Torian Group Times

"Technology with Integrity"

www.toriangroup.com August 2019

Microsoft is requiring that **admin accounts in Office 365 have 2-factor authentication**. To support this, they are offering additional online security tools at no cost to Office 365 users who work with a Microsoft partner (such as Torian Group).
The FBI, Homeland Security/ CISA and NIST, are recommending 2-factor authentication for sensitive accounts as well. Office 365 security checklist.

We have been recommending for a while that all accounts for email be configured for higher security including the following:

- Configure a phone or mobile device to confirm your identity when logging in online.
- Set up Outlook and devices with email or Skype for Business to use separate "app passwords".
- Turn off POP and IMAP access if it is not needed.
- Enable tracking of sensitive accounts by adding a P1 or P2 security license to your Office 365 admin accounts. Enable mailbox auditing for existing accounts.
- Turn on specific security settings in Office 365 including Microsoft Secure Score. (https://security.microsoft.com/securescore on Office 365),

Once a hacker has access to your email, they can use it to recover other passwords (such as bank logins) and to send out malware as you.

Microsoft is also offering a Security Policy tool for deploying Microsoft Office. Computers using Office 365 for the Office suite can use these tools. It requires that the computer be connected to the internet.

Office 365 - As part of your subscription, users can still install and activate Office 365 apps on up to five PCs or Macs, five tablets, and five smartphones. Previously, users who reached this limit were prompted to deactivate an existing install before activating Office on a new device. Going forward, Office will automatically sign the user out of the user's least recently used device when the user exceeds the limit.

Starting September 1, 2019, all new Office 365 customers will be onboarded to Teams and will not have access to Skype for Business Online**. Skype for Business Online** will be retired in 2021. As mentioned before, Skype for Business users will be forced to start using Teams over the next few months. Teams will be automatically installed as a part of Microsoft Office Pro Plus.

Office Online will now be called Office. This is part of a trend to push everyone toward an Office 365 subscription.

If you use **MS Office on a Terminal Server,** FSLogix technology is now available at no additional cost for Microsoft 365 customers with specific licenses. It improves the performance of Office 365 ProPlus in multi-user virtual environments.

Passwordless login in now supported for Windows 10 using FIDO2 Security keys. It's still a bit complex, but something to look forward to.

Microsoft has blocked their Surface Book 2 from receiving the **Windows 10 May 2019 Update** after the upgrade had unintended consequences. PCs that use USB storage or SD cards have the update blocked.

Apple is set to release their new "no fee" **titanium credit card** sometime this month.

Elon Musk tech startup Neuralink announces progress. The company will **build implants that connect brains with computer interfaces** via artificial intelligence. Testing on humans will begin by the end of 2020.

Scientists have created **contact lenses that are able to zoom in** when you blink.

Amazon is seeking permission to launch 3,236 satellites that would create an internet network covering the entire world.

3G Phone networks will stop working soon.
AT&T stopped allowing new activations on the 3G network at the end of 2018 but has committed to keeping their 3G network operational through the end of 2021. Verizon stopped allowing new activations on June 30, 2018 and will deactivate their 3G network at the end of 2019.

The latest figures in Amazon's transparency report said the number of **subpoenas** it received went up by 14% and **search warrants** went up by close to 35%. That includes data collected from its Amazon Echo voice assistant service, its Kindle and Fire tablets and its home security devices.

SECURITY

How to tell if you were affected by the Capital One breach

- Capital One believes the breach exposed credit card application data for those who applied between 2005 and 2019.
- The company says this works out to roughly 100 million individuals in the U.S., and 6 million in Canada.
- The data leaked potentially includes "names, addresses, ZIP codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income" of those who applied, as well as information like "credit scores, credit limits, balances, payment history, contact information."
- Capital One is estimating that roughly 140,000 Social Security numbers were potentially compromised in the U.S., as well as 80,000 linked bank account numbers. In Canada, roughly 1 million Social Insurance Numbers were compromised.
- Transaction data for "a total of 23 days" spread across 2016/2017/2018 was obtained.

Equifax data breach settlement - Use this site to see if your info was compromised and claim free credit monitoring for 4 years or your share of the $125 per person settlement – the actual settlement you will receive with the cash option is estimated at about $2 per person. Other compensation may be available if you can prove you were harmed and it cost you.

StockX was hacked, exposing millions of customers' data
The stolen data contained names, email addresses, scrambled password, shoe size and trading currency.

Thousands of **Android apps** continue to track you even if you opt to deny their permissions - including Apps from big companies like Samsung and Disney.

ElasticSearch data leaks continue to put millions of people and businesses at risk. The most recent server breach was a China data leakage of two databases containing more than 90 million records.

Pearson, the London-based educational software maker, **leaked thousands of school and university accounts**, mostly in the United States. Unauthorized access was gained to 13,000 school and university accounts. The data exposed included first and last names and, in some cases, date of birth and email addresses. Each account could potentially include information about thousands of students.

An unprotected server from VOIPO - an online phone service – allowed access to close to seven million call logs, six million text messages and other internal documents containing unencrypted passwords.

If you use a **Fortigate firewall**, a firmware update may be needed. Vulnerability in the FortiOS SSL VPN web portal.

Microsoft has seen a steady increase in campaigns that use fileless and "living-off-the-land" cyberattacks. This kind of malware is used to evade detection from most anti-virus tools by running only in RAM memory.

A flaw found in **Lenovo NAS** Firmware has been found to expose stored data. More than 5,100 devices containing multiple terabytes of data are open to exploitation.

Microsoft notified 10,000 customers that they were **victims of a cyber-attack** targeted by countries like Russia, North Korea, and Iran.

If you use RingCentral on Apple - There was a flaw found that would allow hackers to access your webcam through RingCentral.

You can be pretty sure that your personal data is on the Internet somewhere. Take steps to lock your credit services, use unique complex passwords, and set up 2-factor authentication for any website logins you care about.

Tim Torian
Torian, Group, Inc.
https://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: https://www.toriangroup.com/newsletter or email to tim@toraingroup.com