Torian Group Times

"Technology with Integrity"

www.toriangroup.com December 2018

The **Windows 10 October 2018 Update** was released Oct. 2nd. The release was then paused (cancelled till they figure out a fix) then released again Nov 13th. More problems were found, which are mostly fixed in a patch currently in beta testing. For now, avoid this update. Clients on maintenance are protected, as we review updates before they are installed.

If you did install the update, get the updated versions of iCloud and Trend Micro Antivirus if you have either installed. Then install this patch: KB4467682 which fixes some serious bugs.

Windows Server 2019 is now available.

Office 2019 "deal" scams on Amazon and Ebay
If it sounds too good to be true, it probably is.
Again, also beware of "knockoffs" being sold on Amazon when Christmas shopping.

Microsoft offers **2-factor authentication** for their Exchange Online (Office 365) email accounts. We strongly recommend you contact us to enable this for your business. We are seeing an increase in hacking and phishing attempts to gain access to email. With your email, hackers can then recover passwords from your other accounts, such as banking and credit card sites.

Microsoft's multi-factor authentication service goes down for second week in a row
Even the most reliable cloud services are vulnerable to outages beyond your control.

We recommend you check https://haveibeenpwned.com/ regularly by entering your email address. I checked tim@toriangroup.com, and found 4 leaks which included my email address, including Apollo (see below) and DropBox. This only tells you that your email was in a past leak. It doesn't mean it is at risk if you have changed your password since then. It does mean you will likely be a target of phishing emails.

In addition, marketing vendors are gathering all kinds of data on you and selling it to anyone who will pay. Even if it wasn't leaked, your name, address, email, phone number, employment, credit info, shopping habits and much more are publicly available.

The goal is to get you to take security seriously – use unique passwords for each online account. Assume that your personal data is public knowledge. Lock your Credit Bureau files. Use 2-factor authentication for sensitive accounts like banking and email.

California's new SB 327 law, which will take effect in January 2020, requires all "connected devices" to have a "reasonable security feature." The good news is that the term "connected devices" is broadly defined to include just about everything connected to the Internet. The not-so-good news is that "reasonable security" is defined such that companies trying to avoid compliance can argue that the law is unenforceable.

'Technical error' temporarily **exposes Amazon customer names and email addresses**

USPS Site Exposed Data on 60 Million Users
In addition to exposing near real-time data about packages and mail being sent by USPS commercial customers, the flaw let any logged-in usps.com user query the system for account details belonging to any other users, such as email address, username, user ID, account number, street address, phone number, authorized users, mailing campaign data and other information. “It seems like the only access control they had in place was that you were logged in."
U.S. Secret Service Warns that ID Thieves are Abusing USPS’s Mail Scanning Service

Marriott's Starwood database hacked, 500 million may be affected
Starwood brands include W Hotels, St. Regis, Sheraton, and Westin Hotels. Passport details, phone numbers and email addresses of some 327 million Marriott customers were exposed. The breach appears to be the second-largest on record.

Hacker hijacks 50,000 internet connected printers to print ads. Be sure your printer web management has a password if it is connected to the network.

GovPayNow.com Leaks 14M+ Records
Government Payment Service Inc. — a company used by thousands of U.S. state and local governments to accept online payments for everything from traffic citations and licensing fees to bail payments and court-ordered fines — has leaked more than 14 million customer records dating back at least six years, including names, addresses, phone numbers and the last four digits of the payer’s credit card.

Quora discloses breach impacting 100 million users
Quora is an online survey company. Account info, passwords, emails, private messages, and user votes were exposed.

Emails of top NRCC officials stolen in major 2018 hack
The email accounts of four senior aides at the National Republican Congressional Committee were surveilled for several months … during the 2018 midterm campaigns. …
they privately believe it was a foreign agent because of the nature of the attack.

Apollo Breach Exposed *Billions* of Data Points
Apollo is a data aggregator and analytics service aimed at helping sales teams know who to contact, when, and with what message to make the most deals. The Apollo data enables scammers, fraudsters, and phishers to craft compelling targeted attacks against a huge number of people. You may be on their database, even if you have never heard of them.

Firefox add-in will alert users about recently breached sites
The service has a web component allowing Firefox users may enter email addresses to check whether the email is found in compromised databases, and to sign up for alerts to receive word when their email address is found on a newly leaked database. The Firefox service uses the same database of compromised accounts as https://haveibeenpwned.com/

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@toraingroup.com

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