

Windows 10 Tips and Tricks & A Few Other Topics

Frank May

SIRS Computer Group

May 18, 2017



Agenda

- 1.Ransomware Issue
- 2.Some Tips and Tricks
- 3.Utilizing Two Monitors
- 4.Why You Don't Need 27 Different Passwords
- 5.Windows "Creator" Update



Ransomware Issue

Advice has been to not pay the ransom – but, rather, reconstruct your system

- Use Newer Operating Systems – Windows 10
- Get rid of XP or at least install the available patch from MS
- Installing software patches – Microsoft and other software vendors
- Backing up your files – I use Crashplan
- Move files to cloud services
- Open only attachments or click on links that you know.
- Use antivirus program – Windows Defender is a free option.



Five Tasks to Setup Windows

https://www.youtube.com/watch?v=BT1Mz_TRXvQ#t=32.009771 - Five tasks to setup Win 10

- Customize Start Menu
- Customize Start Bar and Action Center
- Customize Microsoft Edge
- Pin Important Things
- Use Applications
 - Loaded apps and Application Store
 - Snap Applications
 - Set Default Applications



10 Tips and Tricks

<https://www.youtube.com/watch?v=YNvmq5qDHFY#t=0.911935> 10 tips and tricks

- Secret Start Menu
- Storage Manager
- “God Mode” Menu
- Snipping Tool
- Sticky Notes
- Windows Remote Assistant
- Problem Steps Reporter
- Voice Recorder
- Malicious Software Removal Tool
- Windows Memory Diagnostic Program



15 Tips and Tricks

<https://www.youtube.com/watch?v=WXpZD5uYfOo> 15 tips

- Right Click and Drag
- Text Select Options
- Chrome In-Site Query
- Chrome Bring Back Tab
- Loop YouTube Video
- Change Website Content
- Win + Tab
- Easy Command Line Prompt
- How To Get Your PC Fixed
- Avoid Installation Bloatware
- Gmail Undo Send
- Modify Gmail Addresses
- Bypass Update and Install
- Tab In Text Field
- "Off" Button



Utilizing Two Monitors

The screenshot displays a dual-monitor workstation. The left monitor shows a Microsoft PowerPoint presentation titled "Windows 10 Tips and Tricks 05182017.pptx". The current slide is titled "15 Tips and Tricks" and contains a list of 15 tips, with a red box highlighting the title. A text box on the slide contains a YouTube link: <https://www.youtube.com/watch?v=WXpZD5uYfOo> 15 tips. The right monitor shows a Microsoft Outlook inbox. The selected email is from Neil Schmidt, titled "Protecting From Ransomware". The email content discusses ransomware attacks and provides advice on protection, including a link to "Take a hard look at your computer's operating system".

15 Tips and Tricks

- Right Click and Drag
- Text Select Options
- Chrome In-Site Query
- Chrome Bring Back Tab
- Loop YouTube Video
- Change Website Content
- Win + Tab
- Easy Command Line Prompt
- How To Get Your PC Fixed
- Avoid Installation Bloatware
- Gmail Undo Send
- Modify Gmail Addresses
- Bypass Update and Install
- Tab In Text Field
- "Off" Button

<https://www.youtube.com/watch?v=WXpZD5uYfOo> 15 tips

Protecting From Ransomware

There has been a tremendous amount of press on the recent ransomware attacks and I suspect there will be a lot of interest in the topic at Thursday's CAT meeting. The following WSJ article does a good job briefly summarizing how to protect yourself from ransomware. One recommendation that I hadn't seen elsewhere is storing files in the cloud.

How to Protect Yourself From Ransomware

Security pros recommend opting for recent operating systems, paying attention to software patches, and backing up your files. The past few days have alerted the wider world to the dangers of ransomware, and it has been an ugly awakening for victims including doctors at the U.K.'s National Health Service, employees at Russia's Interior Ministry, and staffers at some FedEx Corp. offices. Ransomware, which has been on the rise for the past few years, encrypts files on a computer so that they can't be read and the device becomes essentially useless. It gets its name because the culprits post messages on victims' computers demanding payment, generally in the digital currency bitcoin, to undo the encryption (a promise they don't always fulfill). The good news is that there are effective measures to protect against the software in Friday's attack, generally called WannaCry, and other Ransomware. Here is what security pros recommend:

Take a hard look at your computer's operating system

Still running Windows XP because it is good enough to get your web browsing and emailing jobs done? Then the recent WannaCry headlines are warning sirens. The first thing to do is download the emergency Windows XP patch Microsoft Corp. made available here. That will protect you from the attack that WannaCry uses to spread. But it is important to know that Microsoft is no longer providing regular software updates to Windows XP, which means there likely are many other unpatched flaws on your system that could cause problems later. The only way to address that is to upgrade your operating system (which could require buying new computers). If you are running Windows 10, you are protected from WannaCry.

Update, always

If you see those Windows Update messages on your PC, don't put things off: Update your computer. Microsoft issued the software that protects against the WannaCry worm on March 14, which means some of those who have been infected merely needed to follow instructions and they would have been shielded. While WannaCry spreads via a Windows bug, other forms of malicious software can spread through flaws in other software on your computer, such as Adobe Inc.'s Flash and Oracle Corp.'s Java. So the next time you see a prompt for a software update from those programs or others on your system, take the time to install it. It helps.





Configure the Displays

This screenshot shows the 'Customize your display' settings page in Windows. The left sidebar lists various system settings, with 'Display' selected. The main area shows a diagram of two displays, labeled '1' and '2'. Below the diagram are options to 'Identify', 'Detect', or 'Connect to a wireless display'. A slider for text size is set to 100%. The 'Orientation' is set to 'Landscape'. Under 'Multiple displays', the 'Extend these displays' option is selected. There is a checkbox for 'Make this my main display' which is checked. 'Apply' and 'Cancel' buttons are at the bottom. A link for 'Advanced display settings' is at the very bottom.

This screenshot shows the 'Advanced display settings' page. The 'Multiple displays' dropdown is set to 'Extend these displays'. The 'Resolution' is set to '1920 x 1080 (Recommended)'. There are 'Apply' and 'Cancel' buttons. Under 'Color settings', the 'Color profile' is set to 'HP w2338h LCD Monitor'. There are links for 'Color management' and 'Color calibration'. Under 'Related settings', there are links for 'ClearType text', 'Advanced sizing of text and other items', and 'Display adapter properties'.

6 Windows Tips and Tricks

<https://www.youtube.com/watch?v=41Luqd5XJok> 6 tips and tricks

Mail Notifications

Start Menu Customization

Jump Lists

Cortana Voice

Use Cortana to Find Apps

Edge Browser



10 Tips to Make Your Computer Faster

<https://www.youtube.com/watch?v=fd6oYUVrcvk>

- Clear out Startup Programs
- Clear out Startup Services
- Uninstall unused programs
- Scanning for viruses
- Disabling Windows animation
- Keep Everything up to date
- Check power settings
- Check drive health
- Check Windows file integrity
- Check for memory errors
- Reformat and reinstall Windows
- Install SSD
- More RAM



Why You Don't Need 27 Different Passwords

Current State of Affairs

Fifty percent of all breaches in the past year leveraged either stolen or weak passwords

Average person has 27 discrete online logins

Good Password Hygiene

Different password for each account

Use Long Passwords

Special characters, Numbers, Capital Letters

Change Passwords Every Couple of Months

Do not:

Share Passwords Via Text, Email or Chat

Use Easily Identifiable Information Such as Birthday, Child Name

Use an Incredibly Generic Password Such as "12345"



Why You Don't Need 27 Different Passwords

Unmanageable!!

- 37 Percent Forget a Password Once a Week
- Security Fatigue
- How Do You Remember Passwords?
- Do You Use the Same Password For Multiple Logins?

So What To Do?

GET A PASSWORD MANAGER!



Why You Don't Need 27 Different Passwords

“For those who might not be familiar, password managers assist in generating, storing, and retrieving passwords from an encrypted database. They typically require that users create and remember one master password to rule them all. One master password to find them. One master password to bring them all, and in the darkness bind them.”

While most password managers have similar setups, they secure passwords in different ways.

- Web-based password managers store your passwords encrypted in the cloud.
- Some are built into browsers, such as Safari, Firefox, and Chrome.
- Others may store your passwords locally in an encrypted file on your computer, tablet, or phone.



But aren't I just asking to be hacked by storing everything in one place?

While some folks might be wary of using a single point of access for all their sites, remember that password managers still use your individual passwords to log in to your accounts. Those passwords are locked in an encrypted database, which is way more secure than a post-it on your office desk or a faulty memory. Ask yourself this: is it safer to store all your money in one bank or to hide it in piles underneath several mattresses?

As for fear of password managers being breached—sure, it's possible. In fact, it's already happened, as was the case in 2015 when [LastPass was breached](#). However, even though cybercriminals got their hands on some email addresses, they were unable to crack master passwords. This is because master passwords are protected with military-grade security, hidden behind thousands of rounds of hashing, or algorithms that convert strings of text into longer strings of text. So far, no reputable password manager has leaked consumer master passwords (that we know of).



So which password manager should I use?



The following password managers come highly recommended by our staff and tech reviewers from *The New York Times*, *Lifehacker*, and *PCMag*:

[1Password](#)

[LastPass](#)

[Dashlane](#)

[Sticky Password](#)

Also Roboform

If you don't trust third-party apps with all of your personal information, you can try an open-source password manager such as [KeePassX](#), though it requires a fair bit of technical know-how to set up.

<https://blog.malwarebytes.com/101/2017/05/dont-need-27-different-passwords/>

Windows Creator Update

<https://www.youtube.com/watch?v=EX7j8tj22PA>

- Auto Update Changes
- Start Menu Folders
- Night Light Mode
- Storage Sense
- Game Features
- Paint 3D
- Mixed Reality Portal
- Better Privacy Settings
- Troubleshooters
- Dynamic Lock

