Published on *The National Law Review* https://natlawreview.com

Hackers Spoofing Zoom to Obtain Credentials and Passwords

Article By:

Linn F. Freedman

After incidents of Zoom “bombing,” including a recent intrusion by hackers to disrupt a church service with foul content (don’t these guys have better things to do?), it has been reported that hackers are now taking advantage of the surge in the use of Zoom for videoconferencing to spoof Zoom invites to try to obtain users’ credentials.

First, when using any videoconferencing platform, you may wish to consider requiring that a password be used to get into the conference in order to reduce the risk of Zoom bombing.

Second, when receiving a videoconference invitation, as with any other email you receive, treat it like a potential phishing email that is a scam. Check to see who sent it to you, that it is someone you know and trust, and that the email address is correct, and don’t click on the invitation unless you are expecting it. Further, no videoconference invitation is going to request your user name and password, so just as you would not give your user name and password to a random email phishing for information, the same is true for accepting Zoom or other videoconferencing platform invitations.

Finally, when logging in to a videoconference, check that you are logging in to the actual site, and not a fake link that has been sent by a hacker.

Hackers are creative and up to speed on the technology businesses are using, particularly during the pandemic. Be aware that they are going to use all their creativity in new ways to try to spoof and scam you. Educate your employees on the newest tricks and encourage their continued vigilance to avoid becoming a victim of old tricks using new technology.

National Law Review, Volume X, Number 135