Cyber Security for Perverts

Presented at Black Rose Tuesday Education 10/22/13

By: Alex McGeorge, available at http://fapsec.net/csfp/index.html

Introduction

This document provides a quick and *simple* checklist for home users to improve their overall security posture.

Windows based computers

Done?	Priority	Description
	HIGH	Start > Programs > Windows Update , apply them all
	HIGH	Use some type of anti-virus, ensure it is up to date
	HIGH	Use the proper network profile (Public/Private/Business)
	MED	Windows 7 and 8 deliver **significant** security improvements, upgrade to 7

Mac based computers

Done?	Priority	Description
	HIGH	Run software update
	HIGH	Enable the OSX Firewall
	INFO	Chill out Steve Jobs Jr., OSX has a ton of security problems too

Smart phones

Done?	Priority	Description
	HIGH	Allow phone to apply any OS and app updates. Review app permissions
	HIGH	Only turn on wireless selectively, do not join unknown wireless networks
	MED	Consider uninstalling banking applications

Wireless Routers

Done?	Priority	Description
	HIGH	Use WPA2 based wireless authentication schema
	HIGH	Disable WEP and WPS
	HIGH	Check manufacturer websites for firmware updates for this model
	HIGH	Change router default administrative password
	MED	Create new wireless keys every 6 months

Browsers

Done?	Priority	Description
	HIGH	Are you using the latest support version of your browser?
	HIGH	Use a browser that supports HTTPS Everywhere (Firefox / Chrome)
	HIGH	Install a plugin which allows you selectively enable Flash
	HIGH	Uninstall Java, ensure Adobe Acrobat is at version XI if you need it at all
	MED	Consider using the following browser plugins for privacy: Ghostery, DoNotTrackMe, NoScript/NotScript, AdBlock

Laptops

Done?	Priority	Description
	HIGH	Realize that WEP/WPA2 does not protect your traffic against other people with the key
	HIGH	Use a VPN service when you take your laptop off a trusted network
	HIGH	Make use of bitlocker or other full disk encryption technology

General

Done?	Priority	Description
	HIGH	Use a significantly different password for each website you use
	HIGH	Use TrueCrypt to create an encrypted container on a USB drive for sensitive files. Unplug when not in use.
	HIGH	Use password safe or keepass for secure password storage
	MED	Don't use sites/services that ask for your password to *other* sites/services
	MED	Don't use a site that offers to store all your passwords

Informational

Done?	Priority	Description
	INFO	Need to watch porn but on your business laptop? Use a Linux Live CD
	INFO	Need to wipe a computer before you donate it? Use DBAN. Unless it's an SSD, then wipe it and smash it
	INFO	Don't receive personal email at work, don't visit personal sites at work
	INFO	You can do backups yourself by copying your sensitive data to an external HD and keeping it in a fire safe, don't forget to encrypt the drive!
	INFO	Before you take your computer in for service, take out the HD