TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

current topics >>>

In the News:

- CloudBleed: The Latest Internet Security Disaster
  - Gizmodo
- High Severity Bug in Microsoft Edge/ Internet Explorer, No Patch
  - Ars Technica
- Broken SHA-1 Hash Function Finally Declared Dead
  Ars Technica
- Video: Which Lock Screens Secure Your Phone Best
  - Lifehacker Security
- Gmail Now Blocks All JavaScript Attachments
  - Naked Security

Signal Private Messenger

Updated Features

Our favorite private messenger, Signal recently released a major update. Versions 3.29.6 (Android) and 2.7.1 (iOS) were released on February 17. It includes several features that expand Signal's utility. The main features of the upgraded version are:

- **Video Calling**: Signal now supports end-to-end encrypted video calling to other Signal users. Because this feature is still in beta, users will have to enable it by going into Signal's Settings >> Advanced >> Video and toggling it to ON. Video calls are currently only supported between users who have upgraded and enabled video calling.
- **CallKit Support**: If you are an iOS user, you have probably experienced the following situation: you are on a Signal call when a call comes in through your regular phone line. Because the regular call has priority, you are kicked off your Signal call. This is no longer a problem CallKit support gives Signal calls the same priority as normal telephone calls. It also allows you to answer them directly from the lock screen, and it shows them in your phone call log. To enable CallKit open Settings >> Advanced >> Use CallKit.
- **Next-Generation Calling**: If you have made calls with Signal you have doubtlessly experienced dropped calls. This, too, should be resolved thanks to Signal's upgraded backbone servers. Calls are now more stable and reliable. We have tested this and were pleased with the results

There is also one other slight change to Signal. If you have used it heavily for voice calling, you have probably noticed the "Short Authentication String" (SAS) (the two words used to verify your call is not being intercepted). These are no longer present on the new Signal calling interface. Signal has eliminated the SAS because the Signal Protocol has an separate authentication channel that they feel is sufficient. (for more information visit **https://whispersystems.org/blog/signal-video-calls-beta/**).

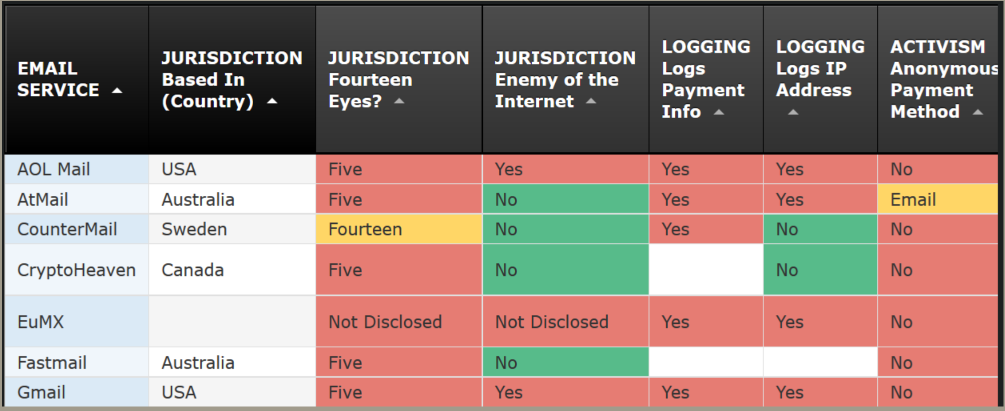
set the stage >>>

Email Comparison Chart

That One Privacy Guy

If you are familiar with virtual private networks, you have probably seen the VPN comparison chart that is maintained by “That One Privacy Guy”. The chart is maintained at a https://thatoneprivacysite.net, and is now accompanied by an email comparison chart. The chart examines over 30 different email services against 45 different privacy and security criteria. These criteria are broken down into ten larger categories: jurisdiction, logging, activism, server configuration, security, availability, website, pricing, and business ethics.

We have used and recommend the VPN comparison chart when selecting VPNs and will doubtlessly refer to the email comparison chart in future research for email providers. The chart is an excellent quick reference when evaluating email services for yourself, your team, or your business. Check it out at **https://thatoneprivacysite.net/email-comparison-chart/**



EMAIL SERVICE ▲	JURISDICTION Based In (Country) ▲	JURISDICTION Fourteen Eyes? ▲	JURISDICTION Enemy of the Internet ▲	LOGGING Logs Payment Info ▲	LOGGING Logs IP Address ▲	ACTIVISM Anonymous Payment Method ▲
AOL Mail	USA	Five	Yes	Yes	Yes	No
AtMail	Australia	Five	No	Yes	Yes	Email
CounterMail	Sweden	Fourteen	No	Yes	No	No
CryptoHeaven	Canada	Five	No		No	No
EuMX		Not Disclosed	Not Disclosed	Yes	Yes	No
Fastmail	Australia	Five	No			No
Gmail	USA	Five	Yes	Yes	Yes	No

Upcoming Events:

Law Enforcement Intelligence Units

May 1-5 2017, Bloomington, MN

Associated Locksmiths of America Expo

June 16-22 2017, Rosemont, IL

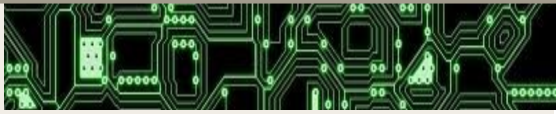
National Technical Investigators’ Association (NATIA) Annual Conference

July 12-23 2017, Tampa, FL

BlackHat USA

July 22-27 2017, Las Vegas, NV

The easy button >>>



NitroKey Start

Hardware PGP Key Storage

The NitroKey Start is a hardware storage solution for PGP key pairs that works with PGP email encryption. We have talked about PGP in the past using Thunderbird for manual PGP or ProtonMail for transparent PGP. We have also talked about the advantages of hardware encryption vs software encryption. The same is true about encryption keys: a hardware solution is always better than a software solution. A hardware solution is also a lot easier to lose and harder to back up securely, so it’s not a perfect solution but it defi-nitely helps significantly when it comes to security.

The NitroKey Start integrates very nicely with the Thunderbird extension Enigmail. Enigmail sees the NitroKey Start as a smart card and it allows you to generate and integrate the keys straight from the device. Enigmail automatically imports the keys and uses them as if they were stored locally on your computer. The keys stored on the device are protected by a PIN which can be anywhere from 6 to 64 digits long. Be sure to set a recovery password if you are worried about losing this PIN. We bricked one of these devices during testing by forgetting the original PIN.

As soon as you unplug the NitroKey Start, you no longer have access to the keys stored on the device. This means if you use PGP on a daily basis, encrypt all of your messages and use the key stored on the NitroKey Start, when you unplug the device, neither you or anyone else will be able to read any of the messages stored in Thunderbird. This device should be treated like any other hardware solution such as the YubiKey or IronKey. There is an option to export the keys from the device, but for absolute security, keep the keys on the device and keep track of it. For more information visit **https://www.nitrokey.com/introduction**

Little Snitch

Outbound Mac Firewall

If you are a hardcore Mac user, you have probably heard of Little Snitch. Little Snitch is probably one of the best applications for Mac we have seen. Little Snitch monitors your Mac's outbound connection and alerts you to any application that attempts to establish an outbound connection. Little Snitch is so effective that most Mac malware scans to ensure that it is not active before executing.

Every time an application attempts to establish an outbound connection, you will be prompted to make a decision. This can be intimidating, because the first few times you use your computer after installing the app, you will be bombarded with pop-ups. Though this can be annoying, this is a good thing because it shows you just how many apps are attempting to gain network access.

As you address these connection attempts, you can make a decision about whether to allow the connection or not. If you choose to allow it, you can decide whether to allow it permanently, or for a predefined period of time. You can also choose to deny it. When in doubt, we recommend denying the connection. This can always be reverted later if you are experiencing issues.

Little Snitch can also be set up in a variety of configurations depending on the network you are using. For example, you may choose less restrictive settings for your home network, somewhat restrictive settings for your work network, and extremely restrictive settings for all other networks.

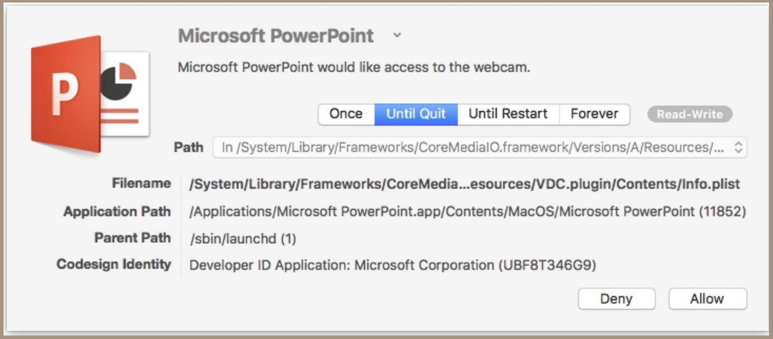
Because it can take some time and patience to properly configure Little Snitch, we recommend setting it up when you are not rushed and can focus on it. Little Snitch is free to try but costs $35 for the full version. We believe this is well worth the cost. Little Snitch is available at **https://www.obdev.at/products/littlesnitch/index.html**

Little Flocker

File Security for Mac

Much like a firewall restricts network access, Little Flocker is a program that protects access to your files. During your day-to-day use of your computer, dozens of applications attempt to access your files. Some of these attempts are legitimate. For example, iMessage may request access to your photo library and this is necessary if you wish to transmit photos via iMessage. Some of these may not be legitimate though. Malicious programs that attempt to exfiltrate data from your machine will also require access to your files. Ransomware that encrypts all your data and demands a ransom will also require access to your files before it can begin encrypting them. Little Flocker can protect you from such attacks.

You may be a little overwhelmed upon initially installing the application. Little Flocker will immediately begin showing pop-ups, asking you to make decisions about the applications that are attempting to access your files. In most cases these requests will be legitimate and necessary for the app to function properly. You can make a decision about whether approval is granted until you quit the application, until your restart your computer, or forever. As an excellent side benefit, Little Flocker also restricts access to your camera and microphone.



Microsoft PowerPoint would like access to the webcam.

Path: In /System/Library/Frameworks/CoreMediaIO.framework/Versions/A/Resources/...

Filename: /System/Library/Frameworks/CoreMedia...esources/VDC.plugin/Contents/Info.plist

Application Path: /Applications/Microsoft PowerPoint.app/Contents/MacOS/Microsoft PowerPoint (11852)

Parent Path: /sbin/launchd (1)

Codesign Identity: Developer ID Application: Microsoft Corporation (UBF8T346G9)

Because of the massive number of applications that will request access, we recommend waiting to install Little Flocker until you have some time to work with it and set it up properly. Little Flocker costs $15 and is available at **https://www.littleflocker.com/**. In our opinion it is well worth the price if you are a Mac user.

coming soon >>>

In Future Issues...

Computer Security Basics

- *OS Hardening*
- *User Accounts*
- *Antivirus/Anti-Malware*

If you would like to see a specific product or service reviewed in the Digital Update, please don't hesitate to get in touch. We are always looking to make content as relevant as possible to our readers. You can reach out to us through TPIDG.us or email directly to admin@tpidg.us .