Torian Group Times

"Technology with Integrity"

www.toriangroup.com May 2024

The Professional and Home editions of **Windows 11 22H2** reach end of life on October 14, 2024.
Users on Windows 11 22H2 should move to 23H2.
To check your version: Settings | System - scroll all the way to the bottom to click About. Look for the Version.

Included in the April patches for **Windows 11** 22H2 and 23H2 is the Moment 5 release.

The Windows 11 File Explorer interface is changing - it's not you; the way it works is being updated. Updates are being released gradually. You may find that the menu changes as Windows updates are applied. File Explorer recently got tabs. There are problems with the tab names, making it hard to navigate. The right-click menu also has been changing. Open With doesn't work as expected when multiple files are selected. Some missing items can be found under "more options."

Microsoft experimented with ads in the Windows 11 Start menu in November 2022, promoting some of its products, including OneDrive, in the Start menu's sign-out flyout menu. They are expanding the feature in March 2023 with new "treatments."

Windows 11 24H2 is coming this fall. Expected features:
Copilot will let you access a wider range of commands and controls directly from the desktop.
The Voice Clarity feature uses AI technology to improve the audio experience on Windows.
"Sudo for Windows," which lets you run elevated commands.
Notepad upgrade with a new AI feature named "CoWriter."

Teams 2.0: The deadline for upgrading has been extended by one year to July 1, 2025.
Teams classic client exits support on July 1, 2024. On July 1, 2025, the Teams classic client reaches "end of availability" and is blocked.

Microsoft Teams (work or school) will be renamed to Microsoft Teams. The personal version on Windows 11 will be called "Microsoft Teams – personal." Users will be able to add and access their additional accounts in the upper right corner of Teams by selecting their profile picture.

Microsoft Teams is deploying "**Voice isolation**" starting in April 2024, which uses AI to filter out background noise during calls and meetings. The feature will be enabled by default, and users can enroll their voice profile to improve audio input quality.

WordPress 6.5.2 has been released. It is a security update to the recently released 6.5 version.
Details here.

T-Mobile Acquires Mint Mobile.

Peacock Premium will rise in price by $2 per month to $7.99, while Premium Plus will increase by $2 to $13.99. They have an exclusive on the upcoming Olympics.

Google rolls out new Android **Find My Device** network.

It will also be possible to locate other items using a compatible Chipolo or Pebblebee Bluetooth tracker tag. Google and Apple are working together to help prevent unwanted tracking using these devices.

AI

"Artificial-intelligence image generators now produce such lifelike output — and the AI apps are improving their accuracy every day — we're seeing an increasing number of surprising, enraging, and manipulative videos and stills. All this forces us to ask, "Is it real, or is it AI?"
AI-generated images have achieved such realism that most people, at first glance, assume that the pictures or videos are real.
Phony images — often called deepfakes or fauxtography — are scrambling free elections around the world. And AI-generated videos that overlay women's faces onto the nude bodies of porn stars can ruin the mortified victims' lives and even cause suicides.
…an international study that found 96% of deepfakes misused people's faces in pornography without their consent, and more than 99% of the victims were women, according to an article by the Centre for International Governance Innovation (CIGI)." From AskWoody newsletter (subscription required).

"The advent of AI threatens to destroy the complex online ecosystem that allows writers, artists, and other creators to reach human audiences." A long, interesting article by Bruce Schneier from his security blog.

SECURITY
If you **use your phone for MultiFactor Authentication (MFA)**, be sure to plan to move this function when you replace your phone.
Do not turn in your old phone for a refund, rebate, or credit until you have completed your migration.
You'll need to work out an arrangement with your provider so you have enough time with both phones to do the work. You must ensure that the new phone handles the MFA requests and that the old phone does not. Then, you can do a factory reset and turn the phone in.
If you have not migrated MFA and the old phone is destroyed or wiped, you may find yourself involved in numerous support cases with services, trying to convince them that you are who you say you are — and that the new phone you're using is actually yours.
How do I export my Authenticator to a new phone for 2FA?.

You want a "lifetime" email address, something that will remain the same as long as you live — and also briefly after that. If you change your address and have not visited every service or website for which you have previously established credentials, you'll end up locked out of those accounts. You'll have an extremely difficult time re-establishing your identity with those services. We recommend keeping a separate email address for authentication. This improves security and provides access if you get locked out of your primary email account(s).
It is the same for cell phones. Changing that number could disconnect you from services you've forgotten about.

iPhoneOS 17.4.1 fixes security issues and addresses complaints about battery life after installing 17.4.

USPS Phishing Traffic: Be sure you are on the real post office website.

Cisco Duo warns third-party data breach exposed SMS MFA logs.
The hacker did not access any contents of the messages or use their access to send messages to customers. However, the stolen message logs contain data that could be used in targeted phishing attacks.

Properly **dispose of printers**:
Your printer may know your Wi-Fi credentials, including the password. Scanners that send files by email may have email credentials. Reset everything to factory defaults, thus wiping out any personal connection to you. If you own the printer, consider destroying the printer's hard disk and not just resetting it to factory default.

DropBox says hackers stole customer data and auth secrets from the eSignature service.

UnitedHealth CEO estimates one-third of Americans could be impacted by Change Healthcare cyberattack. The hacked portal was not protected by multifactor authentication, or MFA, which requires users to verify their identities in at least two different ways.

Kaiser Permanente: Data breach may impact 13.4 million patients.
The data exposed does not include usernames, passwords, Social Security Numbers (SSNs), financial account information, or credit card numbers.

Collection agency **FBCS** warns data breach impacts 1.9 million people.
Data includes: Full name; Social Security Number (SSN); Date of birth; Account information; Driver's license number or ID card.

Okta warns of "unprecedented" credential stuffing attacks on customers.

Cisco warns of large-scale brute-force attacks against VPN services.

Cybercriminals pose as **LastPass** staff to hack password vaults.

AT&T now says the data breach impacted 51 million customers.

LG Smart TVs may be exposed to remote attacks.

The **U.S. Federal Communications Commission** (FCC) levied fines totaling nearly $200 million against the four major carriers — including **AT&T**, **Sprint**, **T-Mobile** , and **Verizon** — for illegally sharing access to customers' location information without consent.

Tracking Firm **LocationSmart** Leaked Location Data for Customers of All Major U.S. Mobile Carriers Without Consent in Real Time Via Its Web Site.

Red Canary report on hacking:

- accounts were the fourth most prevalent attack technique Red Canary detected, affecting three times as many customers in 2023 as in 2022.
- Detections for malicious **email forwarding rules** rose by nearly 600 percent as adversaries compromised email accounts and attempted to modify payroll or wire transfer destinations.
- Half of the threats in the top 10 leveraged malvertising and/or SEO poisoning, some leading to ransomware precursors.
- **humans remained the primary vulnerability** that adversaries took advantage of in 2023.

State highway police were acting lawfully when they forcibly unlocked a suspect's phone using their fingerprint.

Companies and governments are gathering massive amounts of personal data for the purpose of identifying people using facial recognition.

HUMOR

TORIAN GROUP

We welcome Daniel Bernal to our staff. He will be providing desktop support to our clients. He has over 7 years of experience in IT support.

Invoices are now being sent from the email address accounts@toriangroup.com. This will help us better respond to billing questions.

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