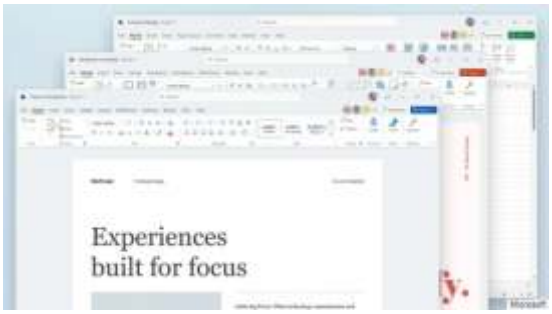
SIM2K
Adapting Technology to Your Business Needs

10•21
Information you can use

SIMformation

Microsoft Releases Office 2021

Microsoft has released Office 2021 for consumers, students, and small businesses as a "non-subscription" version, meaning you can purchase a copy to install on your PC rather than use the on-line version, Office 365. The enterprise and consumer Office 2021 versions have a similar set of new features. While the office suite maintains the same functionality as in the past, Microsoft has improved on some of the features previously found in Office 365. For example, although Microsoft trumpeted live collaboration as a key feature in Office 2016, it turned out that the full real-time collaborative editing experience (what Microsoft calls "co-authoring") was reserved for Office 365 subscribers. The new perpetual release gets a handful of features that were already present in Office 365/Microsoft 365, with many other features left out. And like Office 2016 and 2019, Office 2021 will receive no new features in the future, though it will receive security updates.



Earlier Word and Powerpoint desktop clients for non-subscribers offered a kludgy sort of group collaboration, in which you had to keep saving the shared document to share your changes with others and see the changes they were making. To actually see changes in real time, you had to use the less powerful online versions of Word and PowerPoint. And the Excel 2016 desktop client didn't offer live collaboration to non-subscribers at all.

In Office 2019, real-time co-authoring did come to Word, but not to Excel or PowerPoint. Non-subscribers still had to use Excel Online and PowerPoint Online to collaborate in real time. With Office 2021, real-time co-authoring is finally available in all three desktop clients, as long as the documents you're collaborating on are stored in Microsoft's cloud storage service, OneDrive. Everyone working on the documents sees the changes everyone else makes as they happen. Colored cursors indicate the identity of each person.

And, it was no coincidence that Microsoft released Office 2021 on the same day it began to roll out Windows 11. As shown in the image, Office 2021 is getting a visual update so that it looks much like Windows 11, with rounded windows, a more neutral color palette, and an overall softer look. Despite that new look, Office 2021 still works with Windows 10.

Office 2021 is integrated with the chat and video features of Microsoft Teams. You'll be able to chat and participate in Teams video calls from directly within Office.

Teams has been built into Windows 11, but with Office 2021 you'll be able to use it on Windows 10 and macOS as well. However, note that the version of Teams built into Office 2021 is not the full business version, and lacks features such as channels, being able to search through message archives, and others.

There are several other new features in Office 2021 that were introduced previously in Office 365/Microsoft 365.

Excel gets a variety of new features and functions, including XLOOKUP, which lets you find things in a table or range. Also new to Excel are a number of dynamic arrays, which let you write one formula and have it return an array of values. Excel 2021's new XMATCH function lets you search for an item in an array or range of cells, and then return the item's relative position. You can also use it to return a value in an array.

In PowerPoint, there are improved Record Slide Show capabilities, which include presenter video recording, ink recording, and laser pointer recording.

Outlook gets an improved search called Instant Search, as well as the ability to translate messages into more than 70 languages and to use ink to annotate email messages.

Access (available only with certain enterprise Office editions) gets an updated Linked Table Manager and a new Date/Time Extended data type.

Overall, there are more stock images and icons; a Microsoft Search box for searching content from multiple Office applications; AutoSave, which automatically saves changes to OneDrive; support for the OpenDocument format (ODF) 1.3; and some under-the-hood performance improvements, among other changes.

Prices for Office 2021 remain the same as for Office 2019: Office Home and Student 2021, which includes Word, Excel, PowerPoint, OneNote, and Microsoft Teams, costs $150. Office Home and Business 2021, which includes all that plus Outlook, costs $250 and includes rights to use the apps for business. Each can be used by only a single person. You'll need a Microsoft account to use them. And you will only get five years of support for this version of Office.

Text Messaging System Hacked

A company with an expansive impact on millions, if not billions of cellphone users around the world has quietly disclosed that its systems were breached by hackers five years ago, according to media reports. Though the hacking started in May 2016, the company reportedly only discovered the breach in May 2021. The company, Syniverse, provides backbone services to wireless companies like AT&T, Verizon, T-Mobile, and other international carriers. It processes more than 740 billion texts annually, routing them from one carrier to another.

A former Syniverse employee said that a hacking of that scale could have potentially exposed metadata like phone numbers, the locations of the parties on either end of a call, and the content of text messages. The breach was disclosed in a filing to the U.S. Securities and Exchange Commission on Sept. 27. Documents stated that an unknown "individual or organization gained unauthorized access to databases within its network on several occasions," and more than 235 clients had been confirmed to have been directly affected. Experts say that the five-year hack could have exposed many, many more, given Syniverse's scale.

"Syniverse is a common exchange hub for carriers around the world passing billing info back and forth to each other," said the source, who asked to remain anonymous. "So it inevitably carries sensitive info like call records, data usage records, text messages, etc. [...] The thing is – I don't know exactly what was being exchanged in that environment. One would have to imagine though it easily could be customer records and [personal identifying information] given that Syniverse exchanges call records and other billing details between carriers."

In response, Syniverse released this statement: "As soon as we learned of the unauthorized activity, we implemented our security incident response plan and engaged a top-tier forensics firm to assist with our internal investigation. We also notified and are cooperating with law enforcement. Syniverse has completed a thorough investigation of the incident which revealed that the individual or organization gained unauthorized access to databases within its network on several occasions and that login information allowing access to or from its EDT environment was compromised for certain customers. All EDT customers have had their credentials reset or inactivated, even if their credentials were not impacted by the incident. We have communicated directly with our customers regarding this matter and have concluded that no additional action is required. In addition to resetting customer credentials, we have implemented substantial additional measures to provide increased protection to our systems and customers."

The company stated that it "did not observe any evidence of intent to disrupt its operations or those of its customers and there was no attempt to monetize the unauthorized activity. Syniverse did not experience and does not anticipate that these events will have any material impact on its day-to-day operations or services or its ability to access or process data. Syniverse has maintained, and currently maintains, cyber insurance that it anticipates will cover a substantial portion of its expenditures in investigating and responding to this incident."

But again, we see how cybercriminals can gain access to major data carriers and dip into personal information from users. This is why every company must maintain cyber-awareness and fortify networks against intrusion. Call SIM2K for more information on how we can help you protect against hacking.

Ransomware Attacks and Fallout

Some patient and employee data stolen during a May cyberattack on Eskenazi Health has been released on the dark web, the health care provider has disclosed. Eskenazi Health had said in August was there was no evidence the attack resulted in bank or credit card fraud, but the health care provider is now suggesting people check with credit reporting agencies and get free credit monitoring and identity theft protection.

The stolen data included medical, financial and demographic information of patients and employees, Eskenazi said. The information released on the dark web may include names, dates of birth, ages, addresses, phone numbers, email addresses, medical record numbers, patient account numbers, diagnoses, clinical information, physician names, insurance information, prescriptions, dates of service, driver's license numbers, passport numbers, face photos, Social Security numbers, and credit card information. In the case of deceased patients, this information also may include causes of death and dates of death. People affected by the data breech will receive letters detailing which specific types of their information were involved. The data breech happened around May 19, and the health care provider learned of the breech around Aug. 4. Eskenazi said in late August that it had notified the FBI, which was working with the health care provider on its investigation.

Then, Johnson Memorial Health in Franklin says it was a victim of a cyberattack on October 2 that disabled its computer network. Doctors and nurses at Johnson Memorial Health are having to rely on pen and paper for much of their work following the cyberattack that forced the hospital system to shut down its computer network.

Hackers got into the hospital system's network at 10:31 p.m. Friday. Within a couple minutes, the cybercriminals began infecting the system with ransomware. At 10:40 p.m. the IT Department detected the hack and shut down the computer network a few minutes later. It's still not known if the hackers got hold of any sensitive medical or personal information. The FBI is leading the investigation into the attack. "We don't know what has been compromised we are still doing those diagnostics and trying to determine the extent of the threat," a spokesman said.

And now, at least three U.S. grain distributors' systems have been infected with ransomware, raising concerns that hackers have found an easy target in a vital part of the U.S. food supply chain. The victims are Midwestern grain cooperatives that buy grain from farmers and then process, store and resell it for uses like livestock feed and fuel. The attacks have slowed the distributors' operations, hampering their ability to quickly process grain as it comes in. The timing is particularly bad, as farmers are going into harvest, and this is when they're taking in a large amount of grain and putting out a large amount of grain.

Like many industries, grain production involves heavily digitized operations that were previously done by hand. Hackers who deploy ransomware, locking up their computers and demanding payment may not be able to stop the distributors entirely, but they can severely slow them down. So we see that no industry is shielded from cybercriminals, so we urge you to be aware of this threat.

SIMformation is the monthly newsletter from SIM2K. Information presented here is designed to inform you of trends in the business world affecting information technology. For questions or comments, write SIM2K, 6330 E. 75th St., Suite 214, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

VoIP Telephone System Woes

Over the last weekend of September, Bandwidth.com, the leading VoIP carrier in the US, began experiencing issues with their telephony services. Zultys, SIM2K's telephony partner, is among the many VoIP providers that use Bandwidth for our Zultys Cloud Services customers.

Despite Bandwidth's best efforts to restore full functionality, the issues persisted, affecting Zultys' customers' ability to receive incoming calls and causing poor sound quality. Bandwidth is a premium provider with a stellar track record that hasn't had an incident of significance in over eight years. Zultys utilizes their services extensively because of their known reliability. While Zultys has redundant carriers in their data center, inbound lines use phone numbers provided by Bandwidth. Short of porting numbers to another provider, which can take up to a week, Zultys did not have a way to mitigate the effects of the service issues at hand.

Zultys has been in contact with their support team, who are working feverishly to resolve these problems. While Zultys' own technology and facilities are not problematic, their team is working to minimize the impact of this incident on customers and investigating ways to prevent similar issues from affecting Zultys in the future.

Subsequent reports say that the cause of the issue was a Distributed Denial of Services (DDoS) attack, wherein threat actors will overwhelm servers, portals, and gateways by sending more requests than can be handled and thus making the targeted devices and servers inaccessible to anyone else As VoIP services are commonly routed over the Internet and require their servers and endpoints to be publicly accessible, they are prime targets for DDoS extortion attacks.

Bandwidth at first did not disclose the cause of its outage, however, Bandwidth customers shared a screenshot on Reddit of a customer support message allegedly from a Technical Assistance Center manager who states that a DDoS attack is responsible for the outages.

"Bandwidth continues to experience a DDoS attack which is intermittently impacting our services. Our network operations and engineering teams continue active mitigation efforts to protect our network," reads a screenshot shared on Reddit.

Bandwidth stated the following Monday night that their services had been restored, but it was not clear if the threat actors stopped their attacks or were paid an extortion demand. Unfortunately, it is common for threat actors to briefly halt attacks while they push extortion attempts, and the DDoS attacks renewed again on Tuesday morning.

A few weeks ago, Canada-based VoIP provider VoIP.ms said it was still battling a week-long, massive ransom DDoS attack. The REvil ransomware group demanded a $4.5 million ransom to end the attack. Cloudflare said last month that its system managed to stop the largest reported DDoS attack in July, explaining in a blog post that the attack was 17.2 million requests-per-second, three times larger than any previous one they recorded.

We know our Zultys users have been impacted by this, as we too use Zultys and were affected. This issue should be resolved but we apologize for issues impacting our VoIP partner.

"Random Tid-Bytes"

SIM2K Add New Feedback Tool

SIM2K is adding a new feature on our Support Tickets to permit immediate feedback. This will help us to gauge our services and make any necessary improvements. When a ticket is closed, you will now see:

Along with the "click" there will be an opportunity for you to comment on why you picked the option you did. This way we can easily collect customer feedback to measure customer service by our team members. It will also permit us to promptly respond to issues uncovered by survey. Internally it will permit us to set goals and measure our initial response time and time taken to resolve issues so we can better use our internal resources when addressing specific trouble tickets. We hope you will be frank when using this new feature, and that our service to you will improve from implementing this tool.

iPhone Users - Update Now!

Ignoring software update notifications can be all too easy. However, Apple's latest software is essential to your iPhone and iPad's security. Apple released iOS 15.0.2 and iPadOS 15.0.2 to compatible iPhones and iPads Monday, Oct. 11. At first, the update appeared to be a minor facelift for the device. But, Apple has confirmed that this new update is much more significant than its name would lead you to believe – 15.0.2 delivers a critical security patch for iPhones and iPads. Apple claims that it was made aware of a zero-day exploit on iOS and iPad OS that could allow bad actors to use an app to run arbitrary code with kernel privileges. In summary, that would allow someone to access parts of your iPhone and iPad that normally nobody should have access to, potentially exposing your device to malicious activity. Apple says that it's possible this security flaw has been exploited already, which makes installing the patch on your device all the more urgent. If your device is too old to run iOS 15, keep checking your software updates; if Apple discovers this security vulnerability affects iOS 12 devices as well, it will issue a special patch.

Connected Printers a Risk

The latest way to make sure printer makers "call the shots" is to insist that printers won't print a page unless they have internet connectivity and are linked to an "HP Smart" account. According to HP, you must connect certain printers to an HP Smart account before they'll even work. However, this could be a major security hole in a network. A printer with a built-in, permanent online connection is just asking for trouble.

Instagram Has Adverse Affect on Teens

For years, people have accused social media, and particularly image-driven sites like Instagram, of being bad for young people, particularly young women. It turns that Instagram's owner, Facebook, agrees.

Thirty-two percent of teen girls said that when they felt bad about their bodies, Instagram made them feel worse was one of the findings of internal Instagram researchers which was included in a presentation slide posted to Facebook's internal messaging board in March 2020. It continues: "Comparisons on Instagram can change how young women view and describe themselves."

The Wall Street Journal (WSJ) has reviewed and revealed the contents of such slides in its latest instalment in the The Facebook Files, a WSJ series of investigative articles based on "internal Facebook documents, including research reports, online employee discussions and drafts of presentations to senior management." Sometimes, included in these reports are findings from other companies the social network giant owns, like Instagram and WhatsApp.

Concerned parents and carers who may have observed or heard something from their teen who is being affected by Instagram would likely get confirmation on what they already know: Instagram is not helping with their body issues and sense of self at all. What may be more shocking to them, is that Facebook knows this too.

According to the Journal, more than 40 percent of Instagram users are 22 years old or younger, with about 22 million teens logging on to Instagram in the US each day. The social media giant is said to have repeatedly found that Instagram is harming its young users, especially teenage girls.

It reports that the research conducted by Facebook revealed that Instagram makes body image issues worse for about one in three girls; that teenagers blame Instagram for increases in the rate of anxiety and depression; and that one in five teenagers said that Instagram makes them feel worse about themselves. The slides also revealed that a percentage of female teens in the US and UK have suicidal thoughts over what they see on Instagram.

Teen girls aren't the only ones affected though. In Facebook's 2019 research report, it found that 14% of boys in the US had said that Instagram made them feel bad about themselves. The following year, they found that 40% of teen boys experienced negative social comparisons. This, the researchers have concluded, is a problem specific to Instagram.

"Social comparison is worse on Instagram," is what Facebook noted after doing a deep dive into body image issues in teen girls in 2020. What Instagram users tend to do is share only the best and most perfect photos and moments, which can trigger negative reactions, and may even lead to eating disorders, an unhealthy outlook towards themselves, and depression.

The Journal claims that Facebook's internal documents reveal that it has done little to address these issues, and even downplays these in public. For example, Adam Mosseri, head of Instagram, has told reporters that the research suggests the app's effects on teen well-being is, "quite small". "In no way do I mean to diminish these issues…. Some of the issues mentioned in this story aren't necessarily widespread, but their impact on people may be huge," Mosseri further said in an interview.

Mark Zuckerberg, CEO of Facebook, said at a March 2021 congressional hearing that, "The research that we've seen is that using social apps to connect with other people can have positive mental-health benefits," which only highlights one side of the story while failing to mention the other.

Instagram's response to the WSJ says the Journal focuses on "a limited set of findings and casts them in a negative light". The company touts its research and efforts to make things better for every user on Instagram, writing that "It demonstrates our commitment to understanding complex and difficult issues young people may struggle with, and informs all the work we do to help those experiencing these issues."

The Journal claims that Facebook executives are struggling to find ways to reduce Instagram's harm while keeping people on the platform. Project Daisy, for example, was a pilot program created as a potential solution to keeping kids from feeling anxious and having negative feelings, based on a focus group feedback, when they see "like" counts. In Project Daisy, "like" counts are hidden. However, the results of the program have revealed that it didn't improve teens' lives. Project Daisy was rolled out, nonetheless, with executives noting in an internal discussion that this, essentially, is just for show.

Mosseri acknowledges in an interview with the Journal that he doesn't think there is a clear-cut solution to fixing Instagram. "I think anything and everything should be on the table," he said, "But we have to be honest and embrace that there's trade-offs here. It's not as simple as turning something off and thinking it gets better, because often you can make things worse unintentionally".

Perhaps what stands out most from the reporting is not a single statistic, or how negatively Instagram has been affecting teens for years, or even that Facebook is well aware of the negative side of its social media empire, but the fact that the teens who are reporting problems are finding it really difficult to unplug or quit the app. The message to parents is: Do not expect Instagram or Facebook to do this for you any time soon, because these online services were engineered to make users want to come back for more, even when they know it's not good for them.

As computer scientist Dr. Cal Newport said in his memorable TED Talk, *Why you should quit social media*, social media is designed to provide a constant flow of small, intermittent rewards, just like a slot machine. "It's one thing to spend a couple of hours at a slot machine in Las Vegas, but if you bring one with you, and you pull that handle all day long, from when you wake up to when you go to bed: We're not wired for that" was his message.

The just-released Facebook documents from a whistleblower alleging that the platform encouraged hateful posts to boost "eyeballs" and subsequent ad revenue is another hit to social media. Perhaps now people will look at these revelations and see social media in a new light and temper their addictions.

SIM2K
6330 E 75th St., Suite 214
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com