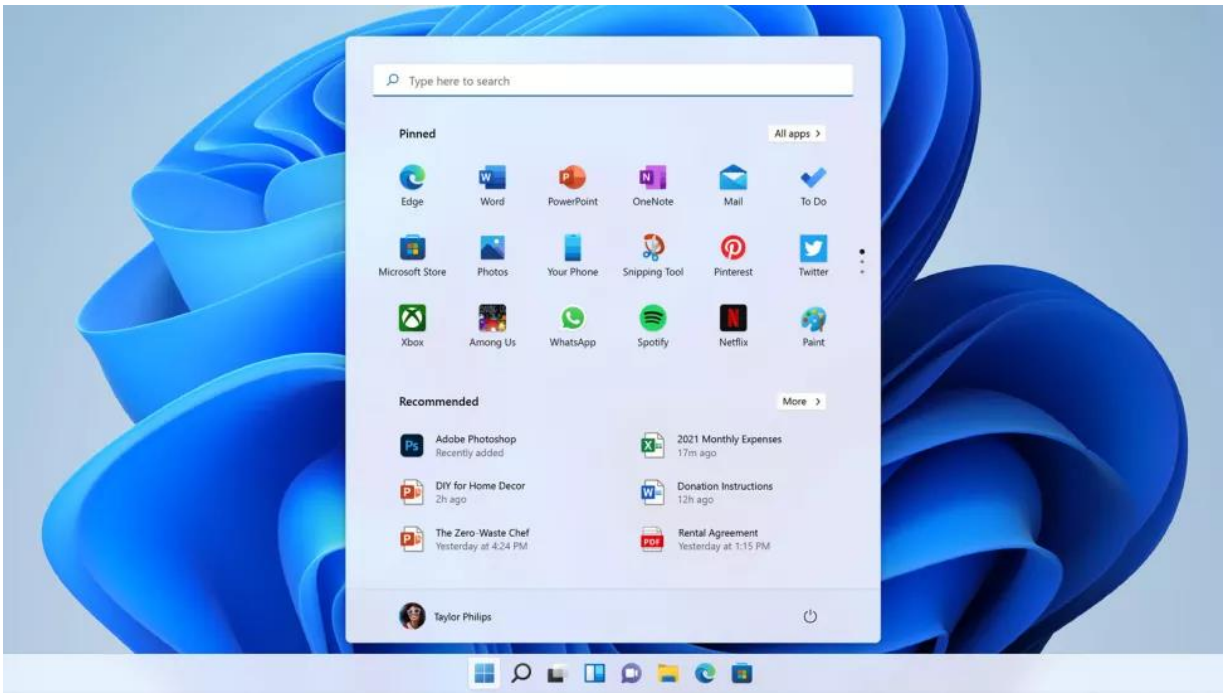
Torian Group Times

"Technology with Integrity"

www.toriangroup.com September 2021

Windows 11 will be available on October 5th. It will be a free upgrade for Windows 10 users. We recommend waiting to install it on business systems.
Windows 11 will require TPM 2 hardware, which is in most recently purchased computers. They have modified the hardware requirements slightly to include more older computers. An updated compatibility checker can be downloaded here, to see if your computer meets the hardware requirements for Windows 11.



It looks and sounds a bit different but should be an easy transition for Windows 10 users.
Most existing software will work. Updated drivers may be needed to take advantage of some new video and security features. The most significant changes are improvements in security.
Windows 11 will get feature updates once a year rather than twice.
Windows 11 FAQ: Everything you need to know. Feature list
Details on Windows 10 and 11 hardware and security features for the technically inclined.

Microsoft will support **Windows 10** through October 14, 2025. The next Windows 10 version (21H2) is planned for early October. It will be a minor update for those that installed the May 2020 or later update, and a reinstall for older systems. Versions prior to May 2020 are no longer receiving security updates, and should be updated right away.

Windows Server 2022 released

New features include improvements in security, storage and networking, and greater integration with Azure cloud services. There is a clear emphasis on pushing customers toward running servers in the Azure cloud rather than on premises. Technical details
Prices have gone up slightly, with the same three editions: essentials, standard, and datacenter.

Windows Server 2022 will be supported for 5 years. Microsoft has now abandoned the semi-annual channel in which server releases were only supported for 18 months.

Microsoft 365, Office 365 to cost a little bit more starting next March
Microsoft 365 Business Basic: $6, up from $5.
Microsoft 365 Business Premium: $22, up from $20.
Office 365 E1: $10, up from $8.
Office 365 E3: $23, up from $20
Office 365 E5: $38, up from $35
Microsoft 365 E3: $36, up from $32
A web version of **Visio** is now included in Microsoft 365 commercial plans at no additional cost.

Microsoft Defender for Endpoint Plan 1 is a new product

If you use the **Microsoft To Do** app, update to version 2.49 or higher before the end of October 2021 to avoid any issues with cross-device syncing. Stay logged in to avoid losing un-synced data.

From early October on, the **Teams app for iOS** will require iOS 14 or above.
Starting September 13, 2021, Outlook mobile (Apple and Android) will stop syncing calendars on Facebook, Meetup, and Evernote.

The Office for Android apps won't be supported on **Chromebook** devices after mid-September. That leaves Chromebook users with Office on the web and Outlook.com in the Chrome browser.
The future of the OneDrive app for Chromebook is unclear.

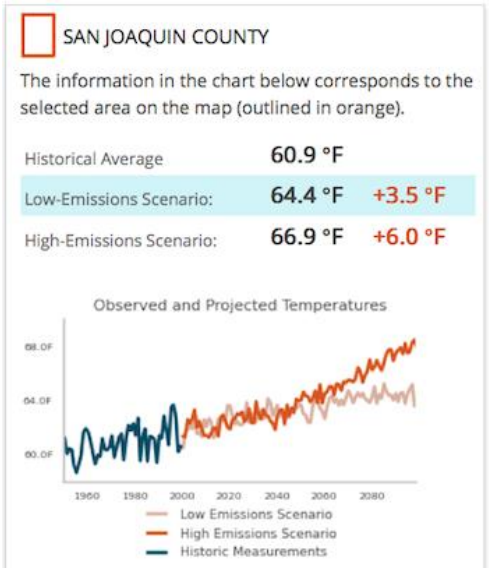
Check out the IFTTT page for **OneNote**

Duo Mobile version 4.0.0 is scheduled to roll out to users starting October 11th.
Be sure to update if you use the DUO app.
Guide to the new **Duo Mobile** version 4.0.0 for Duo administrators

Avast bought by Norton for 8.6 billion US dollars

General Motors will temporarily halt production at all but four of its North American factories due to chip supply constraints.

What **Climate Change** Means for California (pdf from the EPA)
Overview of Projected **Temperature Change in the California Central Valley**



COVID

Watch How SARS-CoV-2 Spreads through Mice

Tracking how the coronavirus crushed California's workforce

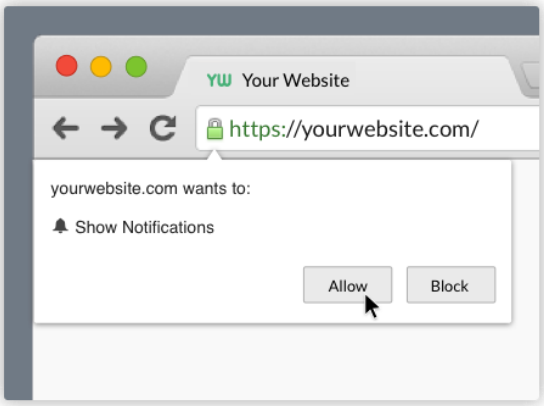
COVID-19: Implications for business (McKinsey update)
"McKinsey's analysis supports the view of others that the Delta variant has effectively moved overall herd immunity out of reach in most countries for the time being."
US consumer spending recovered in the second quarter of 2021, driven by increasing vaccination rates, stimulus payments in March 2021, and the general reopening of the economy.

43% of eligible Tulare County residents are **fully vaccinated**
Experts warn that vaccination deserts in one region can affect the community at large. Areas with a high concentration of unvaccinated residents who do not practice social distancing or mask-wearing can create the perfect conditions for the spread of the Delta variant.
"…These conditions can sew distrust in government, she said. During a pandemic, that could explain why many residents in unincorporated areas are more likely to believe misinformation circulating within their communities rather than advice from government officials or public health departments."

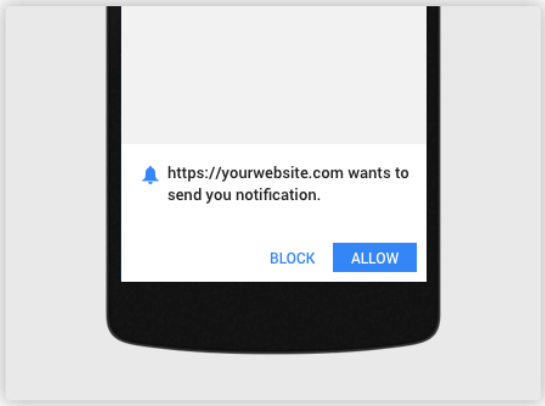
SECURITY

Storing your **passwords in your browser** can be risky. Chrome will automatically import your passwords from other browsers. Chromepass is a free utility to expose all passwords saved in chrome. Other browsers have similar tools. You can encrypt your Chrome data and log out of your browser session each time you close it. However, most people who are still saving passwords in their browser probably won't bother. Be sure to turn off password saving in your browser. You are better off using a more secure password manager such as LastPass or OnePassword.

Browsers now have the ability to send "notifications" to your desktop. It is easy to "Allow" without realizing you are setting yourself up for desktop spam.



Desktop Opt-in

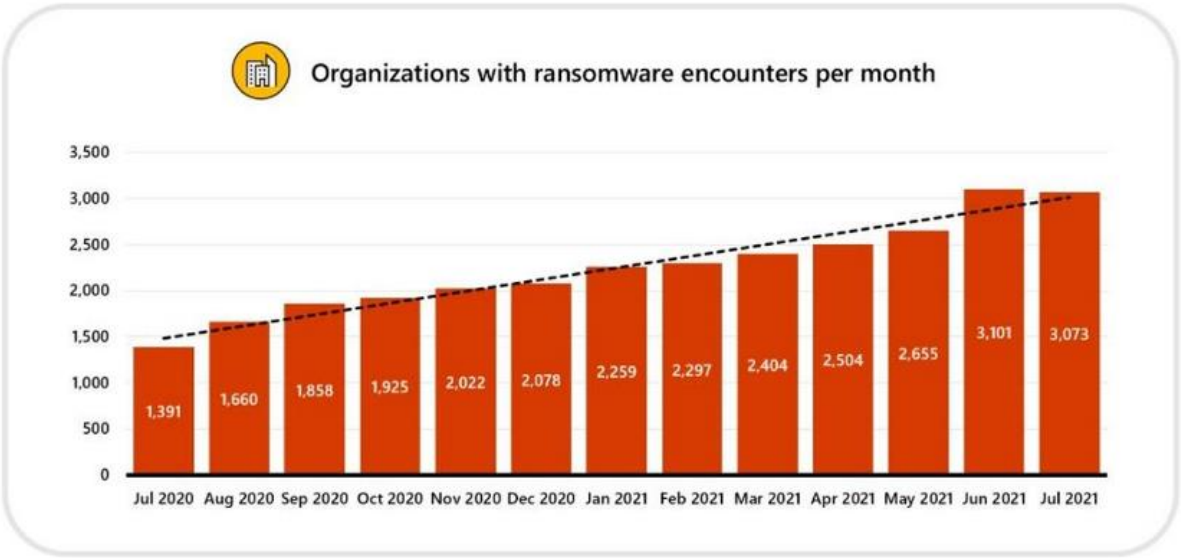


Mobile Website Opt-in

We have had several clients who thought they had malware after allowing notifications on websites.

Cisco router RV models need a firmware update
CVE-2021-1609 impacts RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN routers, while CVE-2021-1602 affects RV160, RV160W, RV260, RV260P, and RV260W VPN routers.
The remote management feature is vulnerable. It is disabled by default on all affected VPN router models.

Cisco Small Business **RV110W, RV130, RV130W, and RV215W Routers** have serious flaws which will not be patched as these models are no longer supported. Turning off UPnP is a workaround, but these should be replaced.



Make sure you have at least protected your email with 2-factor authentication.
A shocking number of cyberattacks are publicly attributed to account compromises linked to a lack of **MFA (Multi-Factor Authentication):** In 2020, Microsoft's Alex Weinert said that 99.9% of successfully attacked Microsoft 365 accounts had MFA disabled.

75% of enterprise security managers plan to increase MFA spending

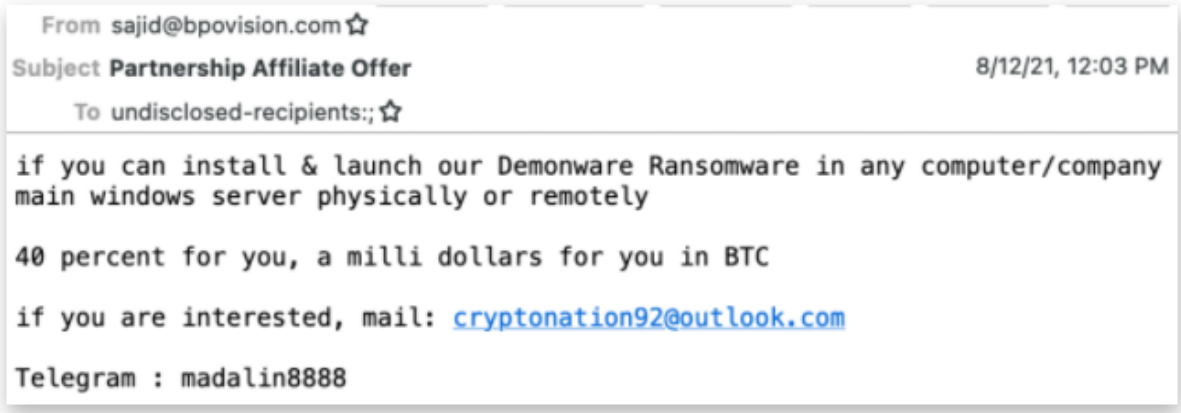
Billions of devices impacted by new Bluetooth vulnerabilities
Vulnerable to these attacks are Microsoft Surface laptops, Dell desktops, and several Qualcomm-based smartphone models. It requires being in Bluetooth signal range (about 30 Ft.).
Turn off Bluetooth if you are not using it.
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28139

Google revealed seven high-rated security threats in **Chrome** on all major operating systems, including Android, Windows, iOS, and Linux.

American Express Card data breach
The Amex Card data breach involved a partner merchant and not Amex itself. However, if you're one of the customers whose credit card and personal information was stolen, the difference is negligible.

AT&T denies data breach after hacker auctions 70 million user database

Wanted: Disgruntled Employees to Deploy **Ransomware.**



Initial email sent by the threat actor.

HUMOR

"Oh I installed the driver all right!"

"Someone cracked my password. Now I need to rename my puppy."

TORIAN GROUP

You may have noticed a set of hidden folders and files showing up on the root of all of your drives.
If not, you can ignore this – you probably have your computer set not to show hidden files.

They look like this:

This was put there by the SentinelOne anti-malware software as a part of the ransomware detection /protection feature of the software.
These files are monitored to see if they get modified by ransomware. If they are, the computer will immediately take action to prevent any other files from being encrypted or modified by the ransomware - preventing the attack from spreading. This is why they are present in the root of each drive or drive share. These files were in the documents folder and were added to the root of each drive with the SentinelOne upgrade released 9/2/2021.

Please leave them alone if possible. Removing them will not stop other malware protection, but it voids the ransomware protection insurance that comes with SentinelOne.

You may also see this message during the update process:

More information from:
Ransomware by Allan Liska, Timothy Gallo | O'Reilly Press
Honeyfiles and Honeydirectories
One method of detecting ransomware on a system or a network is the use of a honeyfile. A honeyfile takes the honeypot concept and moves it to the file level. A honeypot is an exposed system that is designed to look vulnerable to attacks. An attacker will compromise the system, and the security team is alerted to the fact that there is a hacker inside their network or attempting to get inside the network.
https://www.oreilly.com/library/view/ransomware/9781491967874/ch04.html

We do a "dark web" search for compromised login credentials for your email domain as part of maintenance. Contact us if you would like a report.

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