in this issue >>> V.1.16

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

current topics >>>

In the News:

- How to Enable Encryption in Facebook Messenger

  - Lifehacker Security
- Batches of Amazon Passwords Posted Online; Change Yours Now!

  - Naked Security
- Russia Behind Hack to Disrupt U.S. Elections

  - Ars Technica
- More Than 400 Malicious Apps Infiltrate Google Play Store

  - Ars Technica

OOSU10

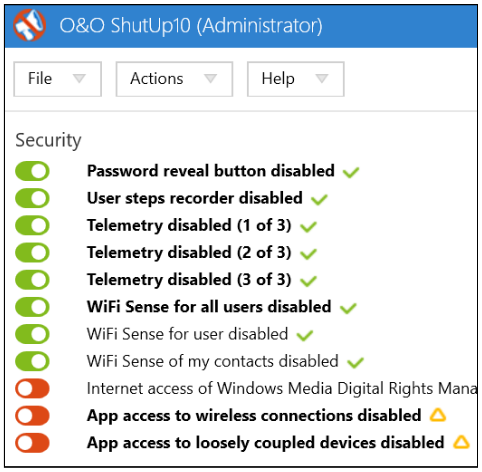
Easy OS Hardening for WinX

We often say that there is no single, software-based solution to "security". There is one new product that comes as close to this as anything we have seen. It is called "O&O ShutUp10" from O&O Software (we call it OOSU10 for short). This is a free product for Windows 10 that attempts to correct many of the privacy and security issues that are built into Windows 10. These issues stem largely from two desires: to give the user the most convenient computer experience possible, and to collect as much data from the user as possible.

OOSU10 is a portable application, meaning you do not have to install it. Simply double-click the .exe file and it will run. The interface is incredibly simple: it shows all of the settings that pertain to security and privacy. Each setting has a simple "on/off" toggle. Additionally, each setting is accompanied by a green check mark, orange triangle, or red exclamation point. These mean settings are recommended, somewhat recommended, or not recommended, respectively.

Clicking the "Actions" tab at the top of the interface brings up some other helpful options. The second of these is "Apply all recommended and limited recommended settings". OOSU10's "limited recommended" settings are those settings for which there is no perfect option. Selecting this will change all of Windows 10's settings to the best possible security and privacy configurations. This makes it incredibly fast and convenient to setup a Windows 10 machine without having to spend too much time thinking about each and every setting.

O&O ShutUp10 is free and available for download at https://www.oo-software.com/en/shutup10. You should run OOSU10 now, and immediately after each time you update your Windows 10 operating system.



Security

- Password reveal button disabled ✓
- User steps recorder disabled ✓
- Telemetry disabled (1 of 3) ✓
- Telemetry disabled (2 of 3) ✓
- Telemetry disabled (3 of 3) ✓
- WiFi Sense for all users disabled ✓
- WiFi Sense for user disabled ✓
- WiFi Sense of my contacts disabled ✓
- Internet access of Windows Media Digital Rights Mana
- App access to wireless connections disabled ⚠
- App access to loosely coupled devices disabled ⚠

set the stage >>>

Email Masking: Blur

In the last issue we talked about email masking as a concept and about 33Mail specifically. We pointed out some downsides to 33Mail, the worst of which is that all your 33Mail addresses are linked by their common, unique domain. Our favorite email masking service doesn't have the same potential vulnerability.

Blur's email masking service requires that you have an account. When you log in to go Masked Email and create a new address. It will look something like this: **cf654abe@opayq.com**. Like other masking services it will forward mail to your primary inbox.

Pros: The "@opayq.com" is not as distinctive as a custom 33Mail domain. Also, 33Mail domains can be made up not only by you, but by spammers, too. With Blur this is not the case—each email address is unique and cannot be created "on the fly". Blur accounts are also much more secure than 33Mail accounts. Blur allows passwords as long as 100 characters (the longest we have tried). Accounts can also be secured with two-factor authentication.

Cons: Using the "@opayq.com" domain positively identifies you as a Blur user which puts you in a relatively small subset of security– and privacy-focused users. This isn't ideal but you are still only one of millions of Blur users. Another downside is that you have to log into Blur to create a new email address. This is alleviated somewhat by mobile apps for **iOS** and **Android** devices and browser extensions for Chrome and Firefox.

If you are a regular reader of the Update you are no stranger to Blur. In addition to offering email masking service, Blur also offers masked phone numbers, masked credit cards, and a built-in password manager. Though Masked Cards and Masked Phones require a premium account, Masked Emails are available with a free account. Go to **https://abine.com/index.html** and set one up today.

The easy button >>>

Signal Disappearing Messages

Our favorite encrypted messenger, Signal Private Messenger, has finally implemented a long-desired feature: message ephemerality. Signal calls the feature "disappearing messages" and has chosen to implement it in an interesting and somewhat unusual way.

First users must enable disappearing messages for every conversation. Unlike Wickr (which set the standard for message ephemerality) there is no way to set a global default message destruction time. Enabling this setting is simple and can be done on Android, iOS, or desktop versions of the application.

Next, users must agree on a destruction interval. Unlike Wickr all users must have the same interval. If User A sets his interval to five minutes, User B will also be set to a five minute interval. We like this because everyone is on the same page, and messages expire in sequence. This does open up the potential for someone in the conversation to turn disappearing messages off, though all users would be alerted to such a change. The available intervals for message destruction are 5, 10, or 30 seconds, 1, 5, or 30 minutes, 1, 6, or 12 hours, 1 day, or 1 week.

What is this actually good for? Messaging systems that delete your messages should only be used with people you trust. Signal offers no screenshot protection on Windows, Mac, or Linux computers, or iOS devices, and even if it did it can be bypassed. The reason we really like disappearing messages is that it allows you to set a destruction interval (let's say 1 day) for each conversation, and know that at most you are carrying around one day's worth of messages. This is greatly preferable to having weeks or months of message traffic on your device should it be compromised.

For more information on Signal visit **https://whispersystems.org/**

Upcoming Events:

Ft. Gordon Cyber Security & Tech Day

19 October 2016, Augusta, GA

Law Enforcement Intelligence Units

1-5 May 2017, Bloomington, MN

For more information go to
www.tpidg.us

Windows 10

SECURITY ROUNDUP

Welcome to your Windows 10 Security Roundup. In this section we highlight our preferred security products for Windows 10. If there are two "Best" options, this means that there was a tie and both products are equally good, but offer slightly different features.

ANTIVIRUS

BEST: AVAST Antivirus. This is one of the most full-featured free antivirus applications we have seen to date. It is light and performs extremely well in independent testing. In addition to offering real-time malware protection, Avast can also assess your network security and tell you if your programs are out-of-date. Avast is available at https://www.avast.com/en-us/index.

ANTI-MALWARE

BEST: **Malwarebytes**. Our favorite anti-malware application is free. Though paid versions offer real-time protection, we like the low impact of the free version, even though it requires the user perform an occasional "on-demand" system scan. https://www.malwarebytes.com/

GOOD: **Spybot Search & Destroy**. It is not a bad idea to get a second opinion if you do find malware on your PC. Our second-favorite option is Spybot S&D, available at https://www.safer-networking.org/

FULL DISK ENCRYPTION

BEST: BitLocker. We really like how easy BitLocker is to use with Windows systems. We don't like that it costs $100. For more information see issue 1.9.

GOOD: **VeraCrypt**… if it works on your system. We really want to like this product, and version 1.18 offers support for WinX systems but we've seen mixed results. When this freeware is fully functional it will be our sole recommendation. https://veracrypt.codeplex.com/

INTERNET BROWSER

BEST: **Firefox**. We prefer Firefox because it offers easy, intuitive security (and is not owned by Google). https://www.mozilla.org/en-US/firefox/new/

We use it with the following add-ons:

Disconnect

HTTPS Everywhere

NoScript

Self-Destructing Cookies

PASSWORD MANAGER

BEST: **Password Safe**. If you don't need your password manager to be cross-platform compatible this is our hands-down favorite, especially for beginners. Password Safe is free and known for being intuitive and easy to use. It keeps all your data local and is secured with very strong Twofish encryption. https://www.pwsafe.org/

coming soon >>>

In Future Issues...

Synology NAS

SightHound Video Surveillance

Teensy

BEST: KeePass. If you do require cross-platform compatibility, we strongly recommend using KeePass. Your data is stored locally and databases can be easily transferred to Mac, Linux, Android, or iOS devices. Best of all, KeePass is completely free and open source. http://keepass.info/

FILE DELETION UTILITIES

Note: secure file erasure techniques do not work with newer solid state drives (SSD). These tools are intended for computers with hard disk drives (HDD).

BEST: **Eraser**. We like eraser because it offers a number of overwrite options from 1 to 35 passes. It is easily used from the right-click context menu. https://eraser.heidi.ie/

GENERAL SYSTEM CLEANUP

BEST: **CCleaner.** This program has a nice interface and cleans dozens of items from your machine. CCleaner is one of the most trusted security applications in existence. https://www.piriform.com/ccleaner

You can add nhundreds more cleaning processes by adding CCEnhancer. https://singularlabs.com/software/ccenhancer/

BEST: **Bleachbit.** Though not as slick as CCleaner, Bleachbit cleans somethings CCleaner misses, and vice-versa. For maximum protection we recommend running both even if there is overlap in coverage. https://www.bleachbit.org/