
Street Smarts for a Virtual World

Lessons In Personal Information Security From
The Military Industrial Complex

T. Stephen Eggleston, DmAt, MSI

Copyright ©2010 by T.S. Eggleston

Dedication a

Introduction..... b

Thank You to..... c

The Author..... d

Threat Assessment: How Vulnerable Are You? 1

 Your Assignment, and You Must Choose to Accept it... _____ 1

 Your Mission is Clear _____ 1

 Good Enough for Government Work _____ 1

 How Do You Classify Your Personal Information? _____ 2

 (Your) Eyes Only: 2

 (PI)Top Secret: 2

 (PI)Secret:..... 2

 (PI)Confidential : 3

 Need-to-Know Basis Only: So you're Still Only 29? 3

 Is It Mission Critical or Mostly Trivial? _____ 3

 What is an Attack? _____ 4

 Potential Threats, Threats and Active Threats _____ 5

Risk Assessment..... 6

 Hardware Cost is Not a Significant Factor _____ 6

 It's all about the Data _____ 7

 What is Your Stored Data and Information Worth to You? 7

 What is Your Stored Data and Information Worth to Others? 7

 The Little Things Aren't Necessarily So Little _____ 7

 Treat Your E-Mail Passwords as (YOUR) EYES ONLY. _____ 8

 Help, I've been Blacklisted! 8

 On the Criminal Side _____ 9

 Reputation is everything _____ 9

 It Doesn't Take a Thief 9

Threat Mitigation 10

Your Own Computer is a Threat to Itself and Your Priceless Information _____ 10

 Heat is Your Hardware’s Number One Enemy 10

 Adopt an Open Door Policy.....10

 A Little Dust Goes a Long Way 10

Hard Drives are Inexpensive and Disposable _____ 11

 Have a Backup Plan and Stick to It 12

 Protect Your Backup Media 12

 Off Premise Backup Storage is Critical..... 12

Hardening the Perimeter..... 13

 Were You Born In A Barn? Please Close the *Back Door* _____ 13

 Mitigate Power Line Threats and Extend the Life of Your Electronics. _____ 13

 120 Volts A.C. is a Myth 13

 Unfiltered Household Electricity Is Dirty! 14

 Practice Safe Computing: Use Power Protection _____ 14

 An Uninterruptable Power Supply is a Mission Critical Investment..... 15

 Sizing Your UPS.....15

 Install Surge and Spike Protection for All Hardware Not On a UPS..... 16

 Avoid Cheap Surge Protectors16

 Check the Joules rating.....17

 Don’t Forget Your Cable TV, Telephone and Network Connections.....17

Defending Against Virtual (Information) Threats: Reducing Vulnerability 18

 Passwords are Not the Weakest Link ... You Are! _____ 18

 Use a Password Manager..... 18

 Choose and Use Strong Passwords..... 19

 A ‘Strong’ Password:.....19

 Networks, Firewalls and Routers _____ 19

 Default Passwords – A Popular Attack Vector 19

 Use the Firewall..... 19

 It’s a Dangerous World Out There: Don’t try this At Home 19

 Keep Your Drivers and Firmware Up-to-date. _____ 21

 Wireless Networks – A Blessing and a Curse _____ 21

 (APSO) – All Possible Security Options: *Company Acronym*..... 21

 MAC Authentication: Protecting You from the Clueless and Opportunistic..... 21

Don't Broadcast Your Network Name (SSID)	22
No one is Immune	23
Don't Create an Attractive Target	24
Good Enough for the Government Encryption	24
Change Your Encryption Key or Password When Necessary	24
<i>Viruses, Worms, Trojans and Malware Delivery Methods</i>	25
The Trojan horse – Beware of Geeks Bearing Gifts _____	25
Worms are designed to spread like Crabgrass _____	25
Infectious Viruses _____	26
All Powerful Invisible Rootkits _____	26
Malicious Macros _____	27
The Cookie Monster _____	27
Spyware _____	28
Adware _____	28
Dangerous Scripts _____	28
Immunize Yourself with Software _____	29
<i>Attacks From Within</i>	31
Separate Logon Accounts for Everyone _____	31
USB Thumb Drives Are Your Friend – Until You Lose Them _____	31
Clean Up and Log Off Before You Go _____	32
The Dog Made the Computer Eat My Homework	32
Don't Get Fraped	32
Identity Theft Lite	33
It's Bedtime – Do You Know Where Your Web Cam Is?	33
Practice Safe Computing: Wear a Lens Cap!	33
Lock the Front Door	34
<i>Warning: Children in the House</i>	35
Time to Have “That Talk” With Your Children _____	35
Good Children Will Do Bad Things _____	35

Sexting - Unintended Consequences 35

Trust – But Verify 38

Children Have Infinite Patience 39

Children are a Lot More Devious than You Think..... 39

Children Compensate for any Lack of Deviousness by Naiveté and Sheer Persistence. 39

Practice Safe Computing: Use Some Common Sense 40

 Even the Good Guys can do Bad Things: Read the Fine Print _____ 40

 Online Contests and Sweepstakes..... 40

 When You Sell Your Home _____ 40

 Photographs don’t have to be Dirty to Be Damaging. _____ 40

 Never Underestimate Your Adversary _____ 41

 The Internet Never Forgets _____ 41

 It’s Not Just Pictures _____ 41

 Stay Away From Flame Wars _____ 42

Recognizing Cyber Threats..... 44

 Does it pass the Smell Test? _____ 44

 Your Bank, Broker or E-Mail Provider Doesn’t Need Your Help..... 45

 Even “Really Big” Companies can get Phished. 46

 Botnets and Zombies, A Club You Don’t Want to Join..... 48

 How Crooks Use Botnets to Smash Their E-Bay Competition 48

 Botnets are used for Blackmail, Cyber Bullying and Vandalism 48

 WHOIS Services: 411 for the Internet..... 48

 They Can Run, but They Can’t Hide 48

 Twitter Will Not Do This..... 50

 We’re Sorry, But the Postal Service Does Not Have Your Package 50

 Drive-By Attacks 51

 The “Classic” Nigerian Money Scam 51

 Making Money At Home 54

 If the F.B.I. Volunteers to help..... 55

Social Engineering and Human Intelligence (HUMINT) 58

 When in Doubt, Check It Out! _____ 58

 If You Hold or Have Ever Held a Security Clearance, You are an Attractive Target! _____ 58

You don't have to be a Spook to attract Spoofer! _____ 58

Proper Situational Awareness Helps Keep You Safe _____ 59

Counterintelligence..... 61

 From Whence Cometh Ye SPAM? 61

 Dissecting a typical E-Mail Header 61

 It Is Possible to Hide on the Internet..... 64

 Reporting Abuse..... 65

 Don't Inadvertently Give Your E-Mail Address to Spammers 65

 Do Not Unsubscribe or Ask to Be Removed from Questionable Lists 66

 Do Not Display Remote Images in your Incoming E-Mail. 66

 Don't Send/Accept Return Receipts 67

 Educate [Discipline] Your Friends and Family. 68

 Don't Ask For Spam 68

Compartmentalize 69

 Proactive E-Mail _____ 69

 Throw Away E-Mail Addresses 69

 Private Business E-Mail..... 69

 Private Personal E-Mail..... 69

 Public / Social E-Mailbox..... 69

 Single Use Mailbox 69

 Spam Catcher Mailbox (Honey Pot) 70

 Message Filters..... 70

 White Lists..... 70

 Everybody Needs an Identity or Two..... 70

 Practice Defensive Finances..... 71

 Limit Your Liability and Exposure 71

 E-Checks 72

 One-Time Credit Card Numbers 72

 PayPal™ 72

 Paperless Statements = Lower Risk 72

 RFID may be Friendly but is it Your Friend? 73

 Smart Cards: Too Smart For Your Own Good?..... 73

 Just Because You are Paranoid Doesn't Mean They are Not Out to Get You..... 73

 Review All Bank and Credit Card Statements As Soon As They Arrive 73

 Get Your Free Annual Credit Review 74

 Proactive Identity Theft Protection 74

Identity Theft Insurance74

Go Google™ Yourself _____ 74

When you're Away From Home..... 75

Laptop Alarm Systems – For More than Your Laptop_____ 75

Bring Power Protection with You _____ 75

Use Online Storage Where Possible and Practical _____ 75

At the Airport _____ 76

Beware Customs and Border Patrol _____ 76

Alternative Telephone Technologies _____ 76

Voice Over I.P 76

Skype..... 76

Vonage 76

Magic Jack 76

Lo-Jack for Computers _____ 76

Visiting Bad Neighborhoods, Phishing in Rough Seas and Sleeping with Pirates..... 77

How to Spot Phishing Holes _____ 77

Are You Swimming with Davey Jones, or Just Testing the Waters? _____ 77

Disasters: Readiness, Response and Recovery..... 78

Damage Control: When an Attack Succeeds _____ 78

Basic Rules: *Nothing Is Secure*; Murphy Was Ahead Of His Time. _____ 78

When the Bugs Bite _____ 78

When Lightning Strikes _____ 78

When the Disk Bites [The Dust] _____ 78

Your Personal Security Plan..... 79

Need to Know Only: Your Personal Information CLASSIFIED _____ 79

Follow Your Own Rules _____ 79

Shred It! _____ 79

Establish and Maintain a Backup Schedule _____	79
Store Mission Critical Information Offsite _____	79
Appoint and Train a Trustee _____	79
Communicate Your Plan _____	79
<i>Your Emergency Tool Kit</i>	80
Mission Critical Tools and Spares _____	80
Basic Hand Tool Kit	80
Spare Power Supply	80
Network Adapter	80
Keyboard	81
Mouse	81
Portable Hard Drive	81
Software Tools and Utilities _____	81
Anti-Malware, Anti-Virus and Ad-Ware Blockers	81
Online Services	82
Free E-Mail Software with Message Filtering	82
System and File Backup	82
Password Management	82
Disk Maintenance Software	83
Military/Industrial Complex Grade Encryption for Commoners	83
Nanny-Ware for Kids and Grownups	83
Snooping on the Spouse and Kids (Be a spy, or just act like one)	83
<i>Online Tools and Resources</i>	84
Companion Website _____	84
[domain to be determined].....	84
Anti-Virus and Security _____	84
Anonymizer Services _____	84
Free Web Based E-Mail Services _____	84
Network Lookup and Tracing _____	84
Online Storage and Collaboration _____	84
Alternative Telephone Technologies _____	84

E-Mail Blacklisting Services and Information _____ 84

Online File Storage and Collaboration _____ 84

Internet Archives and Cached Websites _____ 84

Appendix *i*

List of Top Level Domains and Internet Country Codes _____ i

Security and Intelligence Related Terms and Acronyms _____ i

Potentially Malicious File Types _____ ii

Physical Threat Conditions _____ iv

References..... *v*