

Intro to VMs

Burner Challenge

Opera's Built-in VPN

Web Tracking

Little Flocker Update



**TOUCHPOINT**  
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

# Digital Update



current topics >>>

## In the News:

- [Critical Security Updates For Adobe and Microsoft](#)  
- Krebs On Security
- [The Biggest Misconceptions About VPNs](#)  
- Lifehacker
- [Android Devices can be Fatally Hacked by Malicious Wi-Fi Networks](#)  
- Ars Technica
- [Three Zero-Days Against MS Word Found in the Wild: Patch ASAP](#)  
- Ars Technica
- [Shadow Brokers Just Published its Most Damaging Release Yet](#)  
- Ars Technica

## Virtual Machines

### *An Introduction to VMs for Security*

There is a good chance that many of our readers do not regularly use a Virtual Machine. We hope to convince you otherwise because a Virtual Machine (VM) is one of the strongest defensive measures you can take against malware. Below we address some of the most common questions about VMs.

**What is a virtual machine?** A VM is an operating system that can run inside of another operating system. For example, if I have a Windows computer I can open a VM that is running Linux. Though I don't actually have Linux computer, I can run the operating system through a special program.

**What do I need to run a virtual machine?** First, you need a host machine. The host is a computer that you can install VM software on. Next, you will need software that can run the second operating system. The two that we recommend are VMWare and VirtualBox. **VMWare** is more full-featured, but it is not free. **VirtualBox** is completely free but lacking a few features, and is a little more difficult to use. If you are beginner we recommend starting with VirtualBox. Finally, you will need an ISO file. An ISO file is an operating system image. Perhaps the most popular ISO for VMs is a user-friendly Linux distribution called **Ubuntu**.

**What does a VM protect me from?** Virtual Machines protect you from almost every type of malware. Each time you close the VM, you can revert it back to its prior state. This means that even if the VM becomes compromised by malware your host machine will not. It also means that when you reopen the VM, any malware previously contracted will be gone and you will be working from a clean slate.

**Do VMs offer total security?** No. A VM will not protect you from attacks against your data-at-rest, your data-in-motion, or many other forms of attack. A VM is an extremely strong measure to protect you against malware. If you have taken most of the basic steps we have recommended here in the update, VMs may be a good next-step for you.



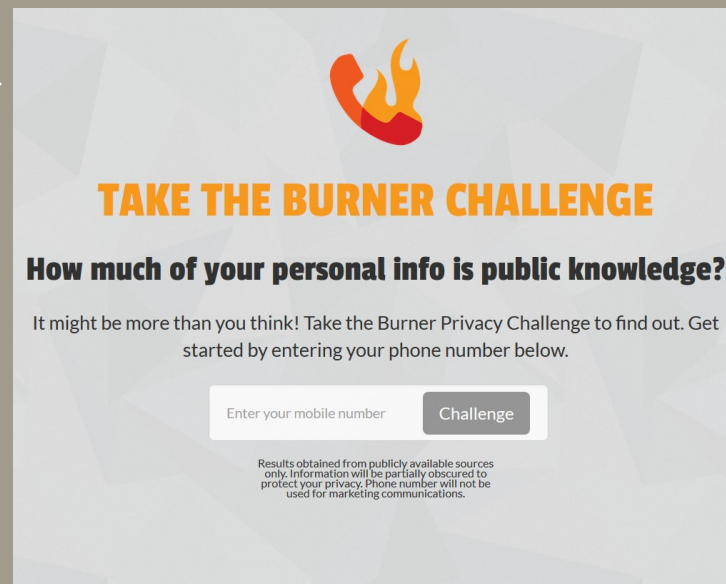
# The Burner Challenge

Your mobile telephone number is increasingly used as a personal identifier. Mobile numbers are used during account creation, as a means of verifying identity, and as a method for transmitting sensitive information. Your mobile account is also associated with a lot of other personal information like your home address. If an attacker knows your phone number, he or she can use it to find this other information.

In the past we have recommended an app called Burner. Burner (available for Android and iOS) allows you to create disposable phone numbers. Burner also offers a unique service called the “Burner Challenge”. This

web-based service allows you to input your phone number and see what other open-source information it is associated with. Awareness of your exposed personal information is a very important part of the self-background check process. Take the Burner Challenge and see what information you have exposed. It may make you think twice about giving out your real phone number in the future..

To take the Burner Challenge visit <http://challenge.burnerapp.com/>



The graphic features a stylized orange and red flame icon at the top. Below it, the text "TAKE THE BURNER CHALLENGE" is written in bold orange letters. Underneath, the question "How much of your personal info is public knowledge?" is posed in bold black text. A paragraph follows: "It might be more than you think! Take the Burner Privacy Challenge to find out. Get started by entering your phone number below." Below this is a form with a text input field labeled "Enter your mobile number" and a grey button labeled "Challenge". At the bottom, a small disclaimer states: "Results obtained from publicly available sources only. Information will be partially obscured to protect your privacy. Phone number will not be used for marketing communications."

The easy button >>>



## Opera's Built-in VPN

*No Substitute for a “Real” VPN*

Following the repeal of FCC regulations that prevent Internet Service Providers from collecting and selling user's browsing data, some articles have recommended switching to the Opera internet browser. Opera made news recently because it has a built-in virtual private network (VPN) that users can enable to protect their browsing activity; however we don't think this is an ideal solution.

The biggest issue we have with this is the limited scope of the Opera VPN. While a true VPN will protect all traffic to and from your computer or mobile device, this VPN does not. It only protects traffic that is generated within the Opera internet browser. This is problematic because a great deal of traffic occurs in other processes on your computer. Some of these processes might be obvious—things like your mail client (Apple Mail, Outlook, or Thunderbird, for example) while others might not. Programs like Microsoft Office are constantly transmitting data from your computer and without your knowledge. This data could be intercepted by a government, hacker, and of course, your ISP.

We respect Opera's initiative in implementing a VPN. This does protect a lot of data that would otherwise be sent completely plaintext. If you use Opera, you may wish to use the built-in VPN as a backup option. To do so enter the browser settings menu, click “Privacy & Security”, and check the “Enable VPN” box.

However, we still recommend using a “real” VPN. As always we use and recommend Private Internet Access. We have written about Private Internet Access before, and currently have an exclusive **25% discount on annual subscriptions** (email [admin@tpidg.us](mailto:admin@tpidg.us) for the link).

## 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*



# Web Analytics

## What Does a Website Know About You?

What does a website know about you, your computer, and your internet connection when you visit it? The answer is, “more than you probably think.” Below are three tools that can help you see your browser through the eyes of the websites that you visit.

**CLICKCLICKCLICK** (<https://clickclickclick.click/>): This website shows you how sites can track your mouse movements around the page. The page itself is a blank page with a button in the center. The page notes where and how you move your mouse, if you click on the page, and the time of day in your current time zone. The website prompts you to turn your volume on; a voice will talk to you in a taunting manner about the information you are revealing.

The best defense against this type of behavior tracking is the use of the NoScript Security Suite. The processes that map your mouse movement on a page are powered by scripts. NoScript will protect you from these scripts and keep your browsing a bit more private.

**PANOPTICCLICK** (<https://panopticklick.eff.org/>): Sponsored by the Electronic Frontier Foundation, this site tests your browser’s unique fingerprint. Your browser sends information to the websites you visit. This information includes your preferred language, screen size and resolution, and the browser extensions you have installed. This data is used to help websites deliver content that is optimized for your device, but it can also be used to uniquely identify you. Visiting the Panopticklick website will show you how distinctive your browser is.

One of the best defenses possible against browser fingerprinting is to keep your browser as “stock” as possible. The more add-ons you install on your browser, the more distinctive it becomes.

**IPLEAK.NET** (<https://ipleak.net/>): This site reveals the IP address information available to the sites you visit. IP Leak will tell you if your IP address, IPV6 address, DNS requests, or location is leaking to websites. You can also find out if your browser is sharing your location data through IP Leak. If you aren’t using a VPN all of this information is definitely being leaked. If you are using a VPN, this is a great way to ensure it is actually working for you.

We hate to keep repeating it, but the strongest line of defense here is the use of a virtual private network. A good one will hide your IP address, protect you from IPV6 and DNS leakage, and encrypt your data-in-transit.

## Little Flocker Update

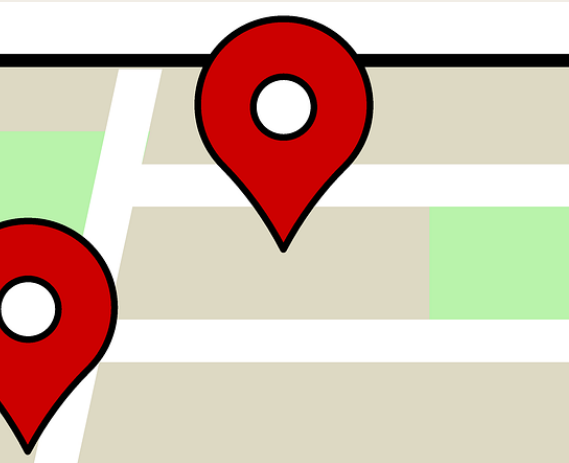
### Popular Mac Security App Website Disappears

In the early March issue of the Digital Update (2.05) we recommended a Mac security product called Little Flocker. Little Flocker was a product similar to a software firewall that protected your files from being accessed by unauthorized applications. Unfortunately, if you have tried to obtain this product within the last few days you have probably noticed that the Little Flocker website is down.

We learned last week that Little Flocker was sold by its author, Jonathon Zdziarski to F-Secure. F-Secure is a reputable company known for producing high quality antivirus applications. Little Flocker will now be known as “XFence”.

Though XFence is bundled into F-Secure’s premium Mac security software products, it will also be available to consumers. F-Secure plans to offer the XFence beta as a free download for personal users. From what we are able to tell it seems that the functions of the old Little Flocker will remain the same, with some minor cosmetic differences. If you are interested in using XFence, visit <https://campaigns.f-secure.com/xfence/>

For the full story you can read F-Secure’s press release at [https://www.f-secure.com/en/web/press\\_global/news-clippings/-/journal\\_content/56/1075444/1968982](https://www.f-secure.com/en/web/press_global/news-clippings/-/journal_content/56/1075444/1968982)



coming soon >>>

*In Future Issues...*

*Internet Browser Comparison*

⇒ *Chrome, Firefox, Opera*

⇒ *Mobile Browsers*

*Firefox Setup Review*

*Browser Extensions*

