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 an academic
Technologist in the public interest
Where's the outrage over the Sony hack?
By Arun Vishwanath
updated 11:00 AM EST, Wed December 17, 2014

Time to rethink apps security
By Arun Vishwanath
Updated 8:00 PM ET, Fri April 1, 2016

Dial 211 for cyberattacks
The Cybercrime Support Network aims to be the 911 for cyberattack victims.
By Roger A. Grimes
Columnist, CISO | OCT 31, 2019 3:00 AM PDT

Consumer Reports launches digital lab to rate on privacy, inform policy

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.

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.
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:

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

55% of companies attacked once, are attacked again!
There appears to never be enough of it...

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 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 Wrong

JANUARY 17, 2017

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 21st 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

Inspired by the health analogy...
Inspired by the health 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 \(1-.90^k\))

• Creates implicit trust in solutions and practices: complacency, conflation, habituation
Lessons from applying good cyber hygiene” practices...

New NIST guidelines banish periodic password changes

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)*

Two-dimensional map of Cyber Hygiene concepts
Cyber Hygiene Inventory (CHI)©: 20 questions

Storage and Device Hygiene
Questions measure patch management, virus protection, and CPU/network use management

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

Authentication and Credential Hygiene
Questions measure 2FA use, password storage practices on devices and browsers

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

Facebook and Social Media Hygiene
Questions measure social media connection counts and authentication

Sample "Facebook and Social Media 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

Email and Messaging Hygiene
Questions measure checking of email headers, domain names, typographical errors, spear phishing awareness

Sample "Email and Messaging 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

Transmission Hygiene
Questions measure computer discovery, restricting Bluetooth connections, SSL quality verification

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

"Yourself"

Sample "Yourself" questions:
• 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
Tracking Cyber Hygiene Using the Cyber Hygiene Inventory (CHI)

- **Storage and Device Hygiene**: Questions measure patch management, virus protection, and CPU/network use management.
- **Authentication and Credential Hygiene**: Questions measure 2FA use, password storage practices on devices and browsers.
- **Facebook and Social Media Hygiene**: Questions measure social media connection counts and authentication.
- **Email and Messaging Hygiene**: Questions measure checking of email headers, domain names, typographical errors, spear phishing awareness.
- **Transmission Hygiene**: Questions measure computer discovery, restricting Bluetooth connections, SSL quality verification.

**20-question CHI Inventory:**

- **Score Range:** 0-100

**Ideal Score Cut-off:**

- **80-85 Benchmarking**

**Perceived (or supplied) capacity**

- **0 – 5**
  - No capacity
  - Fully available

**Likely utilization (or behavior)**

- **0 - 5**
  - Not at all likely
  - Extremely likely

**Perceived knowledge**

- **0 - 5**
  - No knowledge
  - Extremely

**Awareness**

- **0 - 5**
  - No awareness
  - Very Aware
CHI Advantages

• Quantitative
• Granularity
• Agnostic
• Cognitive-Behavioral
• Adaptable
Strategic Map for Prioritizing Cyber Hygiene Solutions
1. High Security Significance – Low Enactment difficulty
2. Low Security Significance – Low Enactment difficulty
3. Low Security Significance – High Enactment difficulty
4. High Security Significance – High Enactment difficulty
Assessing users’ K-A-C GAPS
Assessing training effects
Building a culture of cyber hygiene using CHI
• 1. Measurement driven with CHI

• 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

• 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...

• 4. Public health vs. an OPSEC view

https://www.navy.mil/ah_online/opsec/posters.html
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: arun@arunvishwanath.us;
Website: https://arunvishwanath.us