We all use various applications for keeping in touch with our students, from Skype to messaging apps to Facebook. For many, these work just fine. But what if your student is from a sensitive country where taking part in Christian activities or converting to Christianity can pose real threats to family, health, or position?

Your International Student Ministry staff have researched the security of some of these commonly used platforms and offered suggestions on what truly is secure and what is not.

Recommended platforms have a ★ , and platforms with heavy security risks have a 🚫 . Some poor security platforms, such as MailChimp, can be used under certain circumstances, but never when conveying high-risk information or to communicate with people in high-risk countries.

Other security documents available:

General Communication and Protocol for ISM

5 Easy Ways to Increase Your Internet Security

For more information contact
Chloe Papke at
chloe.papke@intervarsity.org

INTERVARSITY
INTERNATIONAL STUDENT MINISTRY

ism.intervarsity.org

how secure are you?

a guide to commonly used cyber platforms for storage, email, video conferencing, messaging, and networking

v1.0 2016

		SSL		END TO	MULTI-STEP	
		ENCRYPTION	IN-TRANSIT	END	VERIFICATION	NEGATIVES
★	DROPBOX	+	+	+	+	if client-side encryption not enabled, access user data if client-side encryption enabled, can't unlink or restore data
★	GOOGLE DRIVE	+	+	+	+	stored docs only have mid-level encryption
★	OFFICE 365	+	+	+		if user is donor or went to Urbana, some data are public
★	GMAIL	+		+	+	some in-transit encryption, provider can read
🚫	MAILCHIMP	+		+		all free acounts are in one database; all campaigns are mirrored, backed up, make auto web version
★	ZOOM			+	+	end-to-end must be enabled by user; record feature allows sharing and downloading; all recorded videos are stored in Zoom's cloud
★	VSEE	+	+	+		
🚫	SKYPE	+		+		provider can read; calls to landline/mobile phones are not encrypted; voice messages are sent unencrypted to computer; easily find location, back doors for governments
★	VIBER	+	+	+	+	messages and photos from iOS devices aren't necessarily secure
★	iMESSAGE	+	+	+		only available for Apple products
🚫	FACEBOOK	+		+		past communication not secure; privacy and security features set low automatically; opt out of sharing and opt in to security; provider can read
🚫	WECHAT	+				2015 malware not confirmed fixed; hacking fix not confirmed
	WHATSAPP	+	+	+		owned by Facebook
★	THREEMA	+	+	+	+	software code available

SSL: high-level encryption **In-transit: encrypted between servers** **End-to-end: encrypted when leaving and entering servers**