14 For 14
14 Things to Know/Try for a Better 2014

by Aaron Grothe
Security+/CISSP/NSA
IAM/NSA IEM
14 for 14?

I did a 12 for 12 talk in 2012. A 13 for 13 talk in 2013. So not being one to challenge tradition here is 14 for 14 in 2014.

Links are at the end of the talk
Slides will be posted at the NEbraskaCERT website http://www.nebraskacert.org/csf
If you have questions/comments please feel free to ask them anytime. You don't have to hold them until the end of the talk.

If there are other resources similar to these that you think might be useful to people please let the group know.

Hopefully this will be an interactive and productive session.
Avast!

- Used to recommend Microsoft Security Essentials to people. I have stopped this for two major reasons
  - Microsoft will not be updating MSE for Windows XP after April 2014
  - Microsoft’s Virus product has really begun to lag lately in detection rates
- Avast! Anti-virus has gotten some pretty good reviews and seems to be working well for most people
- Several other good alternative A/V programs are listed at http://www.thefreecountry.com
The CryptoParty Handbook is a book that was crowd sourced by the CryptoParty over several days. It has tons of good information on items such as

○ Safer Browsing
○ Encrypted E-mail
○ Secure Filesharing
○ And a whole lot more

A very good book with a lot of useful information in it
Whonix

- Whonix is a very interesting Linux distribution. Actually it is two.
- The first part is the gateway. This is the part that makes all connections to the outside world.
- The second part is the workstation. All traffic from this instance is routed to the gateway via an isolated network.
- This way all traffic coming from the workstation is sent through tor reducing the odds of leakage.
- Very cool little project and worth an install if you're feeling paranoid.
- Quick reminder tor is/can be slow.
Pogoplug SafePlug

- This is a small ARM based solution that is supposed to make it easy for ANYONE to use TOR
- I have ordered one of these and after doing some testing on it I’m going to have my parents give it a shot.
- It says it doesn’t require any software to be installed on your system
- You browse to the device (safeplug) and it is supposed to have a place where you type in the URL you want to go to
- Sounds interesting, not a lot of technical detail I’ve found yet
Malwarebytes for Android

Appears to be a good malware scanner for android
Doesn't appear to be too heavy a scanner and is worthwhile

People are finding ways around the automatic checks in stores such as Google's and Amazon's
Many stores are now starting to track your devices MAC addresses to be able to correlate who you are what you shop for and combined with the cameras and checkout information what you look like.

AVG PrivacyFix is an app that allows you to set certain Wifi hotspots as the areas you’ll see.

Some stores tracking this are Dollar General, Walmart, etc. More are going to be doing this in the future.
Wifi Pineapple costs $100.00 and is worth it

Quite simply if you want to scare the beejeezus out of someone about wifi this is the tool

Almost all of us have open wifi hotspots we use. E.g. Crane’s coffee etc. What our devices do is broadcast these names to see if they are there. What the wifi pineapple does is say “yep, I’m crane coffee” and begins a conversation. Most devices won’t even pop up a warning about this
Turn On Do Not Track

The EFF (Electronic Frontier Foundation) has a good page that tells you how to turn do not track on for various browsers.

The effectiveness of this is open to debate. The Better Business Bureau for example has said it will not penalize companies that do not honor this.

Still it is a good thing to set :-)


EasySec

Quick Plugin for Chrome that does several things

#1. Enforces https access where possible. I prefer https everywhere for this personally

#2. Link expansion - replaces links like bit.ly and so on with their fully expanded equivalents

#3. Typo squatting prevention. If you pass over a link such as idnesy.com instead of disney.com it will give a warning. Works for top 100 websites.
If you are running the stock firmware that came with your router you should consider upgrading your router to dd-wrt or one of the other open firmware for routers such as openwrt or tomato.

DD-WRT and the other firmwares tend to have more features enabled by default and have been reviewed by quite a few people.
Securely Wiping an SSD

Regular Utilities such as DBAN are of limited use with SSDs. SSDs do provide a set of tools to securely wipe them.

This guide lays out how to do this under Linux.

Can be done using a LiveCD, such as Knoppix or Gparted.
BoxCryptor

- BoxCryptor is an application that encrypts your data before it hits Dropbox.
- So even if Dropbox is compromised, your data is still secure... hopefully.
- This service has free and paid plans. Free plans are for non-commercial use.
- New version works with Microsoft’s Skydrive, Google storage, and so on.
EPIC.org

EPIC (Electronic Privacy Information Council) is a group that is committed to protecting personal privacy in the internet age.

They do this through a lot of Freedom of Information Act requests. One of their latest of these is about the amount of radiation that body scanners at airports expose people to.

Disclaimer: I am a member of EPIC and support about 90+% of their agenda.
EFF.org

Electronic Frontier Foundation is another group concerned about privacy and freedom in the internet age.

They do a lot of legal cases such as defending people against certain MPAA suits, Net Neutrality, Freedom of Information Act requests and so on.

Also are authors of some nice software such as httpseverywhere.

Disclaimer: I’m also a member of EFF and agree with most of their actions as well.
Q & A

Questions???
Links

Slide #1 - Avast!

Avast AntiVirus - http://www.avast.com

Slide #2 - CryptoParty Handbook

https://www.cryptoparty.in/documentation/handbook
Links

Slide #3 - Whonix
https://www.whonix.org

Slide #4 - Pogoplug SafePlug
https://pogoplug.com/safeplug
Slide #5 - Malwarebyte Anti-Malware

Slide #6 - AVG PrivacyFix
Links

Slide #7 - Wifi Pineapple
http://hakshop.myshopify.com/products/wifi-pineapple

Slide #8 - Turning on Do Not Track
https://www.eff.org/deeplinks/2012/06/how-turn-do-not-track-your-browser
Links

Slide #9 - Easysec
Search for easysec in chrome store

Slide #10 - DD-WRT
http://www.dd-wrt.com

Tomato Firmware
http://www.polarcloud.com/tomato

openwrt
https://openwrt.org/
Links

Slide #11 - How to securely delete an SSD drive
https://ata.wiki.kernel.org/index.php/ATA_Secure_Erase

Slide #12 - BoxCryptor
https://www.boxcryptor.com/
Links (Last)

Slide #13 - EPIC - Electronic Privacy
https://www.epic.org

Slide #14 - EFF - Electronic Frontier Foundation
https://www.eff.org