Computer Bytes – April 2018 – WebEx & "SCARE" Screen Bug

Provided By: Harv Oliver, HANDS-ON Consultations

Hello Friends & Associates –

"April showers bring May flowers…". We sure could use that old saying to kick in. In the meantime we are enjoying some beautiful weather. Following is our current sharing of information regarding activities in the computer world.

UPDATE: WEBEX VULNERABILITY IDENTIFIED - What Is Happening: A WebEx vulnerability has been identified that can result in a hacker getting access to your system through compromised WebEx meeting links. The most basic description of WebEx is it's an "online" tool that allows for video and/or audio online conferencing. I realize many of you may not have this tool or even be familiar with it. That said, some are, and if you're not, it doesn't mean you could not somehow be compromised so you may just want to take note and be aware.

WHAT YOU SHOULD DO - If you receive a WebEx invitation from someone you do not know, **delete it**. Do not open it, as this will activate the vulnerability and allow the sender to access your system. *Do not click on WebEx Links from unknown senders.*

Supporting Points: - The vulnerability impacts the WebEx Meeting Center software. - You can still use WebEx, just do not click on links that have been sent to you by people you do not know through email or through Outlook. - If you access a meeting link from a web browser, there is no impact.

On another note of scams…

I've mentioned this in my articles numerous times but this problem is still extremely present and active (I average at least 5 clients a week hit by this), and so I feel justifies another update.

When you're "online" and go to a web page, within seconds a screen with a warning not to turn off the computer and call a phone number immediately pops up. It's very scary to those who are not informed and it basically states "the world will come to an end" if you close the window. It won't. In some cases users could just close the immediate window and move on, others could not move forward/backward – just locked up. For the most part this seems to be a 'pop-up' scare tactic to get your money. In other cases it did seem to install other malware we had to run cleanup on to get rid of. The bulk of our clients called us first and we assisted them without going down the wrong path of hooking up with the crooks doing this.

DO NOT CALL AND DO NOT PAY AND DO NOT LET THEM LOG INTO YOUR COMPUTER!

No reputable service would ever do this. The misleading part is if you do let them in, they run bogus files that display supposed errors meant to scare – and unfortunately if you're not familiar with the practices it can be scary. THEY are the bug! Again, DO NOT GIVE THEM ANY MONEY!!! Call your local IT support. The cost will be less if you do have an issue and you're working with someone you can trust and 'see'.

This again brings up the never-ending recommendation of keeping anti-virus/anti-malware tools up to date. Some of these annoyances can still occur but you want to do your best to minimize them.

NOTE: Our sharing of information within articles includes suggestions and tips. USE AND/OR APPLY AT YOUR OWN RISK. If you have any questions or concerns, please contact our offices for professional service/guidance.

Until next time, don't forget your backups! For more information, contact Harv Oliver, HANDS-ON Consultations, (805) 524-5278, www.hocsupport.com