



# Torian Group Times

“Technology with Integrity”

www.toriangroup.com

September 2018

It's almost time for [another Windows 10 Feature Update](#). These updates are released about every 6 months. Be sure to keep your PC at least within the last year's updates to continue to receive security patches. Windows 10 [Version 1703 support ends](#) on October 9<sup>th</sup>.

All [Surface Pro \(2017\) models are now \\$200 off](#) at the Microsoft Store. A new version is [in the works for next year](#).

Apple expected to unveil [new iPhone and Apple Watch models](#) on September 12<sup>th</sup> including a larger iPhone X.

The Samsung [Galaxy Note 9](#) is out and available.

As of Oct 1, Microsoft **Office Home and Personal** subscriptions will be [allowing up to 6 devices](#) rather than 5. They are changing the license count to be based on simultaneous logins rather than devices with Office installed.

[Office 2019](#) (Standalone install) release date is set for Oct 1. [Pricing will go up 10%](#). Office 2019 will not include OneNote.

If you have MS Office through an Office 365 subscription, [you already have the features in Office 2019](#), delivered through regular monthly updates. Microsoft is pushing hard to get users on a subscription.

Microsoft Products [Reaching End of Support in 2018](#).

[Java will not be free after Dec 2020](#).

Oracle will continue to provide Public Updates and auto updates of Java SE 8, until at least the end of December 2020 for Personal Users, and January 2019 for Commercial Users.

**Older Kindles** may require a [manual update](#) to stay connected.

**QuickBooks** and Microsoft (among others) are requiring that workstations connect using the newer and more secure web protocols when using HTTPS:// called **TLS 1.2**. Servers also need to be updates to use the newer protocol.

[Fix for QuickBooks](#) – you will be prompted to update when opening QuickBooks.

[Fix for Microsoft Office 365 web access](#)

[Google tracks your movements](#) on Android mobile devices -like it or not. At a Google Marketing Live summit in July, Google executives [unveiled a new tool](#) called “local campaigns” that dynamically uses ads to boost in-person store visits. [Related lawsuit](#).

Google is also [using data from MasterCard](#) to link in-store purchases to online searches. You can opt out using Google's “Web and App Activity” online console, but the default is to share your data.

[California fire map](#)

Verizon [throttled firefighter data](#).

**[Fax Machines should not be on your network](#)**. [Recent demonstrations](#) show how a malformed fax can be used to hack into a network using a connected multifunction fax/printer. HP OfficeJets have an [update](#) to resolve this issue.

[Russian hackers targeted U.S. Senate, think tanks](#) (again)

Marketers want to [profit from information tracked in your vehicle](#).

**[Voter Database left unsecured online](#)** –perhaps the largest known exposure of voter information in history -3 out of 5 voters.

A misconfigured database containing the sensitive personal details of over 198 million American voters was left exposed to the internet by a firm working on behalf of the Republican National Committee (RNC). The RNC data repository contained roughly 9.5 billion data points scoring 198 million potential US voters (regardless of party) on their likely political preferences... making it possible to piece together a striking amount of detail on individual Americans specified by name. ...the files go on to list a great deal more data, including the voter's date of birth, home and mailing addresses, phone number, registered party, self-reported racial demographic, voter registration status... "modeled religion" and 35+ categories rating modeled political positions on various topics.

There are about 250 Million registered voters. US population is about 325 Million.

### **The ABCs of Hacking a Voting Machine**

Hackers in [Def Con's](#) "voting village" managed to swap out software, wrest control of tabulation and [manipulate the behavior of voting machines](#) that will likely be used in midterm elections. In one example, it takes about [2 minutes and a ball point pen](#). Manufacturers claim the exploits would be difficult or impossible under actual voting conditions, hackers disagree.

### **1.4 Billion stolen passwords [are free for the taking](#)**

There's an easy way to find out if you are on the list. [Have I Been Pwned](#) indexes close to five billion breached passwords, and lets you easily check to see if your account is affected. [No Secrets](#) offers a similar free service. We recommend checking your email address on these sites.

A [new twist on phishing](#) uses these stolen passwords to scare you into sending money.

**Password based authentication is [no longer an acceptable best practice](#)**. "If consumers don't assume that at least some of their passwords have been compromised, they only create a dangerous false sense of security."

The web site [twofactorauth.org](#) lists online service providers with the types of secondary authentication offered. Enable it where you can.

"Just over 10% of people use at least one of the **25 worst passwords [on this year's list](#)**, with nearly 4% of people using the worst password, 123456."

### **[2 million T-Mobile customers data hacked](#)**

Customer names, billing ZIP codes, phone numbers, email addresses, account numbers, and account types are believed to be involved.

Separately, researchers uncovered a bug in T-Mobile's website which allowed anyone to access the personal data of customers using only a phone number.

Fiserv, Inc., which provides banks with web services, [just fixed a glaring weakness](#) that **exposed personal and financial details of countless customers** across hundreds of bank Web sites... Check your bank's browser address bar after login: [secureinternetbank.com](http://secureinternetbank.com) to see if your bank might have been affected.

**Any phone or tablet is subject to arbitrary seizure at airports.**

[An American woman had her iPhone seized and cracked by Customs](#) and Border Protection despite her objection. ... "now everyone's phones, despite country of origin or cause, are subject to nonconsensual seizure and search -- even if we refuse to give up our passwords." ...in March 2017 phone and digital-device searches by Customs and Border Protection agents at airport checkpoints had more than doubled. Those searches had expanded to include password demands. When the new Trump policies began, 5,000 devices were searched in February alone — that's around 180 people a day.

**SingHealth Hacked**

Singapore's largest group of healthcare institutions, revealed that personal data belonging to [1.5 million patients](#) had been "accessed and copied" without consent. National identification numbers, addresses, and dates of birth were involved in the breach.

We are in the process of upgrading the Remote Management Agent we use to support your computers. It is a more capable product from the same vendor (SolarWinds). There is no charge for this upgrade.

*Tim Torian*

Torian, Group, Inc.

<http://www.toriangroup.com>

This and past newsletters, and various articles are available on our web site. You can receive this newsletter via email. To subscribe or unsubscribe: <http://www.toriangroup.com/newsletter> or email to [tim@toriangroup.com](mailto:tim@toriangroup.com)

Torian Group, Inc. 519 W. Center Ave. Visalia Ca. 93291 (559) 733-1940