

Cyber Security E-noculation

(Application of Inoculation Theory)

Dr. Joseph Treglia, Ph.D., Syracuse University

Melissa Delia, MS, CAS Information Security, Syracuse University

**20TH NEW YORK STATE CYBER SECURITY
CONFERENCE**

**12TH ANNUAL SYMPOSIUM ON INFORMATION
ASSURANCE (ASIA)**

JUNE 7 - 8, 2017

EMPIRE STATE PLAZA - ALBANY, NY



Problem

Social engineering is using deception, manipulation and influence to convince a human who has access to a computer system to do something, like click on an attachment in an e-mail.

- *Kevin Mitnick*

It also involves phone calls, mail, personal contact and other deceptive means to obtain information or access.

Problem

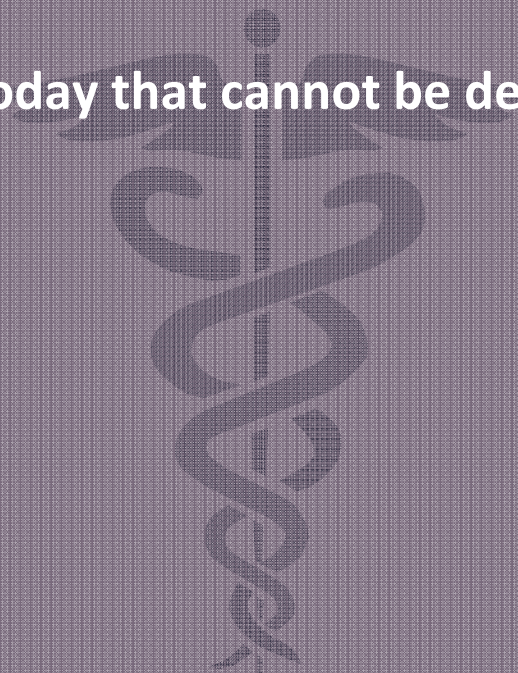
Social engineering has become about 75% of an average hacker's toolkit, and for the most successful hackers, it reaches 90% or more.

- *John McAfee*

Problem

There is no technology today that cannot be defeated by social engineering.

- Frank Abagnale



Problem

There is no technology today that can by itself defeat social engineering.

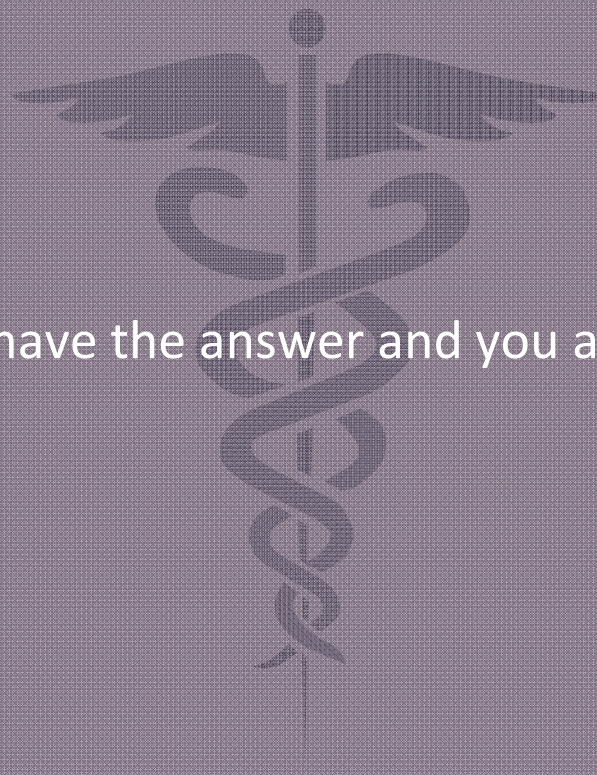
- Joe Treglia



WHAT CAN BE DONE?



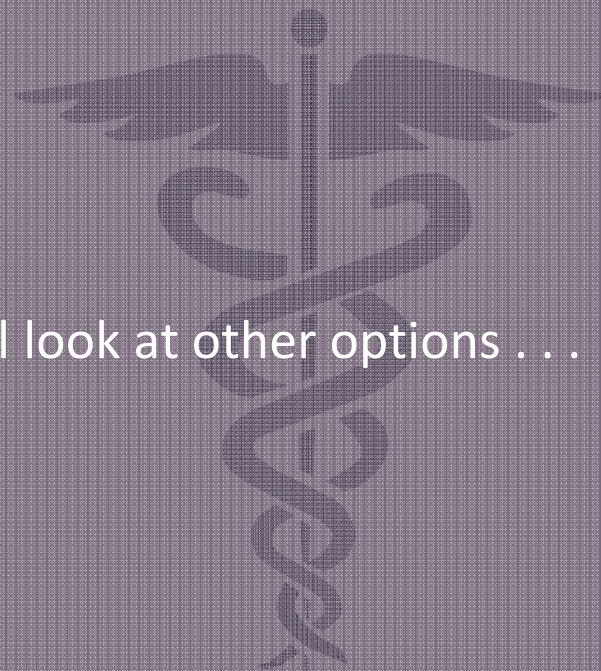
ELIMINATE ALL TECHNOLOGY.



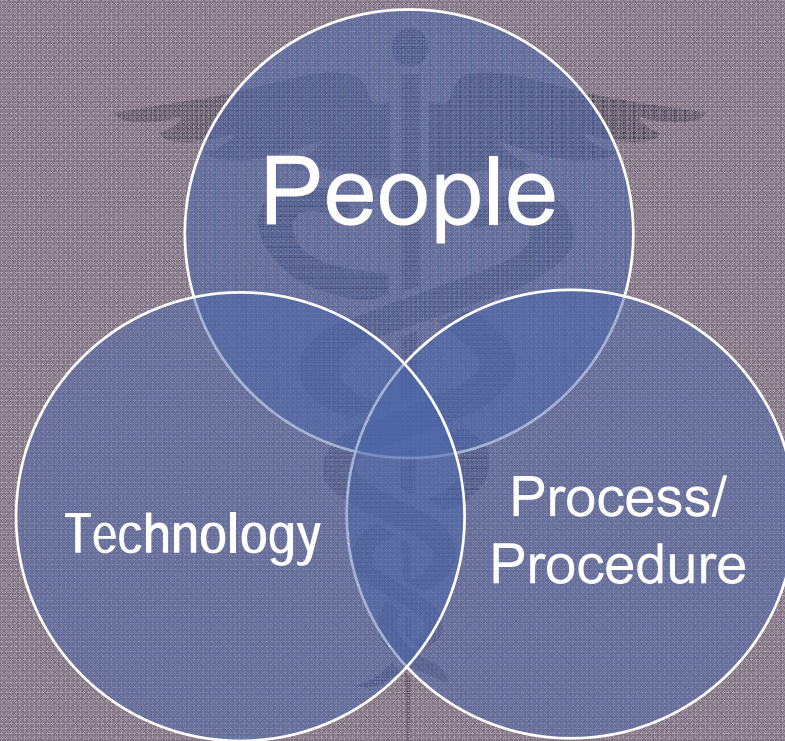
Thank you, we have the answer and you are all free to go.

OR

Ok, fine, we will look at other options . . .

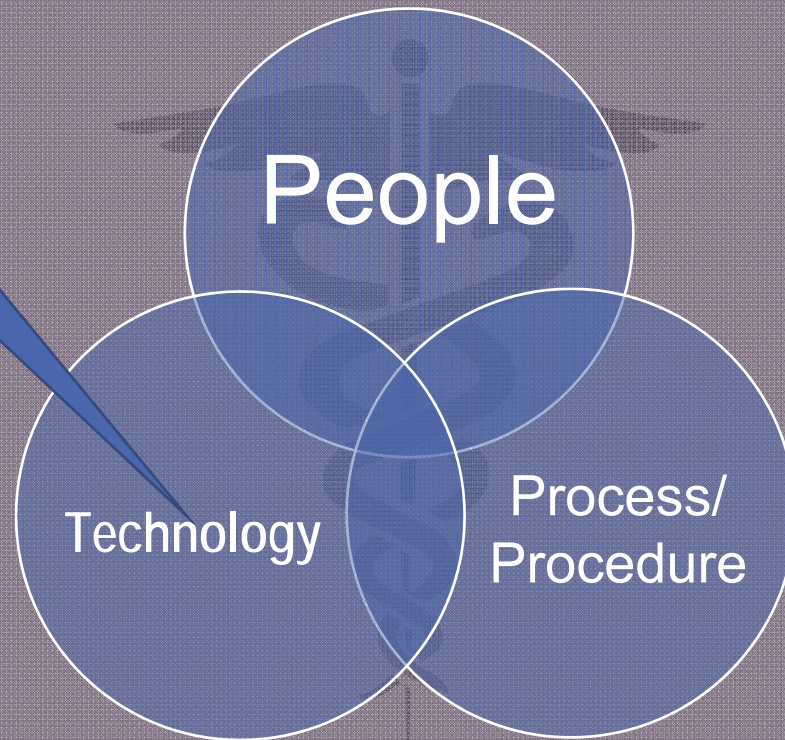


FIX THE “SYSTEM”

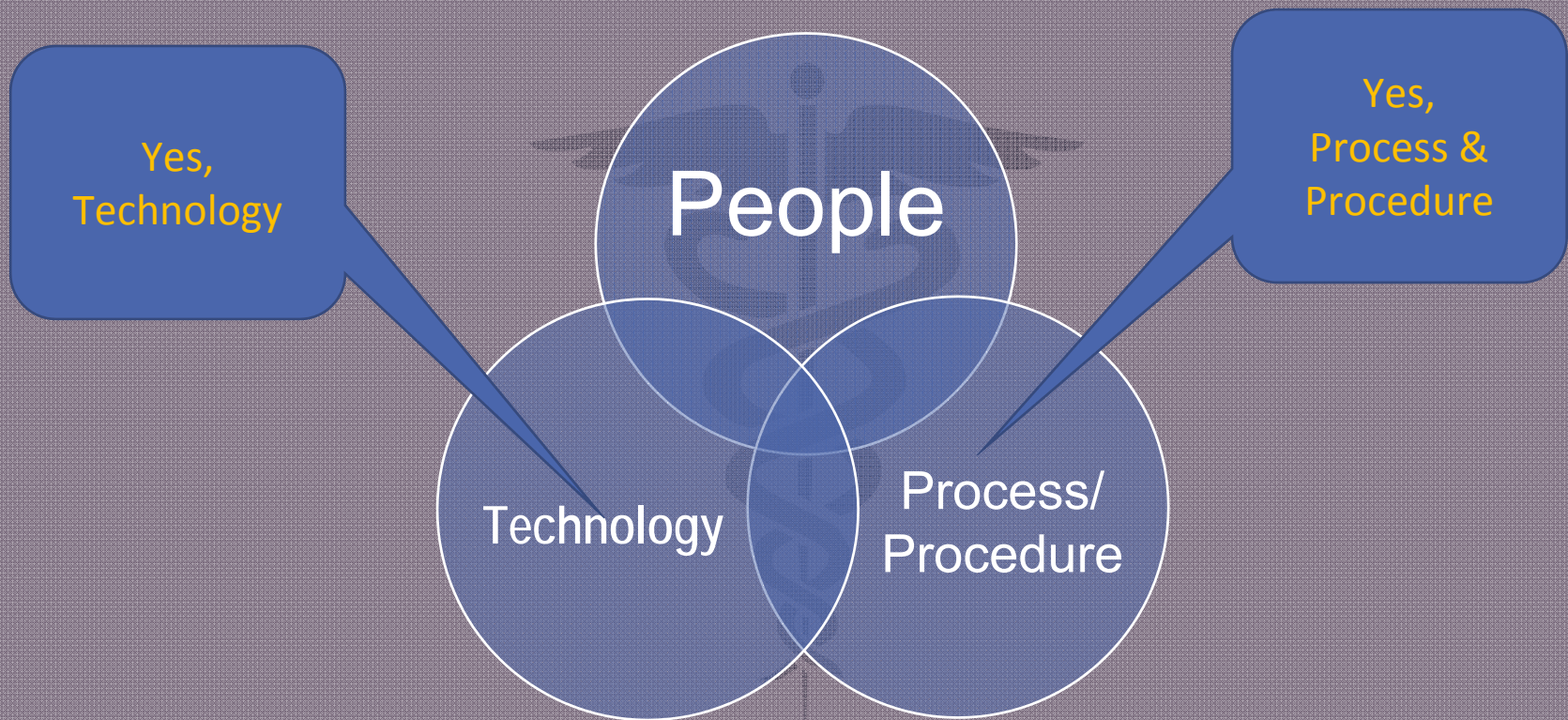


FIX THE “SYSTEM”

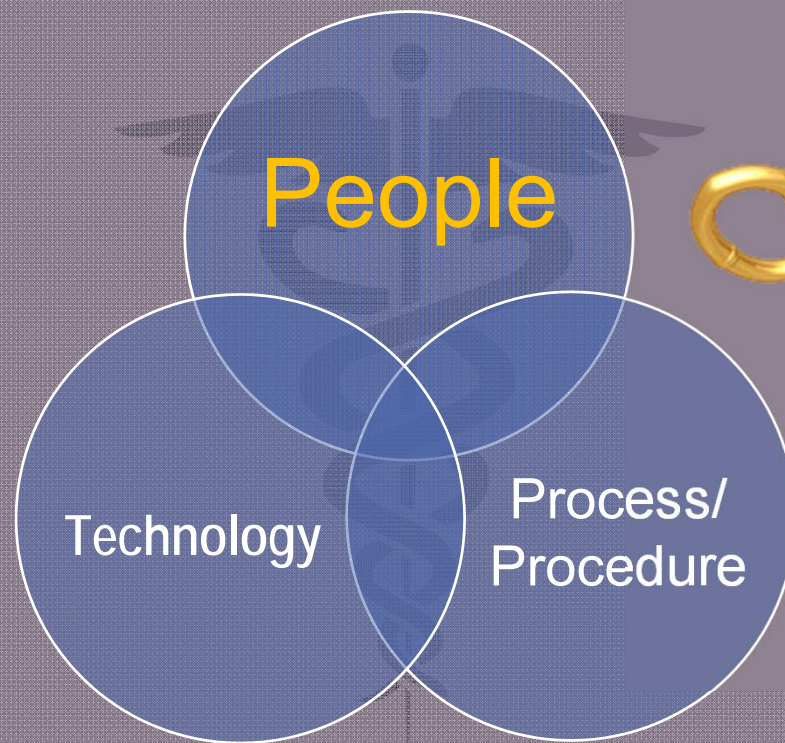
Yes,
Technology



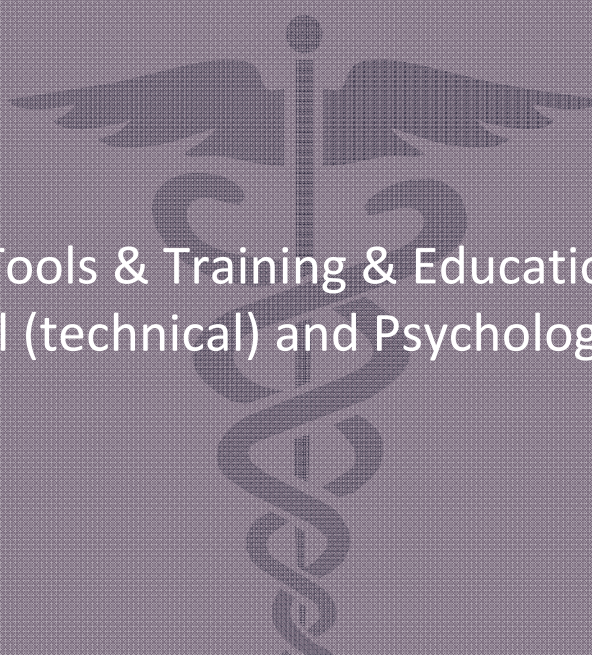
FIX THE "SYSTEM"



FIX THE “SYSTEM”



How?



Tools & Training & Education
– Physical (technical) and Psychological/Social

What?

Common - Tools & Training & Education:

Anti-virus, Firewalls, Media, Education and SOPs

Uncommon – Physical/Psychological/Social:

Inoculation - cyber security & social engineering or

“e-noculation”

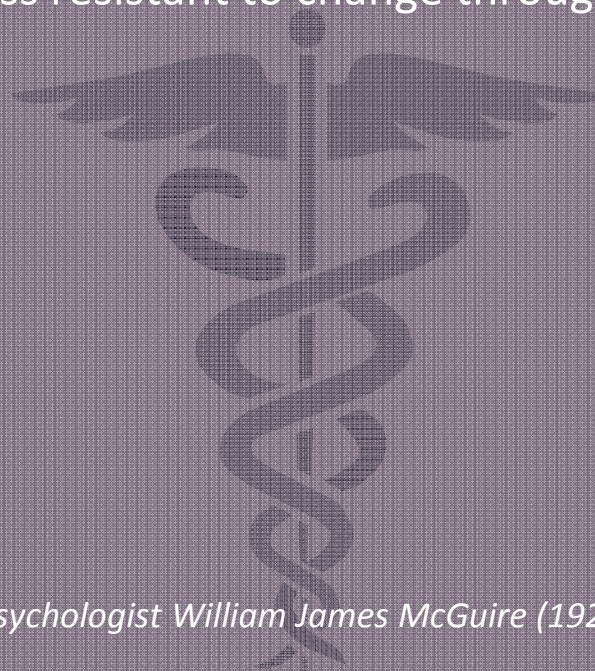
Can Cyber Inoculation solve problems with cybersecurity & social engineering?

Enhancing cybersecurity by protecting against social engineering, malware, virus, spyware or other “cyber infections” through “inoculation,” the key being **improved resistance to influence** *(as a new application of Inoculation Theory)*

Inoculation Theory

Inoculation Theory

A theory of resistance to persuasion according to which most ordinary attitudes and beliefs are more or less resistant to change through having been exposed to repeated mild attacks.



Theory formulated in 1964 by US psychologist William James McGuire (1925–2007); applied in other contexts.

Inoculation Theory

Inoculation Theory

A theory of resistance to persuasion according to which most ordinary attitudes and beliefs are more or less resistant to change through having been exposed to repeated mild attacks.

Theory predicts that resistance to persuasion can be markedly increased by a process of inoculation; exposing the recipients to relatively weak arguments against an issue together with rebuttals that recipients are either presented with or think up for themselves.

Inoculation Theory

Inoculation Theory

A theory of resistance to persuasion according to which most ordinary attitudes and beliefs are more or less resistant to change through having been exposed to repeated mild attacks.

Theory predicts that resistance to persuasion can be markedly increased by a process of inoculation; exposing the recipients to relatively weak arguments against an issue together with rebuttals that recipients are either presented with or think up for themselves.

Though this process people turn out to be much more resistant to persuasion, even when the arguments used in the attacking messages are different from those presented in the inoculation procedure.

Theory formulated in 1964 by US psychologist William James McGuire (1925–2007); applied in other contexts.

Cyber Security Inoculation

Cyber Security Inoculation

Inoculation Theory is referred to as the “most consistent and reliable method for conferring resistance to persuasion”

- Miller et al. in 2013



Inoculation Theory

Inoculation has been applied in varied contexts:

- ☐ Political Communication
- ☐ Marketing and advertising
- ☐ Public Relations
- ☐ Smoking Prevention
- ☐ Drinking
- ☐ Unprotected Sex
- ☐ Health-Related Policy

(now – Cyber security)



Inoculation in Medicine

Inoculation in Medicine

Inoculation (i- ,nä-kyə- 'lā-shən)

Introduction of microorganisms, infective material, serum, or other substances into tissues of living organisms, or culture media; introduction of a disease agent into a healthy individual to produce a mild form of the disease followed by immunity.

- *Dorland's Medical Dictionary for Health Consumers. © 2007 by Saunders, an imprint of Elsevier, Inc.*

Inoculation in Cybersecurity

Inoculation in Cybersecurity

e-noculation (ee nok"ula'shən)

Introduction of an electronic or other media based fraud, trap, trick, swindle, scam, or confidence game to the attention or experience of a person; the introduction of such hazardous or potentially damaging presentation to that person to produce an internalized, heightened awareness state of the hazard potential and delivery method followed by resistance (immunity) to similar or greater complexity threats.

- Treglia – work in progress

Inoculation in Cybersecurity

Inoculation in Cybersecurity

e-noculation - form and delivery

The fraud should be created such that it is similar to current threats that we wish to protect the person from, not cause harm, and be readily identifiable as a threat.

It is important the that threat capture the interest and attention of the person involved, and even create a degree of concern.

Practically speaking – it should look and act like a version of the real thing

- Treglia – work in progress

E-noculation and Social Engineering Cyber Security Application

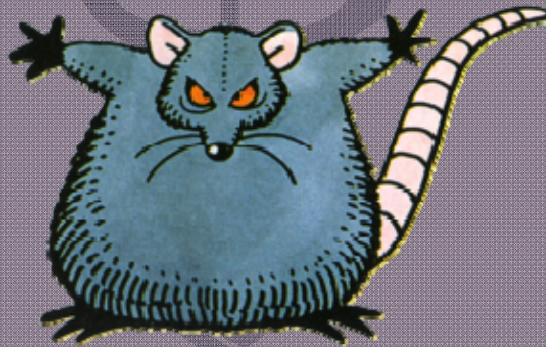
Cyber Security e-noculation for Social Engineering is the proposition that people can be exposed to the virus (Social Engineering attacks) and develop an immunity (response and resistance) to these exploits due to heightened awareness and resilience to scams and other like social engineering attacks.

E-noculation in practice

E-noculation in practice

Next up

- The Rat
- Activity
- Real world





Cyber Security Inoculation

Cyber Security Inoculation

- ❑ Problem –
 - ❑ Malware, virus, spyware, identity theft etc.
 - ❑ Systems increasingly complex, layers of security, logging and monitoring, heuristic IPS/IDS/DLP
 - ❑ People – Easier to exploit
 - Reverence model (Spearphishing)
 - Customer Service (helpful)
 - Unaware/Untrained
 - Social Engineering exploits natural human behavior and herd mentality
 - ❑ Social Media
 - Hacks
 - Exploits
 - Viral social media posts

Issues – “Free Riding”

Issues – “Free Riding”

Herd immunity is vulnerable to “Free riding” - People who lack immunity, and choose not to vaccinate (participate), “free ride” off the immunity created by those who are immune.

However - As number of free riders increases, outbreaks of preventable viruses/attacks become more common and more severe and protection is lost.

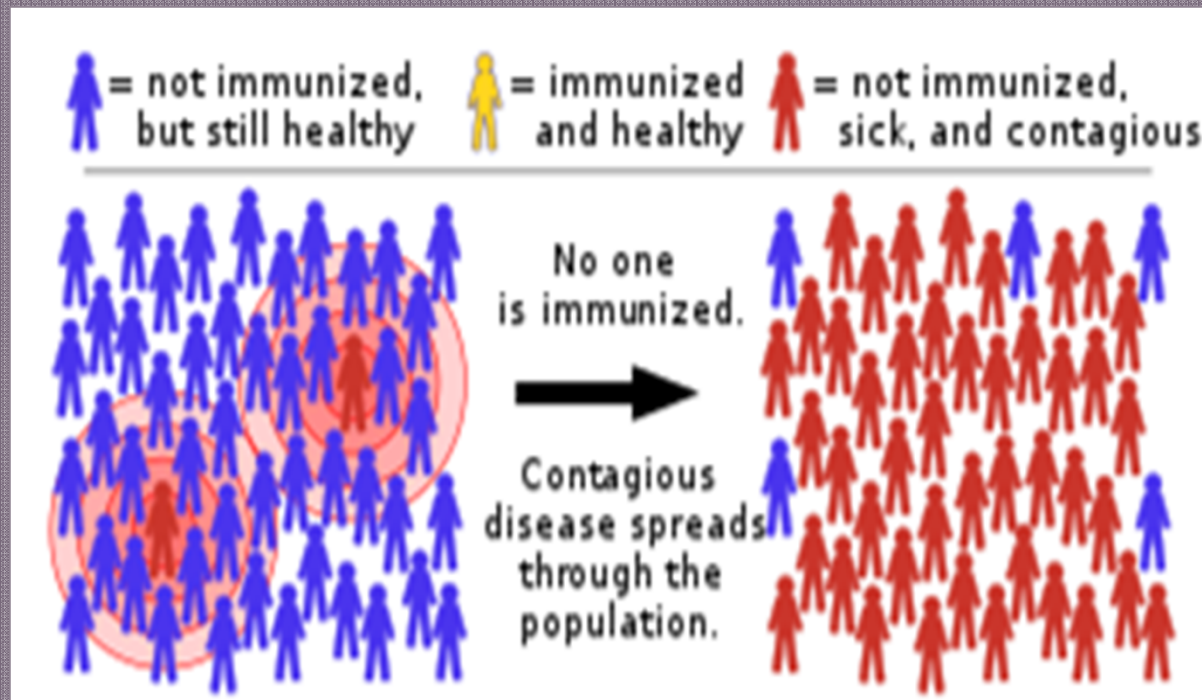
(Fukuda & Tanimoto, 2014; Barrett, 2014; Parker, Vardavas, Marcum & Cidengil, 2013)

OPTIMAL PARTICIPATION IS KEY

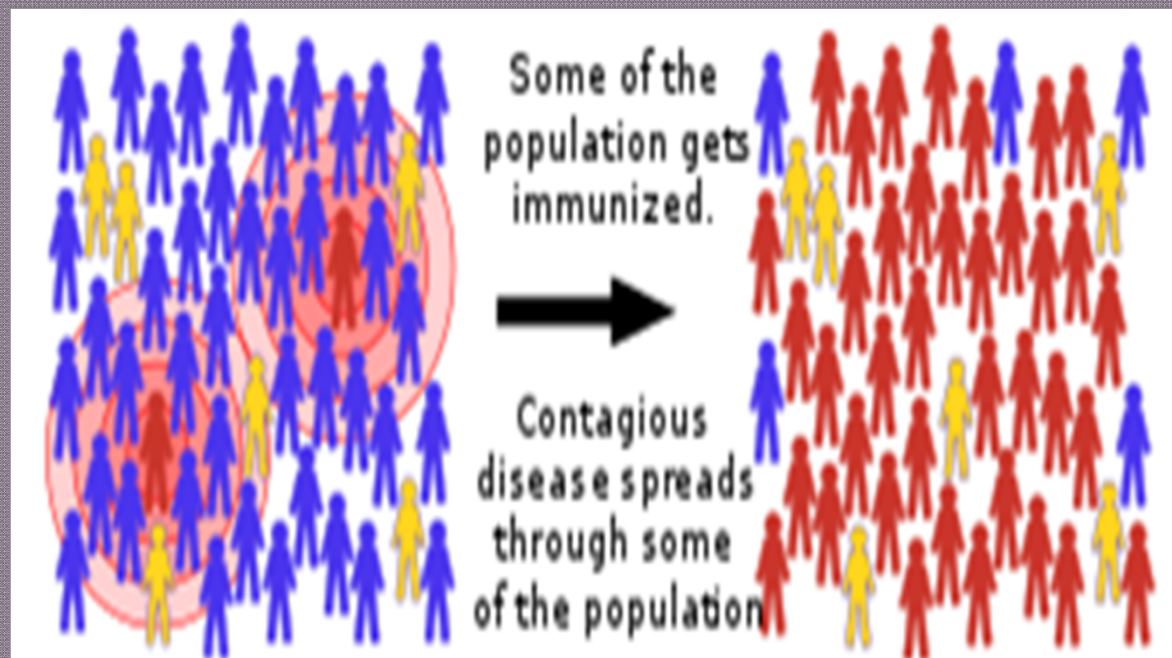
Cyber Security Inoculation

- Immunization Theory and Herd Immunity
 - Just as immunizations are not effective if only a few receive (ex. Flu shot)
 - The group at large must be inoculated for maximum effectiveness
- Inoculation, Herd Immunity and Network Node Theory
 - Inoculate the group, result is heightened sensitivity, more aware.
 - Inoculation works like network theory in that as network nodes expand exponentially to grow the network its value grows.
 - 1-2 nodes will not build a network. 1-2 vaccinations will not help inoculation and improve immunity for the group.

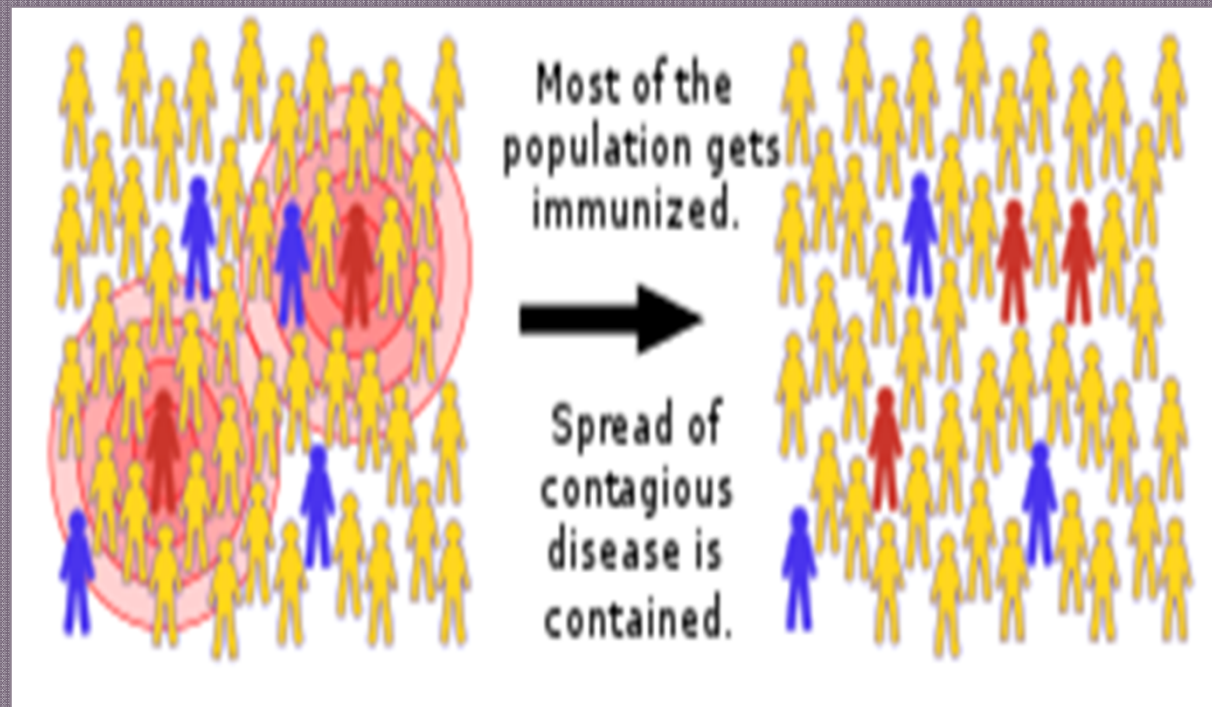
Herd Immunity



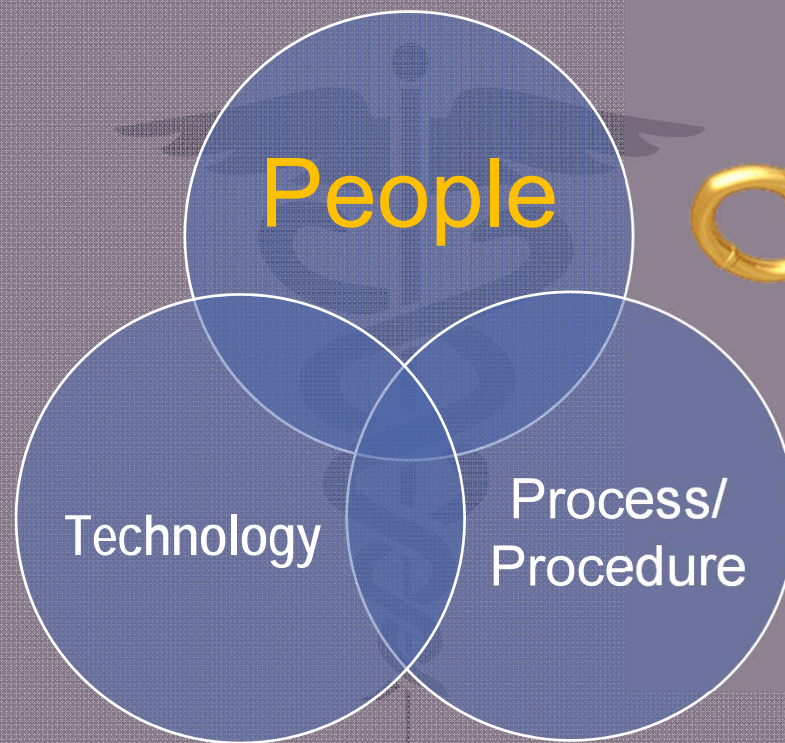
Herd Immunity



Herd Immunity



Solution...People



Real World E-noculation

Real World E-noculation

Phishing campaigns - baited emails, used to seeing and reacting to them

Circulate Training Materials and Workshops

Raise Awareness

Securitoons


Banners and posters

Playing cards

Anatomy of a Phishing Email

Anatomy of a Phishing Email

Even the BEST have flaws...

1. **Paypal** vs PayPal vs Paypal !
 2. HEADER from **Paypal** <test@test.com>
 3. Allow ActiveX
 4. Formatting '**securely**'
 5. **PayPal**-Account Update Form.pdf.htm
- 

You have changed your PayPal email address

Inbox | X

Print all

★ **Paypal**

[show details](#) Mar 27

Reply

Dear **Paypal** member,

You have added adelaidegerard@gmail.com as a new email address for your **Paypal** account.

If you did not authorize this change, check with family members and others who may have access to your account first. If you still feel that an unauthorized person has changed your email, submit the form attached to your email in order to keep your original email and restore your PayPal account.

If you are using Internet Explorer please **allow ActiveX** for scripts to perform all data transfers securely.

Thank you for using **Paypal** !

Please do not reply to this email.

This mailbox is not monitored and you will not receive a response.

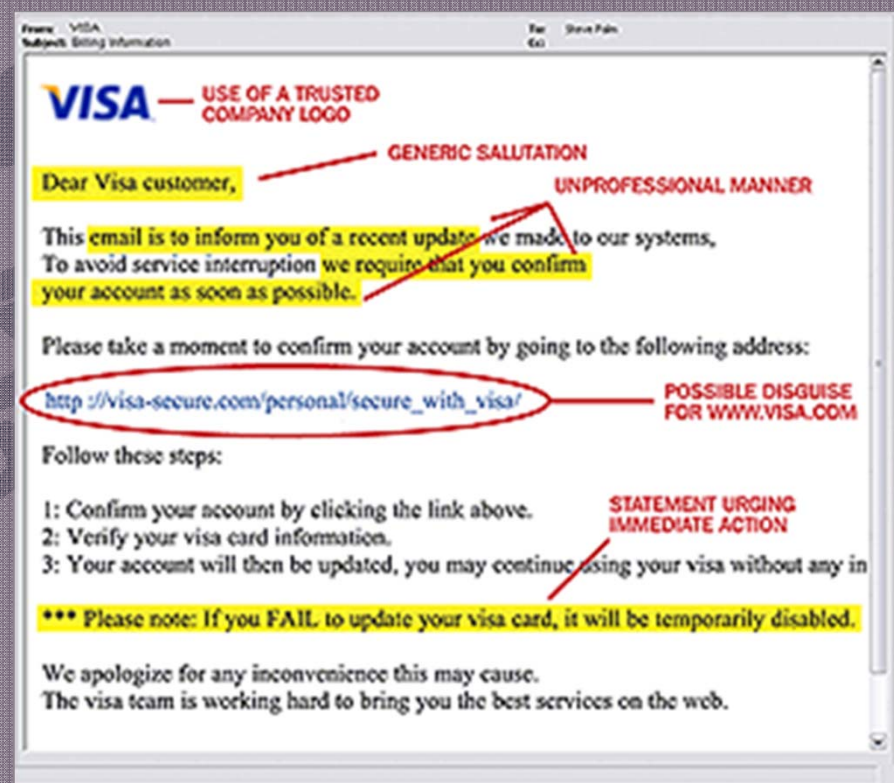
Copyright © 1999-2011 PayPal. All rights reserved.



PayPal- Account Update Form.pdf.htm

32K [View](#) [Download](#)

★ from **Paypal** <test@test.com>
to [redacted]
date Sun, Mar 27, 2011 at 11:34 PM
subject You have changed your PayPal email address



Does the sender's email look as though it belongs to where it suggests it's coming from? Does it look genuine?

From: University of Nottingham Help Desk [mailto:phishing@botmail.up]
Sent: 25 February 2015 12:01
To: Recipients
Subject: HelpDesk Urgent action required!!!!

Be aware of any email asking for urgent action. If it's that urgent they will email you again

Dear User,

Who is the email directed to? Phishing emails are rarely specific.

We are noticing your email account is out of date and needs upgrading.

Please click the following link urgently to validate your email address. [here](#)

<http://giveusyourdetails.com/wewillusethem/againstyou.aspx>
Ctrl+Click to follow link

If you do not do this your account will be no longer be available.

Thank you for your immediate action.

Regards,

Uni of Nottm.

Look out for grammar and spelling. These can be a tell-tale sign of phishing.

Hover over the link without clicking on it. Does the link displayed take you to where you would expect

Oops! You clicked on a phishing email.

Remember these three 'Rules To Stay Safe Online'

✓ RULE NUMBER ONE:

- Stop, Look, Think!
- Use that delete key.

✓ RULE NUMBER TWO:

- Do I spot a Red Flag?
- Verify suspicious email with the sender via a different medium.

✓ RULE NUMBER THREE:

- "When in doubt, throw it out". There are a thousand ways that internet criminals will try to scam you, and only one way to stay safe:
Stay alert as YOU are the last line of defense!



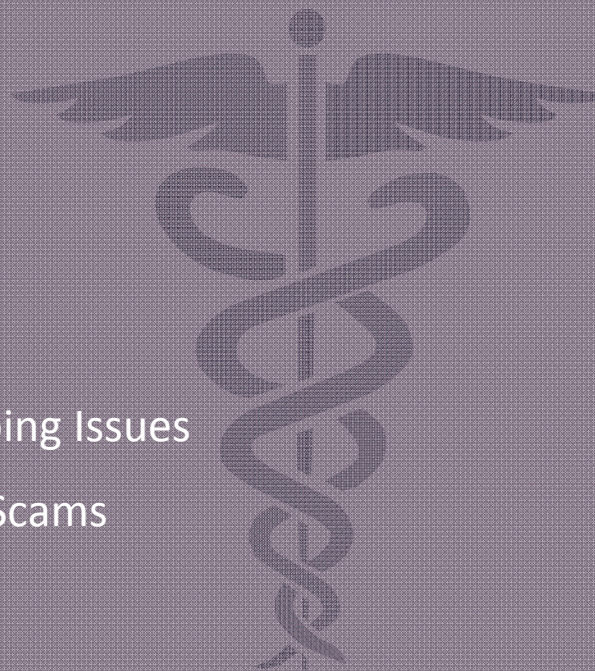
PLEASE NOTE:

This message came from KnowBe4, LLC and not from the company whose name is mentioned in the body of the email message, as that company has no association with KnowBe4, LLC and does not endorse the services of KnowBe4, LLC. The purpose of this message is to demonstrate how phishing attacks can come in emails that deceptively appear to be from reputable companies.

Social Engineering Samples

Social Engineering Samples

- ❑ Phishing
- ❑ Vishing / VoIP Phishing
- ❑ Facebook/Social Media
- ❑ USB Flash Drive
- ❑ “Free” Apps
- ❑ Holiday UPS/FedEX Shipping Issues
- ❑ Natural Disaster Charity Scams



Case Study Training Opportunities

Case Study Training Opportunities

- ❑ Incidents as learning/training opportunities – exposure with an impact
- ❑ Customer Service Call Center “brute force” Vishing
- ❑ Campus-wide “free” USBs
- ❑ Phishing Campaign Converts Wannacry into ROI
- ❑ Printer/Copier Tech Support
- ❑ The “Blind” attack
- ❑ Connect Here for Free Wifi - the AP Hack

Professional Social Engineering Vendors

- ❑ PhishMe
- ❑ KnowBe4
- ❑ Wombat
- ❑ SecOwl



OSINT - Free Open Source Intelligence Tools

OSINT - Free Open Source Intelligence Tools

- ❑ GoPhish
- ❑ Social Engineer Toolkit (SET)
- ❑ Maltego
- ❑ US Computer Emergency Response Team [CERT](#) Resources
 - ❑ Security Organizations
 - ❑ Vulnerability Information
 - ❑ Tools, Techniques, Research, Guidelines
 - ❑ Education
 - ❑ Information Sharing and Analysis Centers (ISACs)
- ❑ [Kali 4Tools](#)
- ❑ Google Hacking Database (GHDB)

Assess Yourself

- [Corporate Security Checklist: A CEOs Guide to Cybersecurity](#)
- [Security Controls Assessment Template](#)
- [SANS checklists and step by step guides](#)
- [Benchmarks and Scoring Tools](#)
- [Microsoft Security Audit and Compliance](#)
- [O365 Secure Score](#)
- [Open Web Application Security Project \(OSWAP\)](#)
- [OSWAP Phishing](#)

Closing Remarks

Closing Remarks

- ❑ NYS IT Director's Conference resource identified gaps working together to identify solutions and shared service opportunities. Can be doing more to share practices, tips and tricks and benefits of the trade to make that sharing happen and additional resource.

Paul.Lutwak@madisoncounty.ny.gov

- ❑ Interactive Engagement
- ❑ Positive Reinforcement and Feedback
- ❑ Ongoing Training

References

- ❑ Banas, John A., and Stephen A. Rains. "A Meta-Analysis of Research on Inoculation Theory." *Communication Monographs* 77, no. 3 (September 1, 2010): 281–311. doi:10.1080/03637751003758193.
- ❑ Benoit, William L. "Two Tests of the Mechanism of Inoculation Theory." *Southern Communication Journal* 56, no. 3 (September 1, 1991): 219–29. doi:10.1080/10417949109372832.
- ❑ Butavicius, Marcus, Kathryn Parsons, Malcolm Pattinson, and Agata McCormac. "Breaching the Human Firewall: Social Engineering in Phishing and Spear-Phishing Emails." *arXiv:1606.00887 [Cs]*, May 28, 2016. <http://arxiv.org/abs/1606.00887>.
- ❑ Compton, Joshua A., and Michael Pfau. "Inoculation Theory of Resistance to Influence at Maturity: Recent Progress In Theory Development and Application and Suggestions for Future Research." *Annals of the International Communication Association* 29, no. 1 (January 1, 2005): 97–146. doi:10.1080/23808985.2005.11679045.
- ❑ "Inoculation Theory | Communication Theory." Accessed May 3, 2017. <http://communicationtheory.org/inoculation-theory/>.
- ❑ Ivanov, Bobi, Michael Pfau, and Kimberly Ann Parker. "The Attitude Base as a Moderator of the Effectiveness of Inoculation Strategy." *Communication Monographs* 76, no. 1 (March 1, 2009): 47–72. doi:10.1080/03637750802682471.
- ❑ McGuire, William J. *Advances in Experimental Social Psychology*. Academic Press, 1964.
- ❑ "U INDUCING RESISTANCE TO PERSUASION." *Advances in Experimental Social Psychology* 1 (1964): 191.
- ❑ Parker, Kimberly A., Stephen A. Rains, and Bobi Ivanov. "Examining the 'Blanket of Protection' Conferred by Inoculation: The Effects of Inoculation Messages on the Cross-Protection of Related Attitudes." *Communication Monographs* 83, no. 1 (January 2, 2016): 49–68. doi:10.1080/03637751.2015.1030681.
- ❑ Pfau, Michael, Steve Van Bockern, and Jong Geun Kang. "Use of Inoculation to Promote Resistance to Smoking Initiation among Adolescents." *Communication Monographs* 59, no. 3 (September 1, 1992): 213–30. doi:10.1080/03637759209376266.
- ❑ Pfau, Michael, Bobi Ivanov, Brian Houston, Michel Haigh, Jeanetta Sims, Eileen Gilchrist, Jason Russell, Shelley Wigley, Jackie Eckstein, and Natalie Richert. "Inoculation and Mental Processing: The Instrumental Role of Associative Networks in the Process of Resistance to Counterattitudinal Influence." *Communication Monographs* 72, no. 4 (December 1, 2005): 414–41. doi:10.1080/03637750500322578.
- ❑ Pfau, Michael, David Roskos-Ewoldsen, Michelle Wood, Suyu Yin, Jaeho Cho, Kerr-Hsin Lu, and Lijiang Shen. "Attitude Accessibility as an Alternative Explanation for How Inoculation Confers Resistance." *Communication Monographs* 70, no. 1 (January 1, 2003): 39–51. doi:10.1080/715114663.
- ❑ "Social Immunity." *Wikipedia*, April 18, 2017. https://en.wikipedia.org/w/index.php?title=Social_Immunity&oldid=775973534.
- ❑ Fukuda, E.; Tanimoto, J. (4 November 2014). Impact of Stubborn Individuals on a Spread of Infectious Disease under Voluntary Vaccination Policy. Springer. pp. 1–10. ISBN 9783319133591. Retrieved 30 March 2015.
- ❑ Barrett, Scott (15 December 2014). "Global Public Goods and International Development". In J. Warren Evans, Robin Davies. Too Global To Fail: The World Bank at the Intersection of National and Global Public Policy in 2025. World Bank Publications. pp. 13–18. ISBN 978-1-4648-0310-9.
- ❑ Parker, A. M.; Vardavas, R; Marcum, C. S.; Gidengil, C. A. (2013). "Conscious consideration of herd immunity in influenza vaccination