## Instilling Cyber Hygiene Among Users and Creating a Culture of Cyber Safety

Arun Vishwanath, PhD, MBA Technologist & CTO Avant Research Group Web: https://www.arunvishwanath.us Email: arun@arunvishwanath.us



For a decade and a half I have been studying the hard problem of cyber security...

...the "PEOPLE" problem.

As a	an a	cade	emi	С
------	------	------	-----	---

Vishwanath, A., Xu, W., & Ngoh, Z. (2018). How People Protect their Privacy on Facebook: A Cost-Benefit View. The Journal of the American Society for Information Science & Technology.

Vishwanath, A. (2017). Getting Phished on Social Media. Decision Support Systems.

Vishwanath, A., Harrison, B., & Ng, Y.J. (2016). Suspicion, Cognition, Automaticity Model (SCAM) of Phishing Susceptibility. Communication Research.

Vishwanath, A. (2016). Mobile Device Affordance: Explicating How Smartphones Influence The Outcome Of Phishing Attacks. Computers in Human Behavior.

Vishwanath, A. (2015). Habitual Facebook Use and its Impact on Getting Deceived on Social Media. Journal of Computer-Mediated Communication, 20(1), 83-98.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decision Support Systems, 51 (3), 576-586.



### Where's the outrage over the Sony hack?

By Arun Vishwanath

updated 11:00 AM EST, Wed December 17, 2014

### Dial 211 for cyberattacks

The Cybercrime Support Network aims to be the 911 for cyberattack victims.

### 🖸 🖪 🛅 🙆 🖸



Columnist, CSO | OCT 31, 2019 3:00 AM PDT

### Opinion Political Op-Eds Social Commentary

## Time to rethink apps security

By Arun Vishwanath Updated 8:00 PM ET, Fri April 1, 2016

#### DPINION

### Forget Facebook, Twitter or Google – it's the internet's 'dark triad' that we need to protect ourselves against

Those platforms and services are mere vehicles providing a convenient platform for what was a much larger propaganda process made possible by spear phishing, trolling and fake news.



O Firefox Monitor

. Sign in

### See if you've been part of an online data breach.

Find out what hackers already know about you. Learn how to stay a step ahead of them



https://slate.com/technology/2013/06/cyber-hygiene-vint-cerf-s-concept-of-personal-cybersecurity-is-problematic.html The idea of cyber-hygiene can be traced back to Vint Cerf, an early architect of the Internet and Google's current "chief Internet evangelist," who says he came up with the idea when thinking about teeth brushing, but, you know, for your computer.

## While there is no question there is a need for cyber hygiene:

US Crime + Justice Energy + Environment Extreme Weather Space + Science

## New Orleans mayor declares state of emergency in wake of city cyberattack

DBIR

verizon



By Amir Vera, CNN () Updated 0130 GMT (0930 HKT) December 14, 2019

55% of companies attacked once, are attacked again!

## There appears to never be enough of it...

	•	•	
9	12	e	_
	Ε.		

HOME WEATHER TALKERS NEWS

## Practice good 'cyber hygiene' to protect your smart devices

Seemingly everything is connected to a WiFi network: Ring cameras, smart TVs, smart locks on your front door and even smart fridges.

Tuesday, December 10th 2019, 6:49 PM EST by Evan Dean

#### The Washington Post

### **PowerPost**

Follow @powerpost Get the Cybersecurity 202 Newslette

**PowerPost** Analysis

The Cybersecurity 202: Agencies struggling with basic cybersecurity despite Trump's pledge to prioritize it

## **Obama's Cyber Legacy: He Did (Almost) Everything Right and It Still Turned Out JANUARY 17, 2017** Wrong

Obama took cyber seriously and tried to tame it, but we're no safer in cyberspace today than we were eight years ago, experts tell Nextgov.

## But what is Cyber Hygiene?

"Cyber hygiene is the most important life skill we'll be teaching our children over the coming decade..." Ben Hammersley, Editor at large, Wired UK

"Fighting infections in the 21<sup>st</sup> century is less about washing your hands and more about not clicking on untrusted email attachments..." Ben Hammersley, Editor at large, Wired UK

ENISA (2016) conclusion "no clear definition or approach" but "cyber hygiene should be viewed in the same manner as personal hygiene"

US-DHS (Dept. of Homeland Security) has instituted CDM (Continuous Diagnostics and Mitigation) that is built on the NIST framework with a hygiene score

REF: <u>https://www.theguardian.com/technology/2013/jun/16/future-of-behaviour-concepts-for-21st-century;</u> ENISA, (European Union Agency for Cyber Security) Review of cyber hygiene practices, 2016.

## Inspired by the health analogy...



https://pbs.twimg.com/media/D-AgpcYWsAE2I8O.jpg https://entertainmentheat.com/good-cyber-hygiene-what-is-it/

## Inspired by the health analogy...





### CYBER SECURITY IS CYBER HEALTH e.g., https://h-xtech.com/blog-healthcare-analogy

- "Poor Heredity" = unreliable or obsolete components
- "Promiscuous sex" = indiscriminate use of unreliable software
- "Unbalanced nutrition" = poor "digestion" of business processes and technological processes
- Pregnancy" = development plans in need of security
- "Psychological help" = subjective security
- Multivitamins = anti-virus patches

# Does it matter how we define or conceptualize it?



## Soaring on the wings of eagles...

• Take the case of human flight









## Difference between public health and computing "health"

- Evolved defenses vs. dummy terminals
- Risk cascades

10 percent failure rate in SSL certificates; used in email based phishing attacks with a 10 percent relevance; on an email network that allowed 10 percent of these emails through; 10 percent of the users opening the email: Probability of a breach = 34 percent (computed (1-.90<sup>k</sup>))

• Creates implicit trust in solutions and practices: complacency, conflation, habituation

## Lessons from applying good cyber hygiene" practices...

## New NIST guidelines banish periodic password changes



Bob Covello 9:47 am, May 19, 2017

01002000100110201	00001001002205101001001000001010011100
10110100100100100101	1001101001001001001000010000100001000000
11011000730.20	Username username 1110120100ce1100
100000100100000	Password 10001000 10 100
1010010010000001	
010000001101100	Login Register 0010010000001101
01000000110011203	010010110001001100010011001010111001001
01000000100110000	0000001001100010000010010000001001000000

While working for the National Institute of Standards and Technology in 2003, Bill Burr wrote "NIST Special Publication 800-63. Appendix A" — a document that included the widely adopted recommendation that strong passwords should include a range of characters and should be changed every 90 days.

"Much of what I did I now regret," Burr, 72, told the Wall Street *Journal* in a recent interview, adding that the recommendation made for complicated passwords.

## So what's the solution?



## Defining user cyber hygiene and measuring it

 Conceptually: the cyber security practices that online consumers should engage in to protect the safety and integrity of their personal information. (Vishwanath et al. 2019)\*

Ref: Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, *128*, 113160.



### Cyber Hygiene Inventory (CHI)©: 20 questions



### Sample "Storage and Device Hygiene" questions:

- how to check your device to ensure it has the latest OS, software update, or patch
- how to accurately monitor different processes such as CPU, power, or network usage on your device
- how to correctly run a virus scan on any new USB or external storage device

## Sample "Authentication and Credential Hygiene" questions:

- how to enable two-factor or multi-factor authentication for logins
- how to change default passwords on all Internet enabled devices
- how to change default username from "administrator" to something unique on all Internet enabled devices

#### Sample "Transmission Hygiene" questions:

- how to manage computer discovery on public networks
- how to restrict who can connect to your device via Bluetooth
- how to appropriately check the quality of the SSL certificate when doing online financial transactions

### Tracking Cyber Hygiene Using the Cyber Hygiene Inventory (CHI)



## CHI Advantages

- Quantitative
- Granularity
- Agnostic
- Cognitive-Behavioral
- Adaptable

## Strategic Map for Prioritizing Cyber Hygiene Solutions





## Assessing users' K-A-C GAPS





## Assessing training effects





Building a culture of cyber hygiene using CHI



• 1. Measurement driven with CHI



https://ireta.org/resources/measurement-based-care-and-outcomes-monitoring-in-addictions-treatment/



Track, Inform, Influence

Does your reporting portal do more than collect emails?

• 2. Adopt a cognitive-behavioral risk-based approach to training and awarding privileges

BLACK HAT	T   WEBCAST	
	INCORPORATING HUMAN VULN	IERABILITY ASSESSMENTS INTO YOUR
About		
Contact	Thursday, March 29, 2018	
Privacy	8:00AM-9:00AM PDT 60 MINUTES, INCLUDING Q&A	VIEW RECORDING

https://www.blackhat.com/html/webcast/03292018-incorporating-human-vulnerability-assessments-into-your-threat-assessment-model.html

### • 3. Change the emphasis from procedural to declarative knowledge





Gloves, however, have created a false sense of security with handlers that bacteria can't get into the food and thus, they only wash their hands 27% of the time it's recommended to...

https://www.foodbeast.com/news/glove-prep-cross-cont/

### • 4. Public health vs. an OPSEC view







### • 5. All or nothing to a graduated information based point system



## What is risk from password reuse?

 Chance of a compromise if you reuse your password on 3 +1 device + 1 child, each with a 5% chance of compromise = 23%



#### https://www.greentreelibrary.org/storyline-online/

## Awareness + Knowledge + Capacity + Communication = Utilization



- For copy whitepaper, CHI questionnaire, training information, email: <u>arun@arunvishwanath.us</u>;
- Website: https://arunvishwanath.us