NKU | OFFICE OF Information Technology

Zoom Security: Remote Teaching Myth vs. Reality

Zoom web conferencing has recently risen to the forefront of the news with concerns for cybersecurity and privacy. NKU wants to reassure our Zoom users that we have put controls in place to address these concerns.

The following are the main concerns raised in recent weeks and, where applicable, how NKU has mitigated these concerns:

Zoom's privacy policy allows them to share information with third parties

Although Zoom publishes a privacy policy applicable to their individual customers, as an institutional account, NKU uses an integrated solution to deliver Zoom services for remote teaching. As part of the integrated Canvas solution, the information shared with Zoom includes: NKU credentials (first and last name, and email address), participant's role (instructor or student) and course name. The updated Zoom privacy statement was reviewed and accepted by NKU's Office of Legal Affairs and General Counsel on April 2, 2020.

The Zoom application on iOS (iPhone) shares private information with Facebook, even if the user has no Facebook account

This issue was reported on March 25 and repaired on March 27, 2020. Zoom claimed that they were not made aware of the data which was shared. Upon further review, it was demonstrated that the data collected by Facebook did not include information and activities related to meetings, such as attendee names or notes. However, it did include: details about the user's device, such as the device model, IP address, phone carrier, and Advertiser ID (a unique advertising identifier created by the user's device which companies can use to target advertising).

Zoom meetings can be accessed by malicious parties, which can then display inappropriate content to other participants (aka "Zoom-bombing")

While this is a known issue in web conferencing tools, it is usually managed by protecting the meeting configuration. There are several ways to achieve this:

- Create a meeting password
- Restrict participants to an approved list
- Do not disclose the meeting hyperlink in public forums (such as social media)
- Use the waiting room feature
- Prevent participants from sharing their screen during the session (by adjusting the security settings)

As part of NKU's implementation, any Zoom meeting created has default settings to restrict the ability for participants to share their screen, however hosts have the ability to change these settings as the default, or by meeting.

Additional guidance is available for instructors on the NKU Virtual Campus site in the Zoom Bombing section.

Questions?
Contact the IT Help Desk at https://inside.nku.edu/it/help.html or (859) 572-6911.

Updated: 4/9/2020

NKU | OFFICE OF Information Technology

The Zoom application on MacOS could allow a local user, without privileges, to install malware and control the camera and microphone (ZoomDoom)

This "zero-day" vulnerability (a vulnerability disclosed publicly before being submitted to the software editor for a fix) was published on March 31, 2020 and repaired on April 1, 2020. It required the cyber attacker to have local access to the computer (locally or through a remote desktop connection) to increase their privileges.

As with all software vendors, vulnerabilities do exist in Zoom. When evaluating a software solution's security, NKU's security specialists not only evaluate the number of vulnerabilities, but the timeliness of the software manufacturer's response in addressing them.

The Zoom application on Windows allows cyber attackers to steal user credentials (account and password information)

This vulnerability was published on March 31, 2020 and repaired on April 1, 2020. It was believed that once exploited, the cyber attacker had direct access to the user's credentials (account and password). In reality, the cyber attacker had access to an encrypted password, which they would still need to decrypt (i.e., crack). The vulnerability to these types of attacks relied on a user clicking a malicious link. As always, exercise vigilance and caution before clicking on any links.

Most NKU computers have various controls and protections in place (advanced anti-malware, strong password protection, user security awareness, etc.) which mitigated the risk until the fix was made available.

Zoom does not support end-to-end encryption

When the cybersecurity team reviewed the Zoom service, NKU never presumed that the service supported end-to-end encryption. A diligent review was completed, concluding that although Zoom's service offering is not truly encrypted end-to-end, it still met NKU's cybersecurity requirements for the urgent need of remote teaching.

Note: Zoom has acknowledged the confusion that could result from their initial "end-to-end encryption" claim and has since updated the description of their offering.

With the increased usage and attention that Zoom has received in the last few weeks, the company has acknowledged their commitment to a continuous cybersecurity improvement process; making efforts to improve their default security settings. Given the urgent requirement for this service during the current COVID-19 pandemic, NKU IT feels confident that Zoom allows for an acceptable course distribution configuration.

From a practicality viewpoint, no tool is 100% secure; however, we must be practical and recognize the importance of using Zoom and other collaboration tools. Recognizing the security of the content being shared and taking actions to reasonably secure your Zoom conference should allow for an acceptable class.

For questions or concerns please contact the NKU IT Help Desk.