The Secret Weapon to Fight InfoSec FUD

Olivia Stella
August 9, 2019

THE DIANA INITIATIVE
BELIEVE & ACHIEVE—TOGETHER

Google Microsoft Uber

Carnegie Mellon University
Software Engineering Institute

DRAGOS
SAFEGUARDING CIVILIZATION   intel   NORDSTROM   Remediant

THE DIANA INITIATIVE
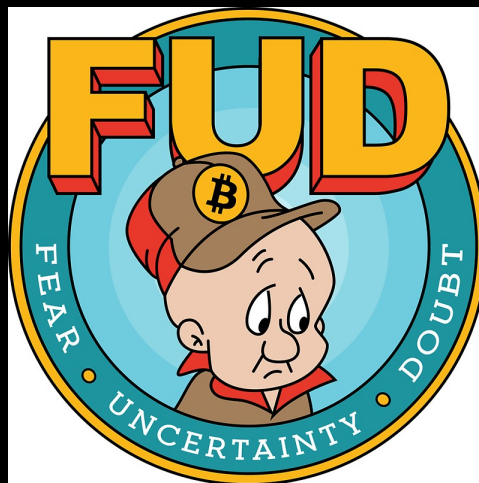BELIEVE & ACHIEVE—TOGETHER

Disclaimer

This presentation is a reflection of my experiences in industry, personal research and a little opinion.

Nothing is endorsed or sponsored by any company that I currently or previously worked for
(because job = money = doing cool events like Diana).

What the FUD?

What the FUD?

FUD & Me

FUD & Me

But Why?

Digital Experience timeline.

1970   1980   1990   1995   2000   2005   2010   2014

But Why?

WHY SECURITY FATIGUE IS SCARIER THAN DATING TAYLOR SWIFT

November 16, 2016

The Internet Age has given us a platform that connects us to our community, financial institutions, social life, retail outlets, and entertainment. The upside of all this connectivity is that it's easier than ever to stay in
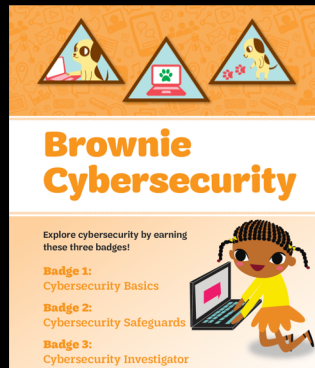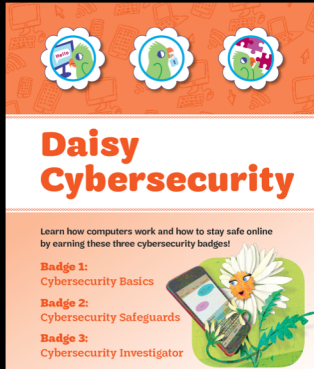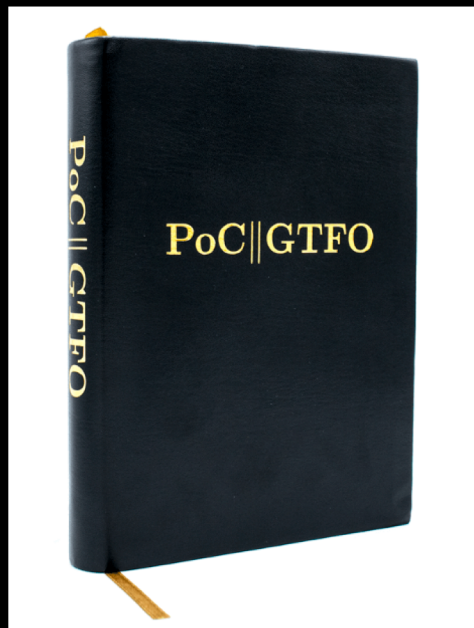
But Why?

How to Fight!

How to Fight!

To All My Corporations (A.K.A Targets)

- You're not a victim
- Provide information timely
- Be transparent
  - The "more you know" = less worried public
- Train teams outside the security department
  - Who makes decision on when & how to release information?
    - Legal, communications, marketing
- Coordinated disclosure & bug bounty programs
  - Know what they are & how they can benefit your company

To All My Researchers

- First, thank you for all that you do!
- Do your homework
  - Cite references
  - Show proof that you tried to contact the target company
- Basics – grammar, spelling, does it make sense?
- Diversify your resources
- Do the best proof of concept you possibly can
  - What are your roadblocks?

To All My Researchers

- Recognize that the people reading your material are not as knowledgeable as you
  - New, stretched info sec teams
  - Management
  - Legal, Privacy, Communication teams

- Coordinated disclosure & bug bounty programs
  - Are not the same – we know that
  - Thoughts? Do we like?

Will you join the fight?

@oliviacurls

References

'FUD - Fear. Uncertainty. Doubt.' Sticker by VectorTony. (n.d.). Retrieved from https://www.redbubble.com/people/vectortony/works/29986049-fud-fear-uncertainty-doubt?grid_pos=3&p=sticker&rbs=a63669b2-4f22-4d97-8e45-0ecca70788ba&ref=shop_grid&searchTerm=FUD

Schofield, J. (2015, November 13). Gene Amdahl obituary. Retrieved from https://www.theguardian.com/technology/2015/nov/13/gene-amdahl

The Corporate Information Security Policy Library: A Minimalist's Perspective. (2018, February 14). Retrieved from https://www.barradvisory.com/corporate-information-security-policy-library-minimalists-perspective/

Prepare for These Information Security Threats in 2018. (n.d.). Retrieved from https://www.business2community.com/cybersecurity/prepare-information-security-threats-2018-01998545

Back-to-School Paperwork. (n.d.). Retrieved from http://www.lisbon.k12.oh.us/News/paperwork20172018#sthash.xAnOahRM.dpbs

Generations X,Y, Z and the Others. (n.d.). Retrieved from http://socialmarketing.org/archives/generations-xy-z-and-the-others/

Pearson, S. (n.d.). Electronics The Digital Revolution. Retrieved from http://www.thepeoplehistory.com/electronics.html

Krebs on Security. (n.d.). Retrieved from https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Reading Room. (n.d.). Retrieved from https://www.sans.org/reading-room/whitepapers/leadership/paper/36697

Peters, D. (2015, February 10). Positive Computing: Technology for wellbeing. Retrieved from https://www.slideshare.net/DorianPeters/slide-share-poscomp15ccare-44528792

Brown, E. A. (2018, July 10). 'Security Fatigue' Can Cause Computer Users to Feel Hopeless and Act Recklessly, New Study Suggests. Retrieved from https://www.nist.gov/news-events/news/2016/10/security-fatigue-can-cause-computer-users-feel-hopeless-and-act-recklessly

Industry insight. (n.d.). Retrieved from https://www.idenhaus.com/why-security-fatigue-is-scarier-than-dating-taylor-swift/

How To Keep Your Kids Motivated in School. (2015, September 30). Retrieved from https://www.oxfordlearning.com/how-to-motivate-kids-in-school/

Gershon, L. (2015, March 10). Don't Give My Kid an Award in School. Retrieved from https://psmag.com/education/dont-give-my-kid-an-award-in-school

Mootz, N. (2018, July 12). Cyberbullying: How Parents and Students Can Understand and Prevent It. Retrieved from https://blogging.com/cyberbullying/

Vinod, -. (2016, September 05). 10 shocking figures which show the cost of cyber security breaches. Retrieved from https://www.cbronline.com/business/10-shocking-figures-which-show-the-true-cost-of-cyber-security-breaches-4888746/

References

Employee Cybersecurity Training. (n.d.). Retrieved from https://planetmagpie.com/employee-cybersecurity-training

Tugend, A. (2012, March 23). Why People Remember Negative Events More Than Positive Ones. Retrieved from https://www.nytimes.com/2012/03/24/your-money/why-people-remember-negative-events-more-than-positive-ones.html

Stafford, T. (2014, July 29). Future - Psychology: Why bad news dominates the headlines. Retrieved from http://www.bbc.com/future/story/20140728-why-is-all-the-news-bad

Online Brand Reputation Management Philippines. (2017, January 18). Retrieved from https://www.gethooked360.com/the-basics-of-online-brand-reputation-management/

Bhasin, H., Bhasinl, H., & Facebook. (2018, June 08). What is Brand Reputation? Importance of Brand Reputation. Retrieved from https://www.marketing91.com/brand-reputation/

PoC||GTFO. (n.d.). Retrieved from https://nostarch.com/gtfo

PoC||GTFO, Volume 2. (n.d.). Retrieved from https://nostarch.com/gtfo2

Palo Alto Networks and GSUSA Collaborate on Cybersecurity Badges - Girl Scouts. (n.d.). Retrieved from https://www.girlscouts.org/en/press-room/press-room/news-releases/2017/palo-alto-networks-girl-scouts-collaborate-cybersecurity-badges.html

(53), S., (37), F., (49), D., (63), S., & (35), C. (n.d.). [EN]Social Engineering - Human weakness - Steemit. Retrieved from https://steemit.com/security/@security101/social-engineering-human-weakness

1. (2018, February 22). Who's responsible for stomping out fake news? – Hacker Noon. Retrieved from https://hackernoon.com/whos-responsible-for-stomping-out-fake-news-39c1e2be81d6?gi=7406fe3c3bfe

Joseph, A., & Nā Leo Literary Review. (2017, January 08). The Real Consequences of Fake News. Retrieved from http://maui.hawaii.edu/hooulu/2017/01/07/the-real-consequences-of-fake-news/

Security researchers: EFF's got your back at this summer's technical conferences. (2017, July 12). Retrieved from https://boingboing.net/2017/07/12/ignorance-isnt-bliss.html

Bajo, G. (2016, December 23). Why information security is not simply a matter of black and white. Retrieved from https://medium.com/team-per-la-trasformazione-digitale/cybersecurity-policy-responsible-disclosure-ethical-hacker-290918f58858

Cairns, C. (2018, February 24). Digital Government Consulting | New bug bounty program solution to secure government digital services. Retrieved from https://skylight.digital/blog/new-bug-bounty-program-solution-to-secure-government-digital-services/