

Information Security Threat Vectors

Phil Withers, CISSP, CRISC

Who is this guy?

- 26 Year veteran of Naval Communications
 - Networks, Satellite, Terrestrial
- Project Manager Navy Global DMS HD
 - Requirements Analysis, Design, Installation, Operation, Hardening, Reporting, IAVM, ISSO
- CISSP/CRISC

Phil Withers BIO

- A Threat Vector is a path or a tool that a Threat Actor uses to attack the target.
- Threat targets are anything of value to the Threat Actor. It can be a PC, PDA, Ipad, Your online bank account... or you (stealing your identity)

What is a “Threat Vector”?

- Web – Fake sites, Session Hijacking
- Wireless Unsecured Hotspots (Bubba)
- Email – Links, Attachments
- Mobile Devices: Iphone/Ipad/Ithis/Ithat
- Social Networking – Facebook, et al
- Social Engineering (including POTS)
- Malware
- USB (removable) media

Threat Vector Types

- Human (80/20 rule)
 - Malicious
 - External – Script Kiddies, Crackers, Competitors, Organized Crime, Foreign Governments/Entities
 - Internal – Disgruntled Employee, The Curious
 - Ignorant
 - George the WonderDummy
 - The George Scale
- System – Misconfigurations
 - Automated privilege elevations

What is a “Threat Actor”?

- 0 – Alan Turing
- 1 – Tim Berners-Lee, Grace Hopper
- 2 – Linus Torvalds
- 3 – Sysadmins, clueful developers, QA people
- 4 – Your average MCSE bootcamp graduate
- 5 – Your average corporate end user
- 6 – Your average AOL user
- 7 – Furry woodland creatures
- 8 – Algae
- 9 – A bag of hammers
- 10 – George

The Help Desk “George Scale”

- US-CERT lists:
 - National Governments (Israel?)
 - Terrorists (cyber or otherwise)
 - Industrial Spies (France?)
 - Organized Crime
 - “Hacktivists” (Wikileaks)
 - Hackers



What the...!?

- Threat Actors possess a motive and seize upon an opportunity
- Threat Actors exploit vulnerabilities

Threat Actors

- Bragging Rights
- Financial Gain
- Competitive Advantage
- Military Dominance
- Political Advantage
- Economic Advantage
- A New World Order
- Anarchy

What do Threat Actors Want?

- IRAN – Stuxnet Boomerang! (HBGary)
- China – DOD/Financial
- North Korea – Anything
- “Anonymous” – Gov. Walker
- Banks – World Bank, Citigroup
- Stores – TJ MAX CC Database
- Your PC – Botnets
- Your online banking credentials

Who do They Target?

- Edu-ma-cation!
 - Ongoing IA Awareness Program
- Honeytokens
- Defense in Depth (Layers)
- Defense in Breadth (Synergy)
- Framework Built on Industry Standards and Best Practices
- AntiVirus, Firewalls, IDS, IPS, Blackholes
- GRC! (not Governance, Risk and Compliance)

Countermeasures

Countermeasures

Your Personal Computer

- Gibson Research Corp.
 - Free!
 - Shields Up! (Pentester)
 - Free!
 - “Perfect Passwords” – 63 Character Pseudo-Random Generator (one time) for your Wireless Access Point
 - Free!
 - <http://www.grc.com>

Countermeasures Too

Countermeasures

- There's no place like LOCALHOST
- Free!
- Managed Host File Insert
- Free!
- <http://www.mvps.org/winhelp2002/hosts.htm>
- Blocks Ads, Banners, 3rd Party Cookies, 3rd Party Page Counters, Web Bugs, and even most hijackers

127.0.0.1 Is Your Friend
Countermeasures

```
Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.mvps.org/winhelp2002/hosts.txt
Norton Safe Search
Blocking Unwanted Parasites with a... x http://www.mvps...2002/hosts.txt x

# This MVPS HOSTS file is a free download from: #
# http://www.mvps.org/winhelp2002/ #
# #
# Notes: The Operating System does not read the "#" symbol #
# You can create your own notes, after the # symbol #
# This *must* be the first line: 127.0.0.1 localhost #
# #
# ----- Updated: February-18-2011 ----- #
# #
# Entries with comments are all searchable via Google. #
# #
# Disclaimer: this file is free to use for personal use #
# only. Furthermore it is NOT permitted to copy any of the #
# contents or host on any other site without permission or #
# meeting the full criteria of the below license terms. #
# #
# This work is licensed under the Creative Commons #
# Attribution-NonCommercial-ShareAlike License. #
# http://creativecommons.org/licenses/by-nc-sa/3.0/ #

127.0.0.1 localhost

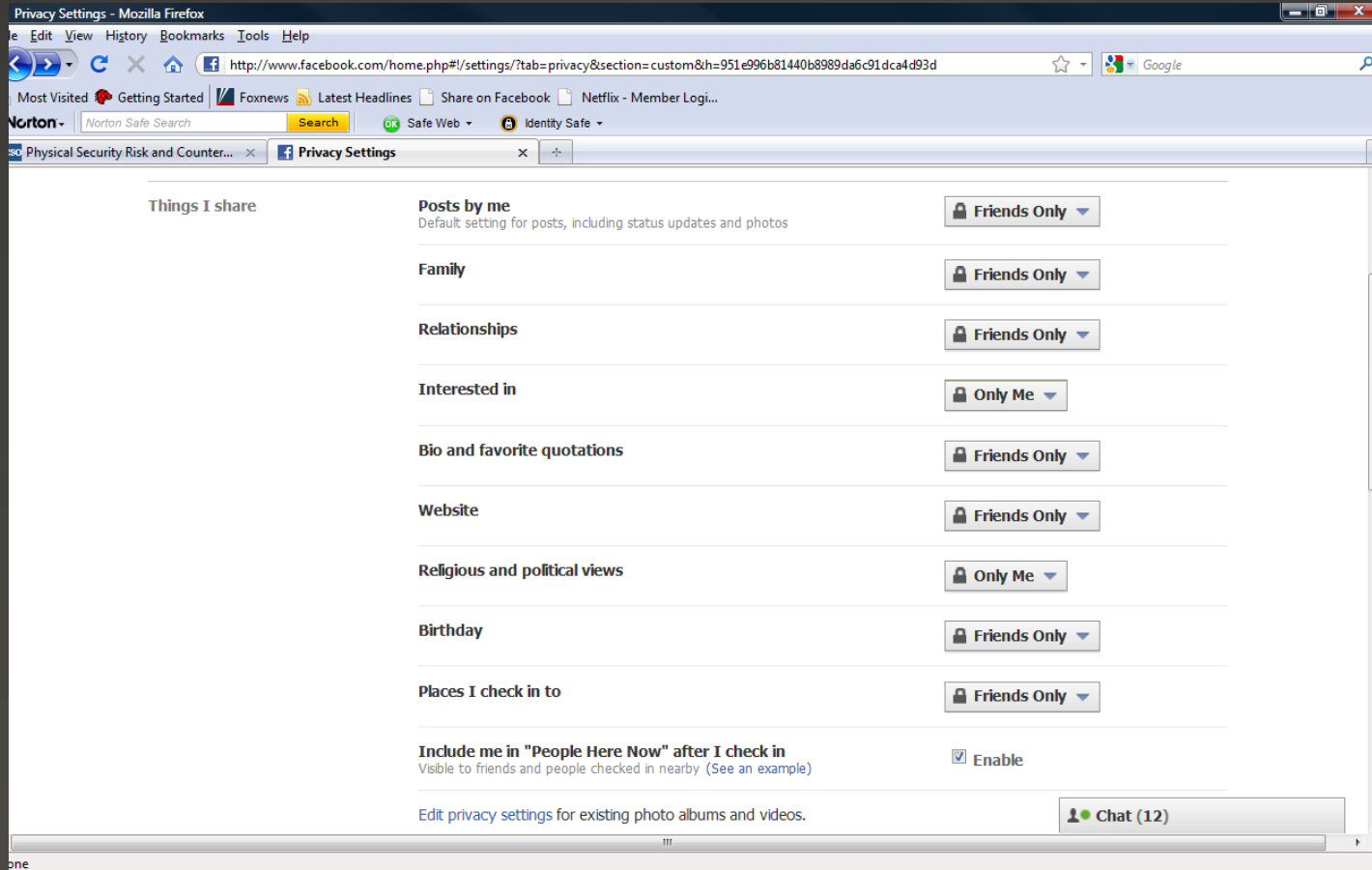
#start of lines added by WinHelp2002
# [Misc A - Z]
127.0.0.1 fr.a2dfp.net
127.0.0.1 m.fr.a2dfp.net
127.0.0.1 ad.a8.net
127.0.0.1 asy.a8ww.net
127.0.0.1 abcstats.com
127.0.0.1 a.abv.bg
127.0.0.1 adserver.abv.bg
127.0.0.1 adv.abv.bg
127.0.0.1 bimg.abv.bg
127.0.0.1 ca.abv.bg
127.0.0.1 www2.a-counter.kiev.ua
127.0.0.1 track.acclaimnetwork.com
127.0.0.1 accuserveadvsystem.com
Done
```

HOSTS file from MVPS.ORG

Countermeasures

Social Media

Let's Use Facebook as an Example



DoD Recommended Facebook Privacy Settings Countermeasures

Things others share

Photos and videos I'm tagged in

Edit Settings

DISABLED!

Can comment on posts

Includes status updates, friends' Wall posts, and photos

Friends Only

Suggest photos of me to friends

When photos look like me, suggest my name

Edit Settings

Friends can post on my Wall

Enable

Can see Wall posts by friends

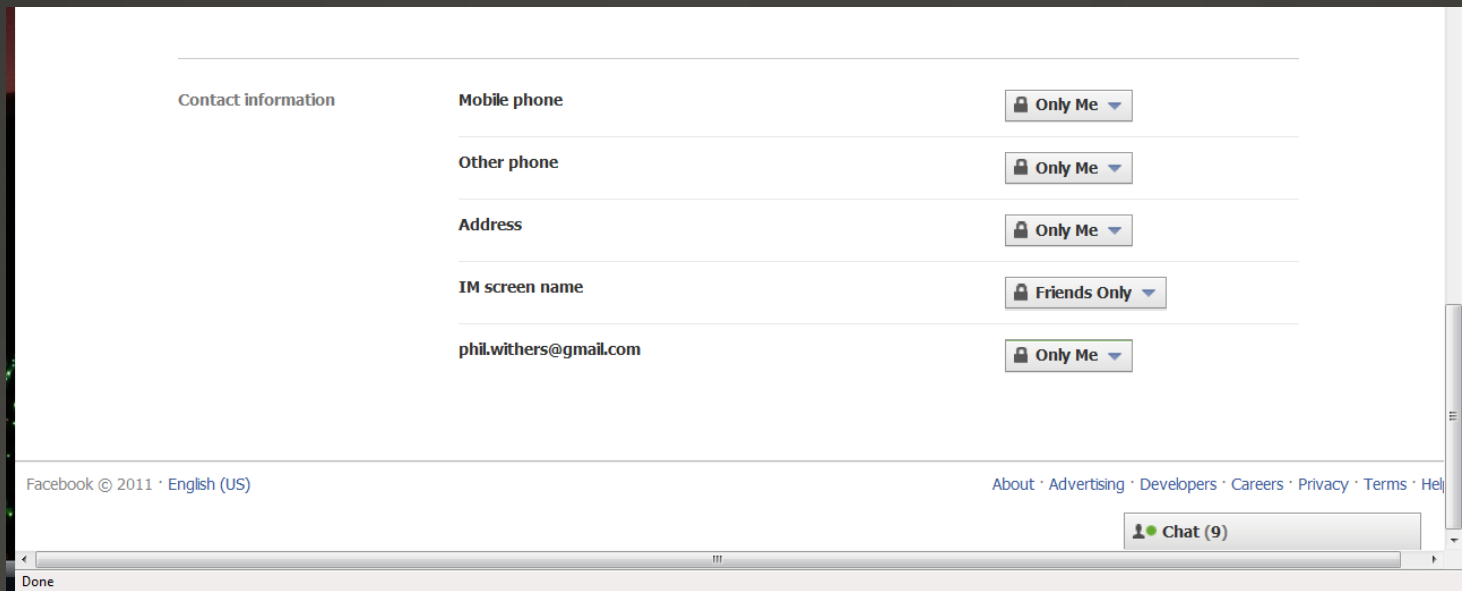
Friends Only

Friends can check me in to Places

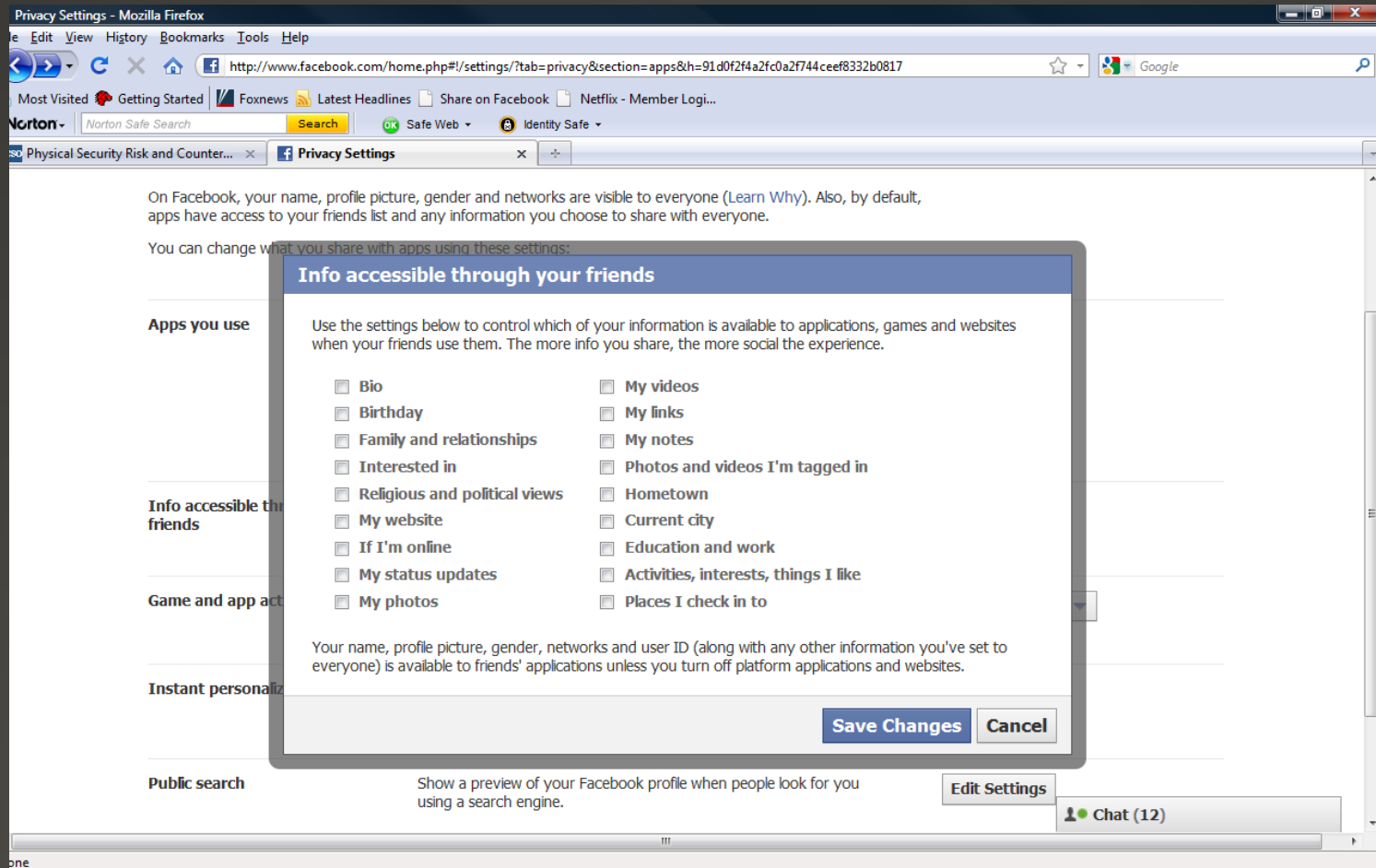
Edit Settings

DoD Recommended Facebook
Settings

Countermeasures



DoD Recommended Facebook Settings Countermeasures



Accessible through friends!!

Turn it off

Countermeasures

- A complete description and rationale for changing the security settings on your FB page can be found at:

<http://slideshare.net/USNavySocialMedia/recommended-facebook-privacy-settings-august-2010>

Get all the settings
Countermeasures

- Threats, Vectors, and Actors are a fact of life
- Know your opponent – get smart
- Reduce your online profile and exposure
- Security through Obscurity

Summary

Questions?

Thanks for Listening!