To: Dalhousie Architecture and Planning Students

From: Privacy Office – Heather Casavechia, Privacy Officer
Information Technology Services – Scott Wilson, Associate Director, Information Security

Date: May 11, 2020

Re: Zoom Privacy Risks and Guidelines for Students

The Faculty of Architecture and Planning is using Zoom to deliver specific functionality to students during the Summer term that will allow enhanced whiteboard features that cannot be accessed through other online learning tools at this time. Zoom has been approved for use for certain courses only. The Dalhousie security and privacy offices have identified the following issues that you should be aware of prior to using the service:

1. Zoom collects and stores personal information and shares it with third parties. Data is collected directly from users and their device. Zoom's Terms of Service provide a lot of leeway for collecting personal information and how it can be shared. Zoom collects the following personal information
   - Name
   - Physical address
   - Email
   - Device
   - IP address
   - If using Facebook to sign on, Zoom scrapes your social media profile and collects additional personal information from your Facebook account
   - Any information that you upload, create or provide while using the service
   - Content in cloud recordings
   - Instant message content
   - Whiteboards shared while using the service
   - Video transcripts that can be automatically created by the service

2. The host of the Zoom meeting has permissions that may not be apparent to other participants including the ability to record the meeting and monitor participants using an 'attention tracking' feature that notifies the host when participants click away from Zoom for more than 30 seconds. There is no mechanism to 'opt-out' of these features while continuing to use the service.

3. Security vulnerabilities in the past 18 months have allowed hackers to access meetings (Zoom bombing), to take over the web cam on Macs, and have enabled personal data leaks. [1]

When using Zoom, we recommend the following guidelines to reduce the risk to participant personal information.

Guidelines for Students

1. Don't discuss, chat, or screen share personal/sensitive information while on a Zoom call.
2. Keep your camera and microphone turned off unless you are speaking.
3. Use a background image to prevent the host and other participants from seeing inside your home.
4. Do not use Facebook to create an account or log-in to Zoom.
5. Register with Zoom using your Dal email address, and a password that is different/separate from your NetID password.
6. Clear cookies and blocking trackers after every call.
7. Opt-out of all secondary data uses where possible.
8. Always keep Zoom clients up to date for protection from new security vulnerabilities.
9. If a Zoom-bombing incident occurs, immediately leave the meeting space.

For additional details, and the latest Zoom guidance from our Privacy and Info Security Offices, please visit https://dalu.sharepoint.com/sites/its/SitePages/st-zoom.aspx.

Questions or concerns about the use of Zoom and the risks and guidelines identified here can be directed to your course instructor, Dalhousie's Privacy Office, Dalhousie Information Technology Services, or the Director of the School of Architecture.

Director of the School of Architecture
Diogo Burnay diogo.burnay@dal.ca

Dalhousie Privacy Officer
Heather Casavechia heather.casavechia@dal.ca

Information Technology Services
support@dal.ca | https://www.dal.ca/dept/its/help.html

[1] Flaw opening meetings to hackers
Zero-Day Bug Opens Mac Users to Webcam Hijacking
Zoom Flaw lets Hackers Hijack Conference Meetings
Zoom Vulnerabilities Expose Users to Spying, Other Attacks
Zoom found leaking personal user data, could also facilitate stealing your Windows sign-in credentials