Torian Group Times

"Technology with Integrity"

www.toriangroup.com November 2021

The first round of patches is out for **Windows 11**, but there are still problems:
Windows 11 known issues and notifications from Microsoft
Brother confirms Windows 11 printer issues
Some users have reported bizarre results where the new operating system becomes a hybrid of Windows 10 and Windows 11.
Office 2013 won't be supported on Windows 11.
Windows 11 bug may only allow admins to print in some situations.

The US defense department is telling Microsoft that DoD won't buy and use Windows unless SHA-256 is built in, which requires TPM 2.0. This may be the main inspiration for Windows 11.

Large makers and users of PCs, servers, and other devices are pressuring Microsoft not to make hundreds of millions of their deployed units unable to run Windows 11. That's the reason MS added its new, permissive Registry key to allow Windows 11 to run even if it doesn't meet the new TPM chip hardware requirements.

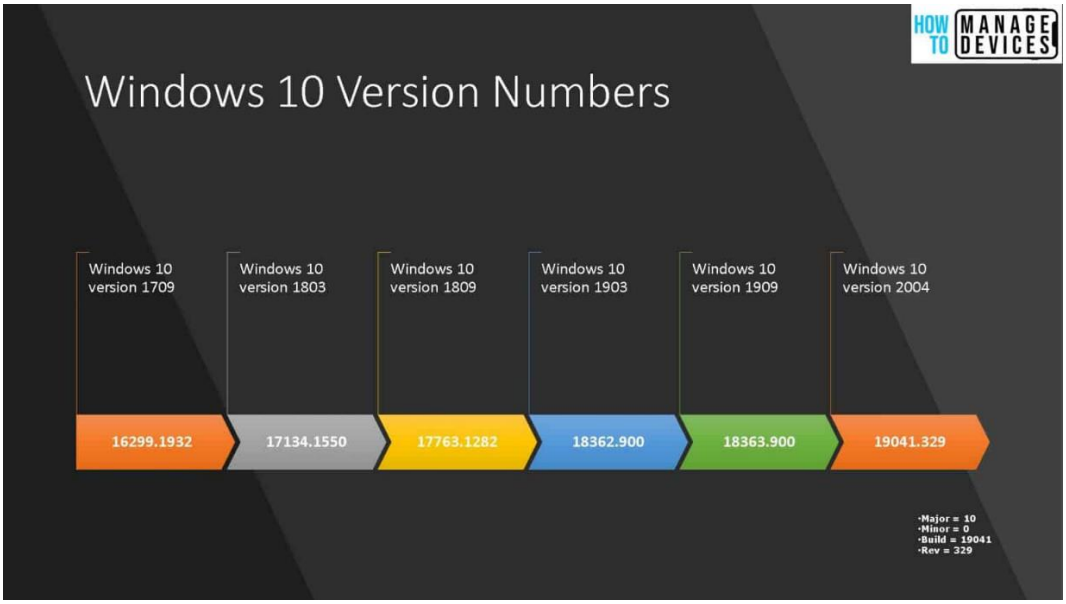
For most businesses, Windows10 is a good choice for now. Let others work out the bugs. Windows 10 is supported through October 2025, so there is no rush to upgrade.

If you are thinking of upgrading to Windows 11, make sure you check with us or your IT staff and plan it out. Test all your software for compatibility and have a full backup.

One compelling benefit of Windows 11 is that it remembers the screen layout when switching between docking stations with multiple monitors.

If you want to install Windows 11 now, you can use the installation assistant.
You can use any Windows 10 product key to activate Windows 11 during installation. Microsoft confirms this behavior is by design.
Windows 11 Home setup requires an Internet connection and a Microsoft account. You won't be able to proceed without either entering an existing Microsoft account address or creating a new one.

The latest Windows 10 update (21H2) is being released now. Again, you must be on a Windows 10 version that was updated in the last 18 months to be receiving critical security updates – 2004, 21H1, or 21H2. Type winver from the search bar to see your Windows 10 version. The first two (2) digits of the Windows10 version are taken from the release year. Windows 10 **21**H1 and **21**H2 are in 20**21**. Prior years are listed below:



All of the Windows 10 21H2 features are already available in 2004, 20H2, and 21H1 versions code, making it a quick and easy update. If your Windows 10 version is 1909 or older, it will be a full reinstall/upgrade of Windows.

Old Versions of Outlook will Stop Connecting to Exchange Online for email on November 1st.

Microsoft has set a definite date, October 1, 2022, to permanently disable Basic Authentication in all Office 365 accounts. It was delayed due to COVID.
POP3, IMAP, and older smartphones will stop connecting.
Switching to "Modern Authentication" is mostly automatic if you are on a subscription plan for Outlook. However, some settings may need to be changed. You should switch to modern authentication sooner rather than later because your data is at risk with basic authentication.

Apple releases iOS 15.1 with SharePlay support. Be sure to stay current to be secure.

Google removes support for FTP and old-gen U2F **security keys** in Chrome 95
If you have an older Titan security key, make sure it will still work.

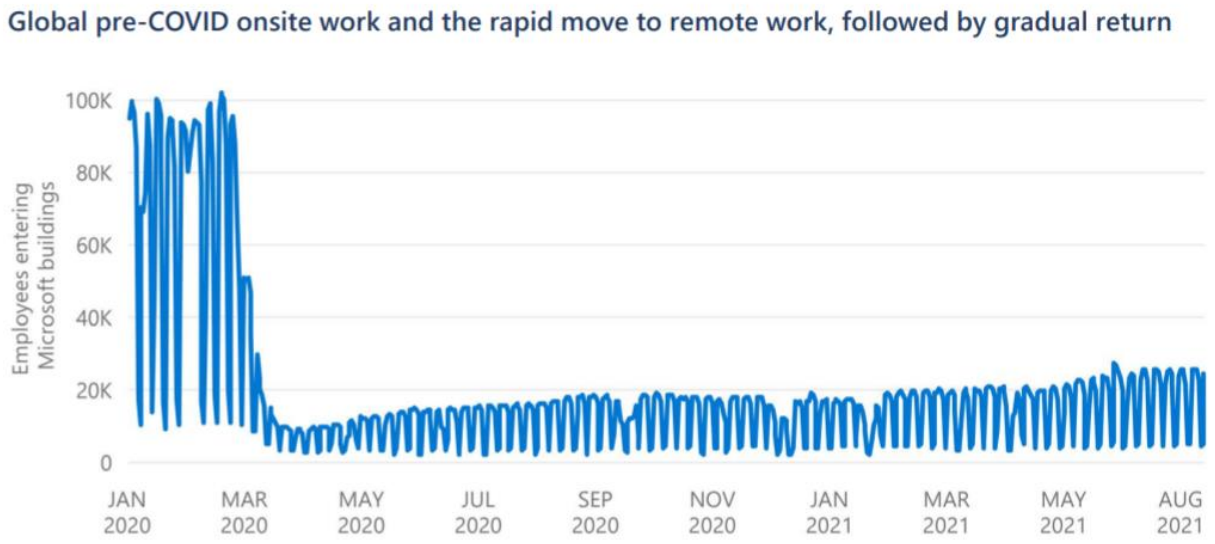
Facebook Corporate is rebranding itself as 'Meta'
The new name doesn't change anything for the main Facebook, Instagram, Messenger, and WhatsApp services, which keep their existing names.

Ray-Ban Stories: **Smart Glasses** that work with **Facebook**
Record the world, taking photos and up to 30-second videos using the capture button or hands-free with Facebook Assistant voice commands.

Comcast Adds Apple TV+ Streaming Service to Xfinity X1 TV service.

COVID

COVID'S **positive impact on technology.**
"…we can exist in the same virtual space, and we can share information instantly. We have learned to define productivity by the results, not by physical location.
…we are being forced to document our business processes so we can reproduce the processes we require with the new technology."
Digital Commerce 360 reports that in 2020, U.S. e-commerce grew by 32.4%.



"Our study (link below) found that 98% of **remote workers** use at least one personal device for work every day. But that's just the tip of the iceberg: Remote workers have an average of eight devices connecting to their home network, including employer-provisioned devices, personal devices, appliances, wearables, and gaming systems. And, on average, each remote worker has three people in their household with devices connecting to the same home network."

"While a simple two-factor authentication, combined with a device compliance check and the security team's ability to continuously monitor these tools, is not entirely sufficient, it will eliminate a majority of enterprise risks…"
Full report (PDF) from Forrester research.

Study Finds Link Between Cybersecurity Attacks and **Remote Work Technology**
Driven by three factors: a lack of visibility into remote employee home networks, the expansion of the software supply chain, and migrating to the cloud.

Ransomware is on the rise due to **home office**.

Is **Remote Work** a Hacker's Paradise?
The giant upheaval brought by the COVID-19 pandemic has led to a staggering 500% increase in the number of attacks.

Beginning this month, the USPS says **standard mail delivery** could take anywhere between two and five days.

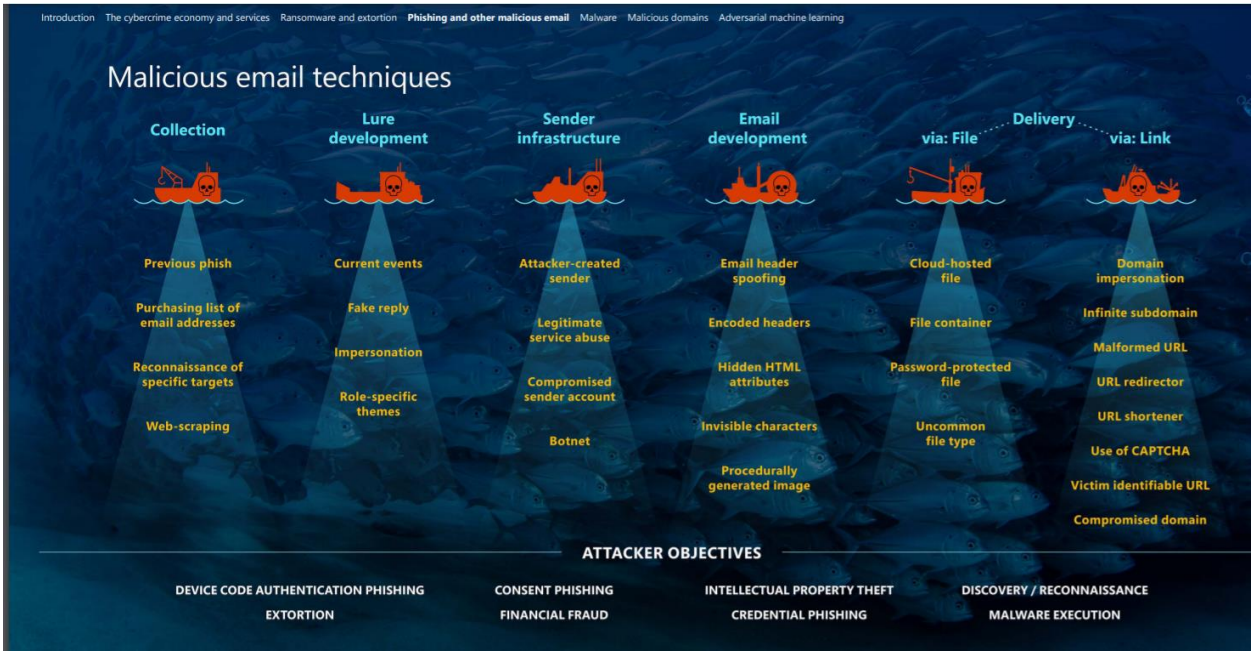
SECURITY

The first Google search result often leads to a virus
Stop before you click anything if a webpage is a "perfect fit" for your original search.
Make sure your antivirus app warns you of hacked websites and downloads.
Make sure antivirus blocks in-memory exploits and doesn't just rely on file scanning.
Make Windows display file extensions so you don't click .js files posing as PDFs.

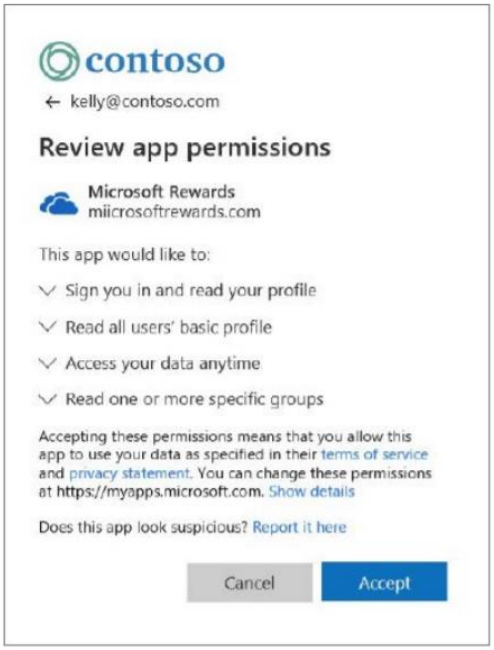
Microsoft Digital Defense Report
In the past year, **web-based phishing attacks** have continued to become more sophisticated.
Phishing kits used by web-based phishing attacks typically use images, context-based content, and other advanced techniques to avoid detection. The language used by attackers has also improved significantly.

Modern kits are sufficiently sophisticated to masquerade as legitimate content in their use of spelling, grammar, and imagery.

One way to make emails look legitimate is by **crafting fake reply emails**. In these cases, the attacker will take the contents of a previous email from a compromised mailbox or create an entirely new email and include it in the body of the email in a way that appears that the new email is a reply.



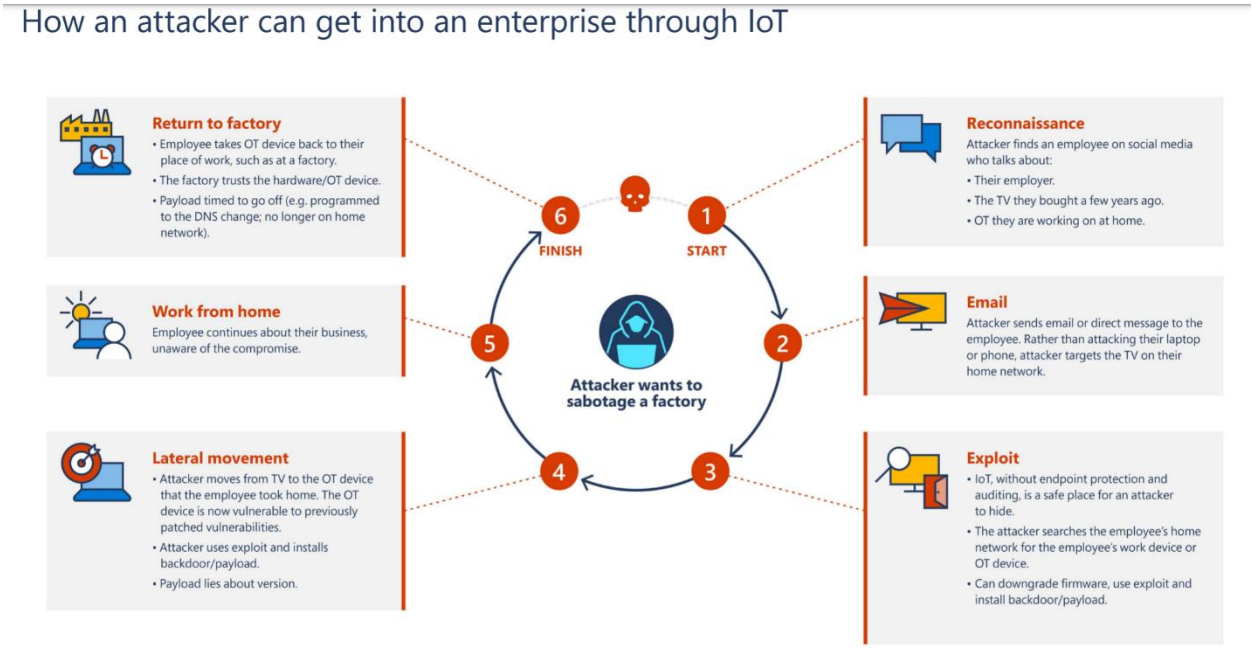
Consent phishing is a bit different. This method attempts to trick users into granting permissions to a malicious attacker-owned application. Strong authentication requirements such as MFA do not prevent attacks that use this technique.



Be cautious of any link that leads to a request for login credentials.
For example, on real DocuSign emails, users are never asked to enter passwords. The request to enter your credentials should be treated as big red flags.

TodayZoo phishing campaign sends links to spoofed Microsoft 365 login pages.
a technique called "zero-point font obfuscation" – HTML text with a zero font size in an email

IoT is short for **Internet of Things** – your Ring doorbell, thermostat, etc.



Factory-set default passwords or weak passwords set by users are the most exploited security vulnerability for IoT devices.

FBI recommends that you keep your IoT devices on a separate network
The FBI says owners of IoT (Internet of Things) devices should isolate this equipment on a separate WiFi network, different from the one they're using for their primary devices, such as laptops, desktops, or smartphones. Any compromise of a "smart" device will not grant an attacker a direct route to a user's primary devices.
Change the device's factory settings from the default password.
Mobile apps support many connected devices on your phone. These apps could be running in the background and using default permissions that you never realized you approved.

Cybersecurity researchers at ESET detected 55 billion new attempts at brute-force password attacks between May and August 2021.

Ransomware has increased 148% year-over-year, with an estimated 2.9 million attacks so far in 2021. The European Union Agency for Cybersecurity (ENISA) recently predicted a fourfold rise in supply chain attacks in 2021 over last year.

Cox Media Group has confirmed it was hit by a ransomware attack in June 2021. The company has sent data breach notification letters to over 800 individuals whose personal data is believed to have been impacted by the attack. Personal information exposed includes names, addresses, Social Security numbers, financial account numbers, health insurance, medical information, and user credentials.

Ransomware hackers steal data from Los Angeles-based Barlow Respiratory Hospital.

As soon as a patient permits their data to leave the health record and head toward a third-party app — like programs that track people's medications, for example — it's easy for hackers to access.
Patient health data is some of the most valuable information to hackers.

Global risks report

More than 50% of the world's population is now online.
Roughly one million more people join the internet each day.
Two-thirds of humanity own a mobile device.
Fourth Industrial Revolution (4IR) technologies are already bringing tremendous economic and societal benefits to much of the global population.

HUMOR

Government: work from home
Lifeguards:

TORIAN GROUP
If you are working from home or have employees working from home and are concerned about security, we can help with planning and suggest tools for insuring the security of your remote workers.

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