OPSEC

FOR DEVELOPERS

©2017 Steven Killingbeck, MMCP, ACE, CSM, XCMD

Why this talk?
My passion for it, friends & family, developer friends, clients… I kept getting call / emails / texts for advice on anything and everything related to security and privacy!

There is an overwhelming amount of content out there and it changes often!
So I started developing training content and this talk.

So I have been developing a training program to aggregate and translate this content for the average and tech savvy user.
Visit my new site and signup for free content and updates and to be notified when I release my comprehensive training.

All MDC2017 attendees will have free access!
Sign up here for free:
http://opsec.school/opsec4dev/
mdc2017@infosec.school

INTRO

Developers have the keys to the kingdom, and that is why they are high-value targets!
Lets take a whirlwind tour through the privacy and security landscape that every Developer should be familiar with and learn some best practices that you can use today!

WHAT?

What this talk is? This field is really deep, really wide, changing fast!
Many things! (cyber / online security & privacy, personal security & privacy)

What this talk is NOT about (Secure Coding / OWASP / DEVOPSSEC)

*DISCLAIMER

WARNING

Today's presentation is for informational purposes only!

I am not making any **legal / criminal / political / moral / ethical statements, judgements or endorsements** of any kind!

Be safe, Be secure! Using any of these resources, tools or techniques may put you, your computer, your network, your company at risk!

All things change, and often!

Any one know?
Operations security (OPSEC) is a term originating in U.S. military jargon, as a process that identifies critical information to determine if friendly actions can be observed by enemy intelligence, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information. - Wikipedia
https://en.wikipedia.org/wiki/Operations_security

Copyright Holder: Google and appropriates sources as seen in search results

History
Military origin
Modern, alive and well
cool posters, youtube videos

Copyright Holder (Left side panel): Twentieth Century Fox Film Corporation, Monarchy Enterprises B.V. and Regency Entertainment (USA), Inc.
http://www.imdb.com/title/tt0137523/

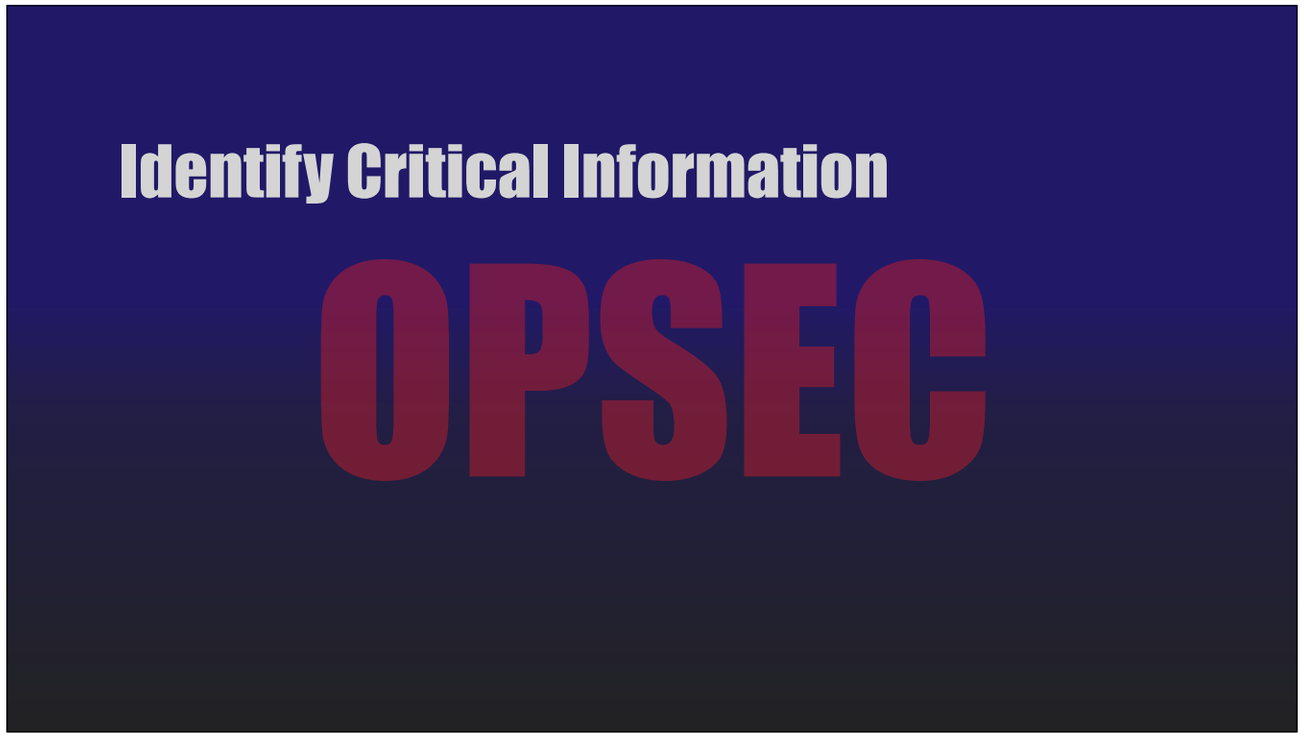
What is this?
This is OPSEC!
They needed OPSEC! Why?
Anyone know what 2nd Rule of Fight Club is?

Don’t talk about your work, projects, code, features, bugs, troubleshooting etc… Don’t share things on social media
OPSEC does not work retroactively!
Once info is out there, it’s impossible to get rid of!
Don’t tell on yourself!
Don’t make it easy for your enemies or competition!

5 Parts of OPSEC

5 Parts of OPSEC

Identify Critical Information
Analyze Threats
Analyze Vulnerabilities
Assess Risks
Apply Countermeasures



Marketing, PR, Timelines, Budgets, Contracts, Policy docs, Asset lists, Org Info, Reports, Transcripts, Infrastructure / Information Architecture, Wireframes, Requirements docs, Security info, Source Code, Algorithms, Certs, Key Pairs, Admin Credentials, API tokens, Browser / Client(cookies, cache, history), Communication / Messaging History, URLs / Hostname / IP#s, Logs, credit cards, PHI, Financial Info, Audio / Video / Screen Recordings, All Media / File types etc…

What else?

HACKERS / Threats, not all hackers are criminals! https://www.youtube.com/watch?v=BzEYP345Rm4

Types:

Script kiddies

Common criminals, Identity Thieves, credit cards, PHI

Exploited Machines, Networks (Malware, BotNets) / AI platform & tools (Defcon AI Combat https://defcon.org/html/defcon-24/dc-24-cgc.html)

Sophisticated criminals, Extortion, Corporate Espionage

Pen testers, Hactivist

LEO / Customs / Border Patrol 100miles

State level actors, 3 letter agencies

Digital Security (hardware, software, networks, information)
Computers
Mobile Devices
Internet / All types of communications
IoT / SCADA, Sensors / Cameras / Microphones / GPS
Access Control

Physical Security (people, places, things, travel)
- Theft, Assault, Robbery, Kidnapping, Murder
- Doors / Windows / Access Control
- Vehicles, Trunks
- Home, Garages, Storage
- Office
- Travel, Public Transit
- Public places, Entertainment, Events

Depends on many factors and the probability and impact of any given incidence!
May very from negligible to complete destruction and mayhem!
This is a difficult yet enlightening process!

Adopt relevant best practices and policies and implement training for Developers regarding Security & Privacy, both physical & digital!

WARNING
Be safe, Be secure! Using any of these resources, tools or techniques
may put you, your computer, your device, your network, your company at risk!
Test all links and downloads with VirusTotal and other tools before using!
All things change, and often!

Some research to get you started!
http://opsec.school/opsec4dev/

Really!

Don’t talk about your work, projects, code, features, bugs, troubleshooting etc… Don’t share things on social media
OPSEC does not work retroactively!
Once info is out there, it’s impossible to get rid of!
Don’t tell on yourself!
Don’t make it easy for your enemies or competition!

THE END

Available for consulting, speaking, training!
Steven Killingbeck, MMCP, ACE, CSM, XCMD
https://www.linkedin.com/in/stevekillingbeck