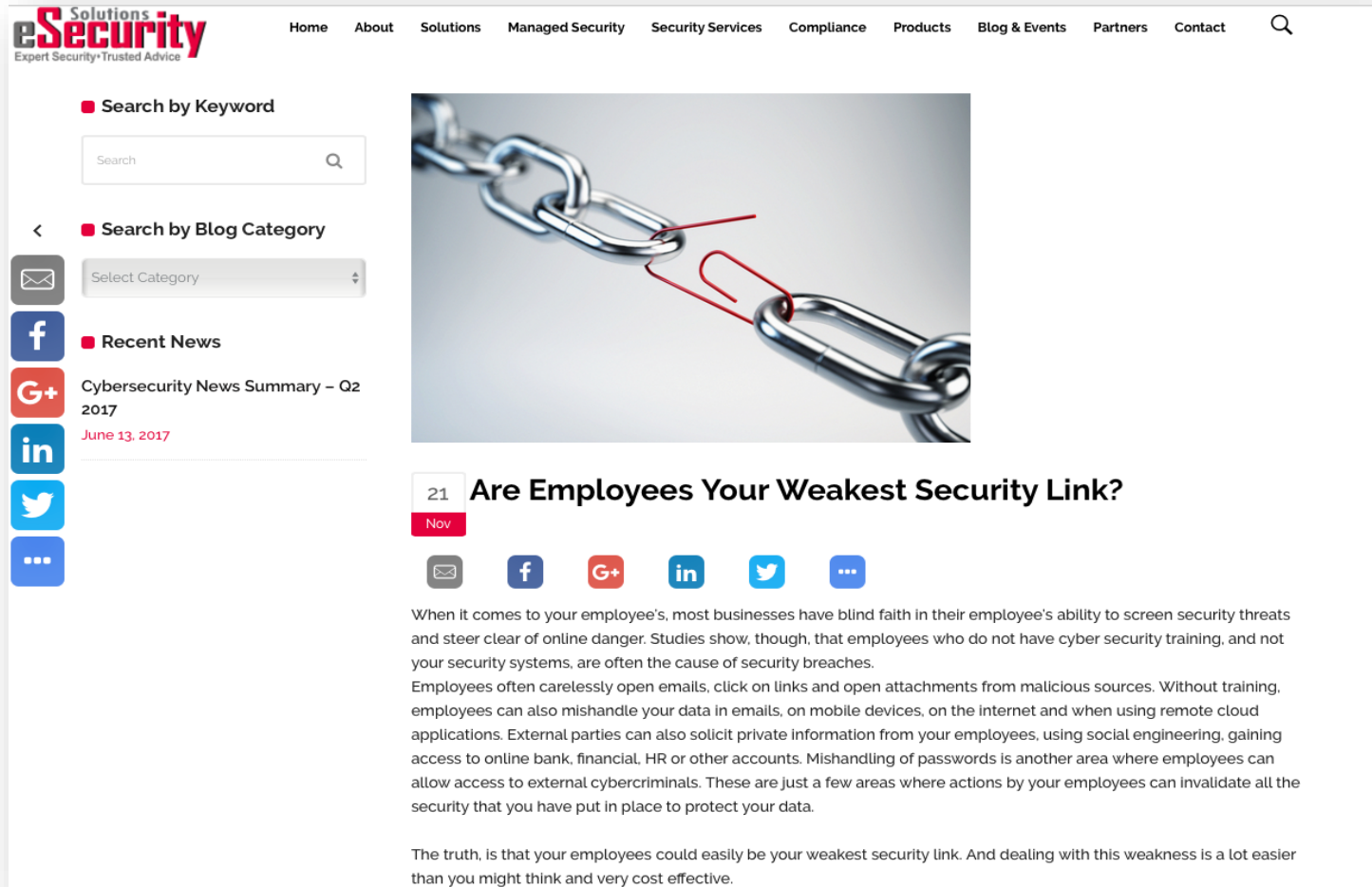
The human element

Uncertainty and decision making

Learning and training

Improving cybersecurity behaviours

The Human Element



Solutions eSecurity
Expert Security • Trusted Advice

Home About Solutions Managed Security Security Services Compliance Products Blog & Events Partners Contact

■ Search by Keyword

Search







< ■ Search by Blog Category

Select Category

■ Recent News

Cybersecurity News Summary – Q2 2017
June 13, 2017

21 **Are Employees Your Weakest Security Link?**
Nov

When it comes to your employee's, most businesses have blind faith in their employee's ability to screen security threats and steer clear of online danger. Studies show, though, that employees who do not have cyber security training, and not your security systems, are often the cause of security breaches.

Employees often carelessly open emails, click on links and open attachments from malicious sources. Without training, employees can also mishandle your data in emails, on mobile devices, on the internet and when using remote cloud applications. External parties can also solicit private information from your employees, using social engineering, gaining access to online bank, financial, HR or other accounts. Mishandling of passwords is another area where employees can allow access to external cybercriminals. These are just a few areas where actions by your employees can invalidate all the security that you have put in place to protect your data.

The truth, is that your employees could easily be your weakest security link. And dealing with this weakness is a lot easier than you might think and very cost effective.



Go Phish: Protecting Your Enterprise From The Weakest Link

By Dan Panesar, VP EMEA, Certes Networks March 21, 2017

👁 1404 💬 0

According to a recent report by PhishMe, 91% of cyber attacks begin with a phishing email. The attack method remains one of the most successful available to hackers as it exploits the inherent weakness of individual users. Since the advent of networked computers, human error has almost always been at the heart of failings in cyber security, and despite increasing attempts to improve user awareness and security training, individuals continue to fall foul. With the average security breach still taking close to 150 days to detect, businesses can no longer afford to leave their security in the hands of an outdated cyber security trust model which means all cyber defences are moot if a phishing email is clicked. If approaches to cybersecurity don't change soon, phishing season will be never ending.

Top ten phishing results show human error is still the weakest link

By Perry Carpenter July 20, 2017 Features

Emails from unknown senders should be treated with great care no matter how official the subject line may seem.



Phishing and ransomware attacks are a serious problem to businesses the world over and have become the logical evolution of cybercrime. Criminals can steal or disable access to corporate or personal finances, sensitive employee data, patient data, intellectual property, employee files and other valuable content.



Fixing The Weakest Link

We are often asked by organizations how they can better train their employees to prevent them from clicking on malicious links or being susceptible to attempts by hackers to make their way into their networks. The rise in the frequency of this question means that organizations are finally starting to realize where the weak links are. Below are some general thoughts on how you might fix the weakest link in the security of your organization.

The State of Security

NEWS. TRENDS. INSIGHTS.

FEATURED ARTICLES LATEST SECURITY NEWS RESOURCES

The Human 'Attack Surface' May Be Your Weakest Link



KATHERINE BROCKLEHURST

Follow @Kat_Brock

NOV 30, 2017 | ICS SECURITY



The term "attack surface" is security jargon for the sum of your security risk exposure. It is the aggregate of all known, unknown, reachable and potentially exploitable weaknesses and vulnerabilities across the organization. All organizations regardless of industry have an **attack surface**.

Fortunately, awareness of weaknesses, prioritization of risk, and layered defenses can reduce the attack surface and limit disruption, enhance predictable operations, and lower business risk.

WHAT IS THE HUMAN ATTACK SURFACE IN ICS ENVIRONMENTS?

ugui ty
it Security-Trusted Advice

Search by Keyword


Search

Search by Blog Category

Select Category

Recent News

Cybersecurity News Summary – Q2 2017
June 13, 2017



Are Employees Your Weakest Security Link?


21

Now

f G+ in t

Most businesses have blind faith in their employee's ability to protect their data. However, most employees do not have the necessary skills to do so, though, that employees who do not have cyber security training are a significant weakness. Employees are often the weakest link in a company's security chain, and they can be exploited by malicious attackers.

Intelligent Data Solutions
A Division of Bogart Associates



Fixing The Weakest Link

We are often asked by organizations how they can better train their employees to prevent them from becoming the weakest link in their security chain. The question means that the weakest link is the most vulnerable link in the security of your organization.

Top ten phishing results show human error is still the weakest link

By Perry Carpenter July 20, 2017 Features

Emails from unknown senders should be treated with great care no matter how official the subject line may seem.

f t p m



Phishing: Protecting Your Enterprise from the Weakest Link

Jan Panesar, VP EMEA, Certes Networks March 21, 2017

According to a recent report by PhishMe, 91% of cyber attacks begin with a phishing email. The most successful available to hackers as it exploits the inherent weakness of individual users. So, computers, human error has almost always been at the heart of failings in cyber security, and despite the fact that security training, individuals continue to fall foul. With the average security awareness training taking 150 days to detect, businesses can no longer afford to leave their security in the hands of an outside model which means all cyber defences are moot if a phishing email is clicked. If approaches to cyber security are not improved, phishing season will be never ending.

The State of Security

NEWS, TRENDS, INSIGHTS


FEATURED ARTICLES LATEST SECURITY NEWS RESOURCES

The Human 'Attack Surface' May Be Your Weakest Link

KATHERINE BROCKLEHURST
NOV 30, 2017 ICS SECURITY



Phishing and ransomware attacks are a serious problem to businesses the world over and have become the logical evolution of cybercrime. Criminals can steal confidential data, access to corporate or personal finances, sensitive employee data, and other critical information.



f t in G+ +

The term "attack surface" is security jargon for the sum of your security risk exposure. It is the aggregate of all known, unknown, reachable and potentially exploitable weaknesses and vulnerabilities across the organization. All organizations regardless of industry have an **attack surface**. Fortunately, awareness of weaknesses, prioritization of risk, and layered defenses can reduce the attack surface and limit disruption, enhance predictable operations, and lower business risk.

WHAT IS THE HUMAN ATTACK SURFACE IN ICS ENVIRONMENTS?

Humans, we're told, are the weak link of security. That was a key theme in the [Verizon Data Breach Investigations Report](#) released last week. After all, ransomware and phishing are effective because they're able to so skillfully target human vulnerabilities.

Here's the problem. Human vulnerabilities will always exist. This old way of thinking—that people are the problem, and we can somehow change entrenched human behavior—isn't getting us anywhere. Even with improved training and education, given the sophistication of the attacks, human vulnerabilities will persist. So we need to rethink this paradigm: What if we started viewing human-computer interaction as a means to increase security? How could we use what humans do best—critical thinking and contextualization—and combine it with what computers do best—automation and scale—to make us all safer?

We can start with a more "human-centric" approach to security—in other words, designing products and solutions with human strengths and vulnerabilities in mind. Here are three examples of ways that this approach could make us all more secure:

Phishing Attacks

Contents of phishing emails:

- appeal to ego/flattery
- familiarity
- credulity
- deception
- social manipulation
- appeal to authority ("Fake CEO" scam)

Bypass or short-circuit cognitive control mechanisms



Dimensions of Personality

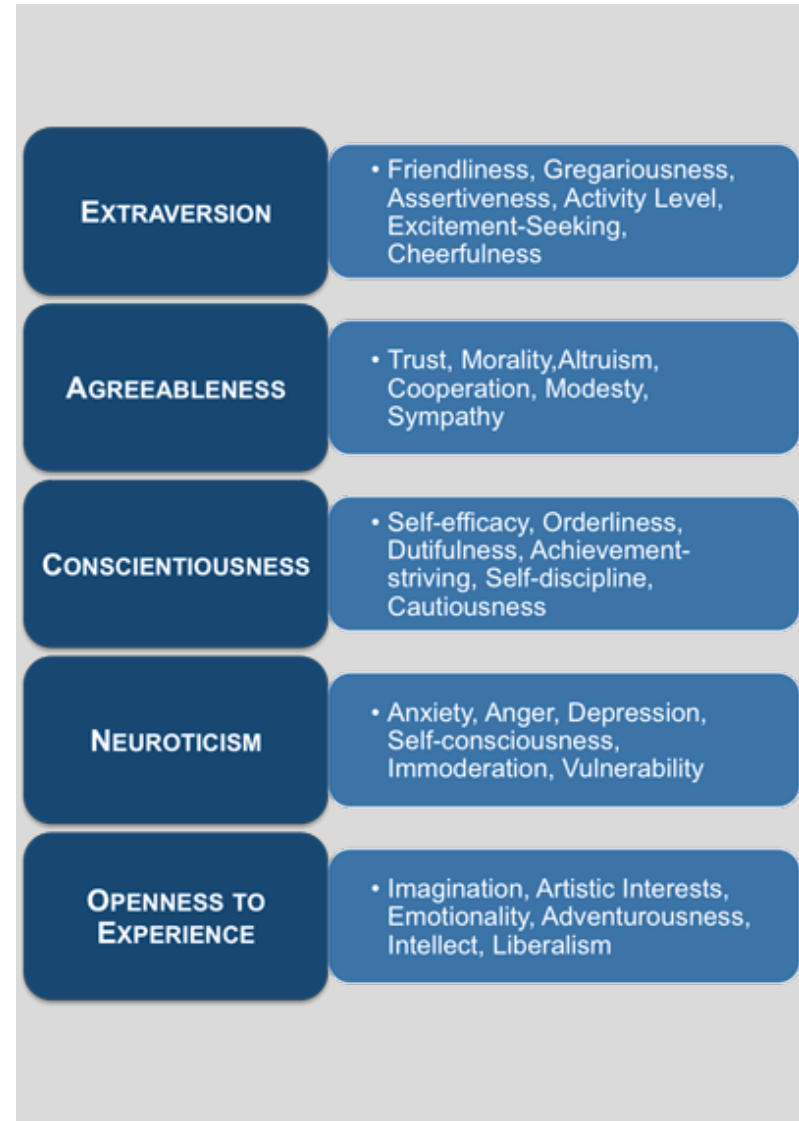
Five-Factor Model of Personality

Big-5 Traits:

- **O**penness to Experience
- **C**onscientiousness
- **E**xtraversion
- **A**greeableness
- **N**euroticism

Situation Specificity?

Online Personality?



Who is Vulnerable?

Does personality influence cybersecurity behaviour?

Halevi, Lewis, Memon, *WWW '13*, 2013

- Neuroticism most associated with responding to phishing email
- Openness with weak security settings.
- **No relationship between awareness of phishing and vulnerability**

McCormac, et al., *Computers in Human Behaviour*, 2017, 69, 151-156

- Conscientiousness, Agreeableness, Stability, Risk-taking explained variance in information-security awareness
- Age, gender did not

When are We Vulnerable?

Multitasking reduces comprehension of persuasive materials (*Jeong & Hwang, Journal of Communication, 2012, 62, 571-587*)

- Maybe also reduces critical analysis of material?
- **Generation Net** – more multitasking behaviours – but no better performance than older generations (*Judd, Computers and Education, 2013, 63, 358-367*)

Cognitive Load reduces learning rate and schema acquisition (*Sweller, Cognitive Science, 1988, 12, 257-285*)

May reduce cybersecurity behaviours (*Pfleeger, Caputo Computers And Security 2012, 4, 597-611*)

Attention/Distraction, Fatigue also likely candidates

The Human Element

- Up to 91% of cyber attacks begin with a phishing email
 - Up to 30% of phishing emails are opened
- Successful phishing attacks play on basic human motivations and emotions
 - Fear, curiosity, flattery, urgency, familiarity
- Individual (trait-level) differences in vulnerability
 - Personality, Working Memory Capacity
- Situational (state-level) differences in vulnerability
 - Multitasking, cognitive load, fatigue, distraction

Uncertainty and Decision Making

Dual-Process Model of Decision Making

Two neural systems:

Impulsive: amygdala-striatum, automatic, habitual, salient behaviours (Robbins, Cador, Taylor, Everitt, *Neurosci. Biobehav. Rev.*, 1989, 13: 155-162)

- Natural and non-natural rewards

Reflective: Prefrontal cortex. Forecasts the future consequences of behaviour and allows inhibitory control of automatic processes

(Everitt & Robbins, *Nature Neuroscience*, 2005, 8: 1481-1489)

- Executive Functions/Cognitive Control
- “Cool” and “Hot” EFs

“Cool” and “Hot” EFs

(Zelazo & Müller, *Handbook of Child Development*, 2002, 445-469)

“Executive Functions” allow conscious control of thought, emotion, and action

“Cool” Executive Functions:

abstract/decontextualised reasoning, working memory, strategic planning, performance monitoring, task switching.

Cognitive Control

“Hot” Executive Functions: self-monitoring for socially appropriate behaviours, emotion regulation, impulse control.

Affective Control

Iowa Gambling Task

Bechara, Damasio, Tranel, Anderson. *Cognition*, 1994, 50, 7-14

Simulates real-life decision making using uncertainty, rewards, and penalties.

High reward, high punishment decks:

Disadvantageous in the long run

Low reward, lower punishment decks:

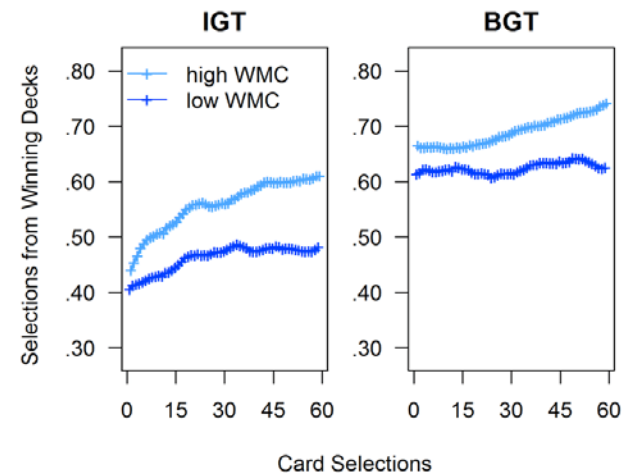
Advantageous

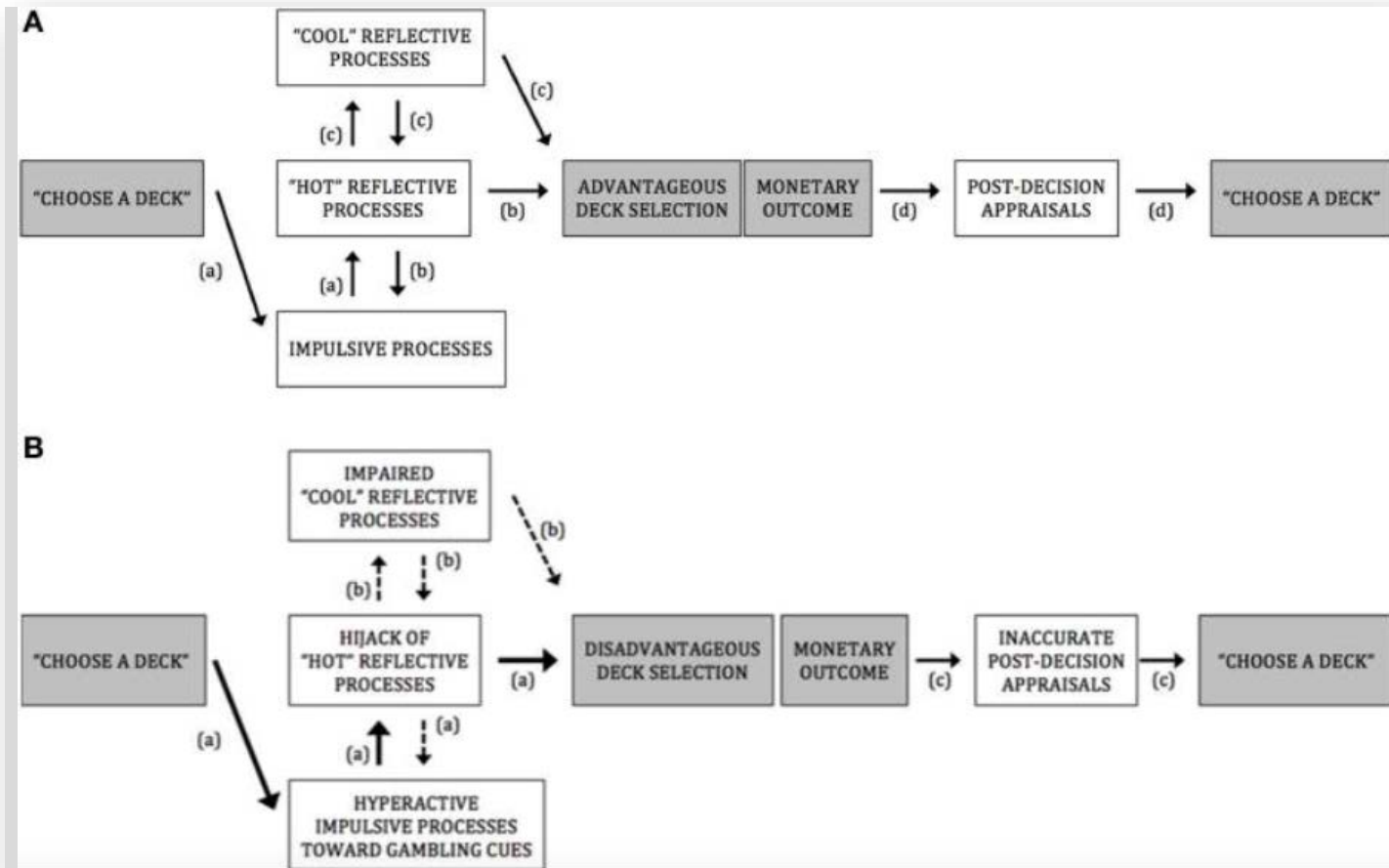
Hot EFs? Application to Cybersecurity?



Iowa Gambling Task

- Orbitofrontal Brain Damage
- Working memory capacity (WMC)
- Psychophysiology
- Intuition (*Turnbull et al., Brain and Cognition, 2005, 57, 244-247*)





Learning and Training

What is phishing?

Ever more convincing imitations of websites such as LinkedIn, eBay, PayPal and Google, and increasingly sophisticated emails have fooled users into allowing hackers past cyber defences. One recent attack mimicked a Gmail login page to near perfection. PayPal users were also targeted with a highly convincing email notifying them of a problem with their account.

It's incredibly effective. According to Verizon, 30% of phishing emails are opened. With reasons cited including fear, curiosity and a sense of urgency – all playing on basic human emotions.

The method is also surprisingly simple: once an employee receives an offer from a business he or she frequents, the user is tricked into entering their access credentials.

Once in possession of log-in credentials for the entire corporate network and systems and the breach begins.

Good Cyber Security Awareness Training is Broad with Online Ease of Delivery

Cyber security training must include multiple components to get the desired results:

1. Training must be ongoing
2. Different levels of employees need different training
3. Combining simulated threats with "lessons learned" training provides real world learning
4. Online course work can effectively teach what the broader threats are and how to react
5. Interactive training can be useful to develop team security behavior
6. Assessment is important to measure improvement
7. Training must be convenient or it will never get done

Feedback

Most effective when feedback occurs in close temporal proximity to behaviour.

In cybersecurity:

- Consequences of successful attack may not be obvious for weeks or months (or ever!)
- No feedback for successful defense



1) Alert fatigue— Monitoring systems with an **overabundance of alerts** aren't just ineffective but lethal. With so many low priority alerts, users simply ignore the alerts or have little ability to differentiate between those high and low priority alerts. And given the vast amount of data, it's impossible to respond to every single alert. For instance, at **Target**, the security team received and ignored alarms—in part because there were just so many. Many have pointed to this as human fallacy, but in reality it is a combination of human-computer interaction failure. With so many alerts, very few teams have the time or capabilities to sift through in depth every alert that is received. Even with the best judgment, systems with little ability to inform and prioritize alerts are simply ignored. In contrast, monitoring systems that integrate automation with human-driven domain expertise and prioritization could be a first step at more precise and **relevant** alerts, decreasing dwell time and expediting incident response.

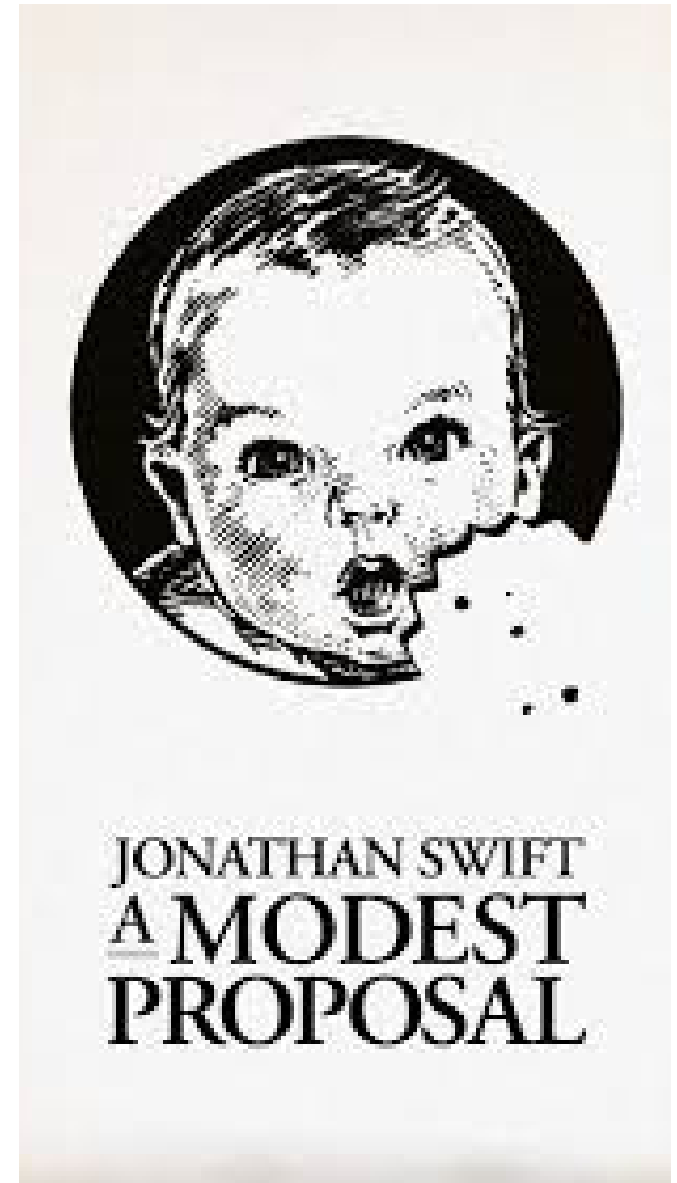
Improving Cybersecurity Behaviours

A Modest Proposal

Need to develop training methods that create mastery/self-efficacy in users.

False-phishing attacks raise awareness of the issue
But awareness does not correlate with behaviour

Rewards for good behaviour!





THE UNIVERSITY OF
AUCKLAND
Te Whare Wānanga o Tāmaki Makaurau
NEW ZEALAND

SCIENCE