ZOOM BRINGS PEOPLE TOGETHER—BUT IS IT SAFE?

Published on May 15, 2020

Nick Cianci
President, Compass Total Benefit Solutions, LLC

The mass transition to working from home has pushed many businesses to communicate with virtual collaboration applications. It has also significantly increased the number of people using these applications to keep in touch with friends and family. We're talking Webex, Microsoft Teams, Slack, GoToMeeting, and yes, the infamous Zoom. So, why has Zoom gotten such a bad rap from media outlets, and is it safe for residents of skilled nursing and assisted living facilities to use to connect with their families?

Headlines like, "The Dangers of Zoombombing," "Zoom is malware," and even "Zoom Accounts Sold on Hacker Forums on the Dark Web" have been circulating in respected media outlets. The intonation provokes caution, if not fear.

So, is there merit to these claims? In short, yes. But it is more complicated than that. As consumers of media, we always need to be aware of hyperbole. Even the term "Zoombombing" sounds more dangerous than it is and is often a result of user error.

i.e., If you turn on the setting "embed passwords in meeting link for one-click join," it sounds like you are simplifying the user experience while still maintaining the security of a password-protected room. In reality, this allows software programs like zWarDial to scan for entry. Krebson Security states:

"[A] single instance of zWarDial can find approximately 100 meetings per hour, but ... multiple instances of the tool running in parallel could probably discover most of the open Zoom meetings on any given day."

Let's take a step back for perspective. Zoom CEO, Eric Yuan, told NBC News, " [W]e did not design the product with the foresight that, in a matter of weeks, every person in the world would suddenly be working, studying, and socializing from home… presenting us with challenges, we did not anticipate when the platform was conceived." The response from Yuan may sound like an excuse for a platform whose security was perhaps underdeveloped. In reality, Zoom jumped from 10 million users to 200 million users overnight.

We live in a world where fraud and cybercrime are not going away. The more technology advances, the more phishing, and scams will continue to evolve. With tech companies, it's not always a matter of scrutinizing what has happened in the past, but how they react and respond moving forward.

"You know, lesson learned... We've got to double down on privacy, double down on security," Yuan said.

As Zoom and other virtual web conferencing applications continue to dial in security measures, here is a checklist from LMG Security to help dial in your settings and security practices.

1. Ensure, "require a password when scheduling new meetings."
2. Ensure, "require a password for instant meetings."
3. Ensure, "require a password for participants joining by phone."
4. Turn off, "embed passwords in meeting link for one-click join."
5. Ensure "use personal meeting ID when scheduling a meeting" and "use Personal Meeting ID when starting an instant meeting" are off.
6. Don't post-meeting links to public places.
7. Utilize the "waiting room" feature to ensure only authorized users join the call
8. Ensure "Join before host" is disabled
9. Restrict remote control to host only
10. Make sure hosts are familiar with "mute," "hold," and similar controls.

11. Use a strong password, at least 14 characters.

When in doubt, look to your IT department or a remote security services company to navigate cybersecurity in your business. Help residents ensure their accounts are set up with the proper security settings so they, too, can enjoy safer social distancing.

Sherri Davidoff, CEO of LMG Security, encourages listeners of a Beazley Academy webinar to remember, "there's no such thing as a free lunch." Software applications that offer free versions of their services may reserve essential security measures for paid customers. Keep an eye on the terms and conditions and recognize who owns the data collected from users.

The golden rule for security is to remember, "Hackers don't break-in, they log in," Bret Arsenault, Microsoft Executive.