# Torian Group Times

**"Technology with Integrity"**

www.toriangroup.com September 2024

The end date to purchase new **QuickBooks Desktop** licenses has been extended to Sept 30.

Reminder: Basic authentication will no longer be supported for Microsoft products after September 16, 2024. Microsoft's article: Modern authentication methods now needed to continue **syncing Outlook email** in non-Microsoft email apps.

**TED Talk** X comes to the Visalia Fox Theatre on Sept. 7 with 10-minute talks by locals.

The **Microsoft Action Pack** will be discontinued in January 2025.

iSlips Online allows you to enter time into Timeslips without purchasing a full user license.
If you use Timeslips, this could save you money.

Intel announces two extra years of warranty amid chip crashing and instability issues.
The manufacturing problem appears to involve oxidation on the chip, something that happens over time.

**Wi-Fi 7** devices are out. Consider Wi-Fi 7 support for any new equipment. If you are upgrading or getting cable service, Wi-Fi 7 is supported on some new cable modems . More on Wi-Fi 6E vs Wi-Fi 7.

"**TikTok** knowingly and repeatedly violated kids' privacy, threatening the safety of millions of children across the country."

**Google** was found liable in search monopolization case.

**Apple** to hold fall event on Sept. 9, new iPhones expected.

**US Social Security Administration** is switching to login.gov for 2-factor authentication for online SSA accounts. ID.me accounts will be migrated to login.gov.

**TV** software is getting loaded with ads, changing what it means to own a TV set.

**AI**

**Deepfake scams** evolve as technology evolves, making it harder and harder for people to tell the real from the fake. Below is a list of top deepfake scams to watch out for:

- Romance Scam
- Recruiting Scam
- Investment Scam

Deepfakes explode in Japan, tearing down the language barrier.

South Korea is on high alert over deepfake sex crimes.

Harmful “undress” websites use AI to remove clothes from real photos to make victims appear to be “nude” without their consent. More than a dozen deepfake websites have been using login buttons from Google, Microsoft, and other companies for months.

**SECURITY**

**Yubikeys can be cloned**
If a hacker can borrow your Yubikey 5, it can be duplicated with some advanced tools. In most cases it would be easier to simply steal it – I don’t think this is a big risk, but something to be aware of.

**National Public Data Breach**
Data brokers like National Public Data typically get their information by scouring federal, state, and local government records. Those government files include voting registries, property filings, marriage certificates, motor vehicle records, criminal records, court documents, death records, professional licenses, bankruptcy filings, and more.
Jerico Pictures Inc., a background-check company doing business as National Public Data, exposed nearly 3 billion records in an April data breach. According to researchers at Atlas Data Privacy Corp., there are 272 million unique SSNs in the entire records set. Atlas discovered that many records are related to people who are now almost certainly deceased. They found that the average age of the consumer in these records is 70, and around two million records are related to people whose date of birth would make them more than 120 years old today. So, it’s not as bad as it sounds.
“If you find yourself in this data breach via HaveIBeenPwned.com, there’s no evidence your SSN was leaked - the data next to your record may not even be correct.”
A related site — the background search service recordscheck.net — was hosting an archive that included the username and password of the site’s administrator.

In 2019, malicious hackers stole data on more than 1.5 billion people from People Data Labs, a San Francisco data broker whose people-search services linked hundreds of millions of email addresses, LinkedIn and Facebook profiles, and more than 200 million valid cell phone numbers.

Should you worry that your SSN and other personal data might be exposed? Not if you have frozen your credit file at each of the major consumer reporting bureaus. Having a freeze on your files makes it much harder for identity thieves to create new accounts in your name, and it limits who can view your credit information.
All of the information ID thieves need to assume your identity is now broadly available from multiple sources from data breaches. In addition, numerous cybercriminal services offer detailed background checks on consumers, including full SSNs. These services use compromised accounts at data brokers that cater to private investigators and law enforcement officials, and some are now fully automated via Telegram instant message bots. If you haven’t frozen your credit files and you haven’t yet experienced some form of new account fraud, the ID thieves probably just haven’t gotten around to you yet.
The Federal Trade Commission announced last year that the bureaus had permanently extended a program that lets you check your credit report once a week for free.

Toyota confirms third-party data breach impacting customers.

**Dick's Sporting Goods** discloses unauthorized third-party access to information.

CBIZ Benefits & Insurance Services (CBIZ) has disclosed a data breach that involves unauthorized access to client information, including contact info, SSN, and date of birth.

Texas is suing General Motors for collecting driver data without consent and then selling it to insurance companies.

**HUMOR**


*Tim Torian*
Torian, Group, Inc.
https://www.toriangroup.com