The following message is being distributed to all UBC employees on behalf of Don Thompson, UBC Chief Information Security Officer. ***For Managers with contractors, please circulate as needed.*** *Communications developed and distributed internally to UBC employees may contain confidential information and should not be circulated or forwarded outside of UBC.*

Hello everyone,

UBC is seeing a significant increase in the volume of sophistication of cyber attacks specifically targeting universities and healthcare facilities. This combined with the recent increase of remote work arrangements for UBC faculty and staff has placed a greater risk to the security of UBC systems and information.

While we already have several technologies in place to help secure remote access (e.g. VPN, DUO, mandated encryption, etc.), these alone are not sufficient to adequately protect UBC. To mitigate these increased security risks, we are making new security software available to all UBC staff, faculty and researchers. The cost of these controls is being covered centrally. There is no cost to the end user.

For devices managed by UBC IT or departmental IT, the IT Desktop Support and Cybersecurity teams will deploy the software directly to the device.
For individuals using their own device for University Business (Bring Your Own computer/device or BYOD), self-serve instructions to manually install and configure the security software is available.

For further information about these increased security precautions, including BYOD instruction please visit this page on the Privacy Matters @ UBC website:
privacymatters.ubc.ca/covid19_increased_security

Like all of our security tools, the software has been configured to ensure your privacy is protected. The purpose of these controls is to protect your device from malicious software. The content of files, emails, passwords, instant messages, etc., is not accessed or recorded. Information about your personal use of UBC systems and devices is protected under the Freedom of Information and Protection of Privacy Act, and by UBC's Information Systems Policy (SC14) and Information Security Standard #10, Accessing Electronic Accounts and Records.

Finally, I would also like to encourage self-responsibility when it comes to protecting UBC. Please stay extra vigilant during this time as we know that universities are a prime target for criminal activity, especially given the fiscal year-end combined with the COVID-19 crisis.

A few simple reminders:

- Don't click on links from unfamiliar sources. Doing so can download malware onto your computer or device even without further action on your part.
- Report any suspicious emails to **security@ubc.ca** – the Cybersecurity team will investigate.
- Protect your password and keep it secure. Don't use UBC passwords for any other websites.
- Complete the mandatory Privacy and Information Security Fundamentals training.

Should you have any questions on this matter, please reach out to privacy.matters@ubc.ca.
Best Regards,

Don Thompson
Chief Information Security Officer
The University of British Columbia
Email: don.thompson@ubc.ca