SIM2K
Adapting Technology to Your Business Needs

4•20
Information you can use

SIMformation

Remembering Mark Finegan

It is with heavy hearts we remember Mark Finegan in this issue of SIMformation. Mark passed away on March 30th after a brief hospitalization. The current social restrictions in place due to corona virus/COVID-19 make a celebration and closure especially difficult. Many of our clients have relationships with Mark going back decades, some almost 45 years – our thoughts and prayers are with you in this time.

We thought it might be healing to take a little jaunt down memory lane. After growing up and going to school in Indiana, Mark created "Strategic Information Management" in 1985 after coming out of the telecom industry. The original office was in his home in Noblesville. He sold accounting software to mostly non-profits. From there, he moved to an office on Alabama St. before moving back to the northeast side of town. In the early 90's, Mark and a group of former Ameritech employees with similar small businesses around the country merged to become "Indetec International" where they continued providing IT services as well as began cost modeling to telecommunications companies around the world. When the "dot com bubble" burst in the late 90's, the assets of SIM were bought back from Indetec and "SIM2K – Systems and Solutions for the next millennium" was formed in 1999. From there, SIM2K grew into the IT Consultant and Managed Service Provider we are today.

Mark is survived by his wife Christy, who many of you know and speak to when you call SIM2K. Their oldest son Ben mans the helm at SIM2K. Their middle son Dan, his wife and their four children reside in North Carolina. Their youngest son David is an artist in Indianapolis.

He was a husband, a father, a brother, a friend, a business owner, a veteran, a mentor and so much more to so many people over the years.

There are no funeral or memorial services at this time. In lieu of flowers, a memorial at the National Kidney Foundation has been created in his honor.

https://team.kidney.org/campaign/Mark-Finegan-Memorial

He will be missed!

– The SIM2K family

Free Conferencing Tools

SIM2K is offering our clients a special offer for the remainder of the year. In light of the COVID-19 pandemic that is affecting communities and businesses worldwide, our provisioning partner Intermedia is committed to decreasing the risk and prioritizing the well-being of our community of stakeholders. To help businesses and organizations that need to support remote workers with effective communications and productivity tools, Intermedia is now offering its AnyMeeting® video conferencing and webinar service at no cost through December 31, 2020.

AnyMeeting Video Conferencing Pro permits remote workers to hold global on-line meetings using high-definition video and audio conferencing, screen sharing, call recording, chats, note-taking and more, with no restriction on meeting length. AnyMeeting is HIPAA compliant and offers end-to-end encryption for all meetings using WebRTC standards.

Webinar Pro enables companies to hold larger live broadcast events for up to 200 people, such as corporate all-hands meetings, webinars, lectures, religious services and other virtual events. Presenters can use video, audio and screen sharing to market products and services to audiences anywhere. Build personal connections, engagement, and trust by simply allowing attendees to see the presenter in real-time and engage through Q&A, Emoji's, and live Polls and more. Reach a broader audience and grow your business with this easy-to-use service that connects and engages anyone, on any device, from anywhere. One license for this will be provide per account.

If your business is interested in either of these products, please call SIM2K for more information and to schedule installation. We have been an Intermedia partner for many years, and can vouch for their services, and believe this is an excellent offer to help your business stay in touch either with employees or your clients. At the end of 2020, pricing will be applied, and we can discuss costs if you wish to continue using these services. Call Today!

Watch Out for Covid-19 Scams

The number of scams, threats, and malware campaigns taking advantage of public concern over the coronavirus is increasing each day. As a result, security companies are monitoring e-mails within their spam honeypot to flag such threats and make sure users are protected.

One such phishing campaign impersonates the World Health Organization (WHO) and promises the latest on “corona-virus.” Right off the bat, the incorrect use of a hyphen in “coronavirus” in the subject line could tip off users with a critical eye for grammar. However, since WHO are often touted as a trustworthy and authoritative resource, many will be tempted to open the e-mail.

In this particular campaign, the cybercriminals use a fake e-book as a lure, claiming the “My Health E-book” includes complete research on the global pandemic, as well as guidance on how to protect children and businesses. The criminals behind this scheme try to trick victims into opening the attachment, contained in a zip file, by offering teaser content within the body of the e-mail. The e-mail content goes on to tell readers that they can download and access the e-book from Windows computers only.

Instead, as soon as they execute the file inside the MyHealth-Ebook.zip archive, malware will be downloaded onto their computers. As seen in the previous wave of spam, the malicious code is a downloader program called GuLoader.

GuLoader is used to load the real payload, an information-stealing Trojan called FormBook, stored in encoded format on Google Drive. Formbook is one of the most popular info-stealers, thanks to its simplicity and its wide range of capabilities, including swiping content from the Windows clipboard, keylogging, and stealing browser data. Stolen data is sent back to a command and control server maintained by the threat actors.

While the threat actors are improving on the campaign’s sophistication by building reputable-sounding content within the body of the email, a closer examination reveals small grammatical errors in their copy. This combined with other minor formatting and grammar mistakes, as well as a mix-and-match selection of fonts make this clever phishing scheme, upon closer examination, a dud. Still, many have fallen for far more obvious ploys.

With a huge swatch of the population now confined to their homes but working remotely, the risk of infecting a highly-distributed network is increasing. That’s why it’s more important than ever to use a discerning eye when opening work or personal e-mails, as employee negligence is one of the top indicators for successful cyberattack/data breach.

We have a story on page 4 with tips for now “work at home” users that will help guide you to security practices for home devices. Whether you are connecting to your business network through a VPN or other connection, having access to your company’s files means that a hacker could have the same access if you are not vigilant about your security. Call SIM2K for more help in ensuring your new dining room table office has the security you need.

Microsoft Throttles Office 365 Apps

It's not surprising with many working and studying remotely as a result of Covid-19 that the demand for cloud services is on the increase. Microsoft has been monitoring that situation as it pertains to Office 365 applications, and has started to take action to preserve overall performance by throttling back some services.

On March 16, Microsoft posted a notice on Office 365 admin dashboards warning about “temporary feature adjustments” that the company would take. Microsoft did say that these would impact “non-essential capabilities” that would not have a significant impact on users’ experiences. Among some of the changes would be things like how often services check for presence; intervals in which other parties typing are displayed; and video resolution quality.

Then, on March 24, Microsoft further added that Office 365 users could expect other “temporary changes” such as:

One Note:

- OneNote in Teams will be read-only for commercial tenants, excluding EDU. Users can go to OneNote for the web for editing.
- Download size and sync frequency of file attachments has been changed.

SharePoint:

- Rescheduling specific backend operations to regional evening and weekend business hours. Impacted capabilities include migration, DLP and delays in file management after uploading a new file, video or image.
- Reduced video resolution for playback videos

Stream:

- People timeline has been disabled for newly uploaded videos. Pre-existing videos will not be impacted.

Industry observers said that service degradations and problems were not surprising given the demand caused by new users of Microsoft365/Office 365 services. Microsoft noted that the number of daily users of Teams, the group collaboration service, was up significantly, hitting 44 million users. Associated services, such as SharePoint Onoline, OneDrive for Business, OneNote and Stream are also experiencing increased demand.

Microsoft officials said they will continue to apprise customers of further restrictions and tweaks they will be making to their services to continue to meet demand.

So if you are now an “at-home” worker using Office 365 or any other Cloud-based application, you may expect to see slow response or limits on what tasks you can complete as the world now is pushing these services to the limit.

SIM2K will continue to monitor Microsoft’s position on its’ Cloud services and if we see any more throttling, we will advise you accordingly. However, there is little we can do to rectify this situation as this is controlled by Microsoft.

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 336, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

Improvements to Windows 10

Microsoft's next Windows 10 feature update, code-named 20H1, is coming very soon. We don't know exactly when it will be released or what its official name will be, but the version number is 2004 (for 2020/April.) Unlike some previous Windows 10 feature updates, version 2004 doesn't introduce a bunch of major new features. But it does include several useful tweaks to the ways business users interact with the OS, such as the option of signing in without a password and a Cortana reboot that puts productivity first.

Cortana has undergone a soft reboot in version 2004. Microsoft has shifted the focus of its digital assistant away from home users to office workers. In fact, Microsoft has killed many of Cortana's features and functions that were meant for the home user, such as the ability to control music apps and home tech devices. Now the emphasis is on using Cortana to assist you for work, mostly with Office 365. You can speak to Cortana or type into its query box for personal productivity tasks such as finding a document, sending an e-mail, or scheduling a meeting. You can also request that it add an item to a to-do list, set a reminder, or update you on your schedule. Instead of being tied to the taskbar, the "new" Cortana acts more like a standard app, opening in its own window that can be moved and resized. This version of Cortana will be available first for Windows 10 users in the U.S.

Passwordless sign-ins will let you use the Windows Hello biometric security system to sign into Microsoft services using facial recognition (assuming you have a webcam on your device), your fingerprint (assuming you have a fingerprint reader), or through a PIN. This means when you sign into Windows 10, Office 365, Outlook.com or other Microsoft services you can use one of these ways rather than the "user ID/Password" challenge.

There is a new version of the Calendar app in Windows 10 2004 with a new layout that brings attention to your day's events better, and a new pane in Month view showing all your events.

File Explorer's search function is now integrated with Windows Search, the search box on the taskbar. You can use File Explorer to search for your documents in OneDrive, too, if you use Microsoft's cloud storage service. Also, when you click inside the File Explorer search box, a drop-down menu opens below the box listing suggested files that you may be looking for. If you type in letters or words, this list drills down to filenames that have these letters or words. You can launch a file on this list by clicking it. Or, to go to the directory where a file is located in File Explorer, right-click on it and select "Open file location" from the menu that opens.

It will now be easier to connect devices and peripherals to your Windows 10 PC through Bluetooth. When a Bluetooth device is nearby and set to pairing mode, a card for it pops up in the lower-right corner of your screen where you can connect the device to your Windows 10 PC, You no longer need to go to Settings to make the pairing. The notification also shows the name of the Bluetooth device and its category (headphones, keyboard, mouse, etc.).

And if you use Snip for screen captures, you can now zoom in or out of a screenshot by pressing Ctrl and scrolling a mouse wheel, using a touchscreen, or pressing Ctrl and the + and - keys.

SIM2K will be watching for the release of this update and checking it for bugs before we recommend installation.

"Random Tid-Bytes"

Updates Put on Hold

Citing "current global circumstances" rather than outright naming the COVID-19 pandemic and its upturning of, well, virtually everything, Microsoft said it would not upgrade the current Edge 80 to the next version, Edge 81. Microsoft is following Google's lead, telling customers that it was suspending releases of its Edge browser. "As the situation evolves," Microsoft said, it will inform customers of other changes, and presumably when it will resume Edge refreshes. Google made a similar announcement mid-March, telling Chrome users it had stopped upgrading the browser a day after it was due to move from version 80 to 81. Google didn't say COVID-19 triggered the decision either, asserting that the "adjusted work schedule" was to blame. Both decisions were, of course, clearly caused by the pandemic and its disruptions, including vast numbers of company employees sent home to work there. Mozilla has not said if it would maintain its every-four-week schedule of upgrading Firefox, which last month accounted for far less browser share than Chrome but more than Edge. The next update, to Firefox 75, is scheduled for early April.

Microsoft Debuts Cloud Printing Service

Microsoft this week opened a private preview of its all-cloud Universal Print service to customers running Windows 10 Enterprise or Windows 10 Education. Those customers also require an available Azure Active Directory (AAD) tenant, to which the personal computers accessing the cloud printing preview must be joined. Microsoft described Universal Print as "a Microsoft 365 subscription-based service;" it was unclear whether that meant only customers licensing Microsoft 365 – the subscription bundling Windows 10, Office 365 and a host of management and security tools – would be eligible for the preview, the final when it debuts or both. Universal Print allows printing without direct device-to-printer links, thus enabling printing from mobile devices such as smartphones and tablets without printer servers to manage printer access and handle department billing, and centralizes printing so that swaths of users can share more sophisticated printers. However, one of the barriers to cloud-based printing is that printer makers must support the functionality of each variation. That typically has meant a lag between the introduction of, say, Google's Cloud Print and Apple's AirPrint, and the appearance of supportive hardware. Microsoft's Universal Print will fight the same headwind. However, this may be beneficial for, say, schools using a centralized printer for student output rather than needing printers in every classroom.

New Tools for Cloud Security

High-profile breaches have sparked interest in an emerging class of security software. The technology, named cloud security posture management (CSPM), scours cloud environments and alerts staff to configuration issues and compliance risks, most of which stem from human error, such as what occurred at Capital One in 2019, when a former Amazon Web Services (AWS) employee exploited a misconfigured firewall at AWS and obtained personal information. Common misconfiguration mistakes expose cloud storage folders and data transfer protocols accessible via the Internet. Previously, staff had to use manual checks or self-developed scripts to detect these errors. Automating these checks in a standardized way will go a long way to helping companies using Cloud storage to check for human errors in the configuration of their Cloud services.

Security Tips for Those Now Working from Home

The coronavirus pandemic and resulting lockdown have forced a large number of employees into unfamiliar territory – not just remote work, but full-time working from home (WFH). Given these circumstances, we thought it would be helpful to share some security tips for now home-based workers, reminding you take precautions.

WFH physical security

First, make sure your work devices are physically safe, and that you avoid offering unauthorized views of confidential information. Here are a few ways to shore up physical security:

- If you need to leave your home for supplies or other reasons, make sure your work devices are either shut down or locked—including any mobile phones you might use to check email or make work phone calls.
- If you live with a roommate or young children, be sure to lock your computer even when you step away for just a bit. Don't tempt your roommates or family members by leaving your work open. This is true even for the workplace, so it is imperative for WFH.
- If you can't carve out a separate work space in your home, be sure to collect your devices at the end of your workday and store them someplace out of sight. This will not only keep them from being accidentally opened or stolen, but will also help separating your work life from your home life.

System access

You may now have to work on your personal laptop – one that you didn't think much about securing before coronavirus "hunker in" mandate. You need to guard against unauthorized access. If you think cybercriminals will refrain from attacking remote workers, you are mistaken.

- Access to the your computer's desktop should at least be password protected, and the password should be a strong one. If the system is stolen, this will keep the thief from easily accessing company information.
- If office network permissions previously gave you full access to work software, now you may be required to enter a variety of passwords to gain access. If you do not already use a single sign-on service, consider using a password manager rather than having a written list of passwords on your desk.
- Encryption also helps protect information on stolen or compromised computers. Check whether data encryption is active on your work machine. If you're not sure, ask SIM2K whether you have it.
- If you're connecting your work computer to your home network, make sure you don't make it visible to other computers in the network. If added to the HomeGroup, make sure the option to share files is set to off.

Separate work and personal devices

Do you have a child being homeschooled now and turning in digital assignments? Are you ordering groceries and food online to avoid stores? Don't mingle these tasks with your work device.

- While it may seem overkill to switch back and forth between the two, do your best to at least keep your main work computer and your main home computer separate (if you have more than one such device). If you can do the same for your mobile devices – even better. The more programs and software you install, the more potential vulnerabilities you introduce.
- Don't pay your home bills on the same computer you compile work spreadsheets. You can not only create confusion for yourself, but also end up compromising your personal information when a cybercriminal was looking to breach your company.
- Don't send work-related emails from your private email address and vice versa. Not only does it look unprofessional, but you are weaving a web that might be hard to untangle once the normal office routine resumes.

Secure connections

Make sure you have access to your organization's cloud infrastructure and can tunnel in through a VPN with encryption. Secure your home Wi-Fi with a strong password, in case VPN isn't an option or if it fails for some reason. Access to the settings on your home router should be password protected as well. Be sure to change the default password it came with.

Cybersecurity best practices

Other security precautions may not be all that different from those you should be practicing in the office, but they are easy to forget when you are working in your own home environment. A few of the most important:

- Be wary of phishing e-mails. There will be many going around trying to capitalize on fear related to the coronavirus, questions about isolation and its psychological impacts, or even pretending to offer advice or health information. Scan those e-mails with a sharp eye and do not open attachments unless they're from a known, trusted source.
- Related to phishing: there may be a rise in Business E-mail Compromise fraud. Your organization may be sending you many e-mails and missives about new workflows, processes, or reassurances to employees. Watch out for those disguising themselves as high-ranking employees and pay close attention to the actual e-mail address of senders.

Other security precautions

Your system may require additional security software now that it has left the safer environment of your organization's network. Check with SIM2K on whether you should install additional solutions. If you're using an Android device for work, should you download security software that can protect your phone? (IPhone users - iOS doesn't allow outside antivirus vendors.)

How will data storage and backup work? Can you save and back up your local files to a corporate cloud solution? Find out which one they prefer you to use in your specific role.

Call SIM2K if you have questions about security for your work at home devices and connections to your company network.

SIM2K
6330 E 75th St., Suite 336
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com