Windows 8 Survival Guide

Introduction

Below are some of the terms covered in this document. Also, you should use this document in conjunction with my web site at www.edwardns.com which has more details on this subject. Just remember, if you don't take necessary precautions, **everything will probably work fine until it doesn't.**

- Recovery Drive - you will need this bootable USB drive if your PC is unable to boot and you want to Refresh it or Reset it or use System Restore. Instructions for creating the drive can be found here. You may never need this if you backup your PC using a disk imaging program.
- Password Reset disc – a USB or CD that is used to recover your password for a Local account only. If you have a Microsoft account you do not have the option to create this. With a Microsoft account there is a different way to reset your password by going to https://account.live.com/resetpassword.aspx
- Backup image – a file that is created by disk imaging software that is an exact replica or image of your hard drive.
- System Restore – lets you revert to a previous state by undoing the last major change. See the info here.
- System Refresh - This option allows you to keep all your personal files and purchased Apps from the Windows Store, whilst removing all downloaded and installed programs. See info here.
- System Reset – this basically restores your PC to the state that it was in when you bought it.
- File History
- Bootable recovery media – these are USB or CD discs that allow you to boot your PC to restore an image that was created earlier. The method to create the media depends on the software you used to create the image. More info later in the document.

What are the first things you should do on your new PC or anytime for that matter?

- Create a password reset disc if you have a Local account.
- Create a Windows 8 Recovery Drive – see the link above.

Next, how do you prepare for disaster?

- Backup your data using one of the following methods
  - Use Carbonite for $60 per year
  - Use Windows 8 File History
  - Use a 3rd party program such as Genie Backup Home 9.0 available here
  - Use OneDrive, 51GB free. I wouldn't totally depend on this but it's a start
- Turn on and learn how to use System Restore
- Learn how to use the Windows 8 Refresh or Reset

If you can't boot your PC you have to perform one of the following:

- Use the Windows 8 Recovery Drive which allows you to perform the tasks below:
  - System Restore
  - System Refresh
  - System Reset

- Use the Recovery media created by one of the programs listed in the table below to restore a disk image previously created by the same program

Programs for creating disk backup images					
Program	**Web Site**	**Cost**	**Works with Windows 8 Secure Boot**	**Comments**	**My Choice in order**
Macrium Reflect Free	Click here	Free	Yes	Relatively straightforward	1
Paragon Backup 2014 Free	Click here	Free	No	Need to tweak the Windows 8 BIOS for it to boot	4
Acronis True Image 2015	Click here	$49.99	Yes	Has more features than you need but is a good program	3
Windows 8 built-in disk imaging	N/A	N/A	Only if you create a Windows 8 Recovery drive	Overly simple. No options such as placing backup file in a folder. Takes longer to run than other solutions. But it works.	2

How to change the BIOS settings

If you can boot your PC normally you can do the following

1. Open the Charms bar
2. Click the Power button
3. Hold the Shift key while clicking Restart
4. Click "Troubleshoot" and then "Advanced Options"
5. Click "UEFI Firmware Settings" to enter the BIOS

If you can't boot your PC you will have to know which key to press during the boot process. Sometimes it will flash on the screen and say "Press the F2" key to enter Setup. If you don't know which key to press you can search the Internet or call the manufacturer. It is usually one of the following:
ESC, Del, F2, F10 or F12. You can't do any harm by guessing. Read more here.

If you want to boot Windows 8 from a USB drive or Optical disc you may have to disable Secure Boot in the BIOS. See the information here and here.

Important note – the password reset disc will not recover your previous password but it will allow you to reset it to a new one.

Various scenarios and possible solutions

1. Browser gets seriously compromised
   a. Use a tool like Adware Cleaner available here or Adware Removal from here

b. Try resetting your browser. For Firefox see the info [here](#) and for IE see the info [here](#) and for Google Chrome see the info [here](#).
2. PC corrupted by malware but can't be easily cleaned by Malwarebytes or other program
   a. Restore a previous image if you created a backup image
   b. Try System Restore (not always successful)
   c. Try System Refresh first, then System Reset if Refresh doesn't fix everything
3. Note – you can always uninstall Firefox or Chrome and reinstall them if they get corrupted but you can't do this with Internet Explorer.

Using an account without Administrator privileges for increased security

Background

A new report confirms what many security professionals have long presumed: Removing administrator rights from everyday Windows user accounts slows down or stops almost all critical malware infections.

"Ninety-two percent of all vulnerabilities reported by Microsoft with a critical severity rating can be mitigated by removing admin rights," states the enterprise-security firm Avecto, of Manchester, England, in a new report.

"Removing admin rights would mitigate 96 percent of critical vulnerabilities affecting Windows operating systems, 91 percent of critical vulnerabilities affecting Microsoft Office and 100 percent of vulnerabilities in Internet Explorer," Avecto said.

That may sounds complicated, but it's not. There are two kinds of user accounts in Windows machines: Administrator accounts, which can add, alter or remove software and change system-wide settings, and standard accounts, which can't do any of that.

Putting it into practice

- Add a new "Local" account with limited rights called a Standard Account in Windows 8. See instructions for adding a new **Local** account [here](#).
- Log out of your Administrator Account and into your new Standard Account for everyday activities.
- To make changes to your PC including installing programs, log back into your Administrator Account.
- Don't forget to log into your Standard Account before going on the Internet.

Summary

Try to do as many of these items as you feel comfortable with. Some of the tools may not be for you but at least be aware of them. I will explain all of these in class.
- Use unique passwords and keep them safe. Use a password manager.
- Run firewalls including a Router (which is a hardware firewall). See the info [here](#).
- Run anti-malware software
- Use a good antivirus program. Windows Defender is built into Windows 8 and is not the best program for this. AVG Free and Avira Free are better.
- Keep browsers up to date
- Avoid Internet Explorer
- Avoid Java
- Backup your data frequently including email addresses
- Keep Windows up to date

- Make a backup image of your PC so you can recover from a system breach or infection
- Set up and use a limited-rights account
- Beware of scams
- Don't click any email links unless you solicited them
- Read "Housekeeping tips for Web browsers" here and read the info here.
- Keep a portable browser handy. Get one here.
- Use 2-step verification where available (see Yubikey here which works with LastPass). Note – this can be set up so that the YubiKey is only required on PCs other than your desktop or laptop.
- If you use a password manager visit the help or their manual.
- Take a look at OpenDNS here.

Cleaning up an infected PC

Here are the options in order of difficulty with the easiest first:

Method	Time	Notes	Preparation	Windows
Restore a previously created disk image.	20 to 40 minutes	This is a proactive action. You will have to restore some data (data created between the time the last backup image was created and the present time)	Previously created a backup image	Windows 7 or 8
System Restore	30 to 40 minutes	Frequently does not work	Make sure System Restore is enabled	Windows 7 or 8
Run anti-malware programs	Could take up to an hour or more	Frequently does not work	None	Windows 7 or 8
System Refresh	Several hours	Must reinstall all programs	Have disks for all of your programs	Windows 8
System Reset	Several hours at least or maybe several days.	Time depends on how much software you need to reinstall and data also.	Backup all data and have disks for all of your programs	Windows 8
Use PC recovery media or hidden partition to restore PC to factory conditions	Several hours at least or maybe several days.	Time depends on how much software you need to reinstall. I've seen cases where this will not work.	Backup all data and have disks for all of your programs	Windows 7 or 8

If none of these options are successful you need to purchase a new PC.

Final thoughts

If you make a backup image of your PC you can forget about using System Restore, System Refresh and System Reset. When you get in trouble, just restore your most recent image.

Remember, that if you restore an image that is several months old, any new data that was created within that period will be lost unless you backup your data regularly.

Restoring an image takes 20 to 40 minutes. Cleaning up an infected PC can take at least several hours and may not even be possible depending on the circumstances.

Best practices

Here's the steps:
1. Create a backup image
2. Backup data regularly
3. Get into trouble
4. Restore image
5. Restore data
6. You're back on the air again in quick time