

Communicating with Clients More Securely Using Technology

While it can be useful to communicate with clients electronically (through email, text, instant messaging or a video call), it is important to avoid sharing sensitive information, and to use the most secure methods available. Abusers may access a client's email or phone physically or remotely, and install spyware or [keyloggers](#). Unless it's a video call, you can't be sure who you are communicating with, or who else can see your message.

Still, more clients and anti-violence workers are appreciating the speed, convenience or need for email, texts and instant messaging. Your client may be Deaf or be living with a disability. She may live in a remote location or lack transportation. She may not have minutes or reception on her cell phone, and may only be able to receive texts.

"We are clear with clients at intake that we prefer not to communicate electronically, as we don't know who is seeing the messages. We check with them about their preferred method of communication and if it is safe to use text or email – and if yes, we let them know it will be for appointment setting only."

A BC Anti-Violence Worker

Electronic communications can be helpful to schedule appointments, or to send hand-outs, forms, information or case updates ahead of or between appointments. Sometimes you may only have time for a quick text to a client before your next appointment arrives, or court starts again.

Following are some basic pointers on safer electronic communications. Bear in mind that technology changes rapidly, "bugs" are always being discovered, and hackers are always finding security flaws they can exploit. Some of this information may soon be outdated.

DID YOU KNOW? End-to-end encryption (E2EE) is a method of secure communication that prevents third parties from accessing data while that data is being transferred from one system or device to another.

Email is considered the least secure form of electronic communication, and has been compared to sending a postcard. Outlook did roll out some new security features to those with an Office 365 subscription in early 2018, but most email still doesn't offer end-to-end encryption for messages while they are in transit.

Text messages are electronic messages sent between two or more users of mobile phones, computers, or other devices such as iPads. Texts may be sent over a cellular network, or through an Internet connection. To be secure, they must have E2EE. While E2EE protects your messages in transit, remember that someone can still intercept the message if they gain access to the phone.

Instant messaging usually involves messaging applications (apps) such as Facebook Messenger, iMessage, WhatsApp, Telegram or Viber. Instant messages are sent over the internet or cellular networks, and many services also allow users to video call. Apps are usually downloaded through an app store.

Video calls are often conducted using services like Skype or Zoom, but many messaging apps also offer video calling.

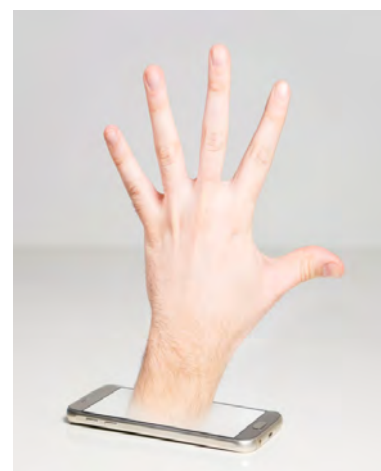



Photo: TeroVesalainen (Pixabay)


[Counsellors] using or considering the use of technology to conduct therapeutic encounters should honestly evaluate their specific skills for the method of electronic counselling they use, and should take steps or training to improve in these areas. They should also remain up to date with respect to the technology they use, in particular where security and confidentiality may be impacted. Failing to ensure competence in these areas while using the technology is unprofessional, and can also be dangerous.


Standard for the Use of Technology in Counselling, BC Association of Clinical Counsellors


Safer Electronic Communications

Four Recommended Free E2EE Messaging Apps

 **Signal** (<https://signal.org/>) is generally considered the “gold standard” of secure messaging apps. Signal allows you to send E2EE encrypted messages, to make voice and video calls, and even to send documents between Signal users. Signal has a feature called “disappearing messages” which removes messages from the sender’s and recipient’s devices after an amount of time that you choose.

 **WhatsApp** (<https://www.whatsapp.com/>) now uses the same encryption protocol as Signal. WhatsApp also offers texts, voice and video calls, and allows you to send attachments (including documents). The app also has a desktop version.

 **Viber** (<https://www.viber.com/>) rolled out end-to-end encryption for calls and messages in early 2016. The E2EE works on Viber's desktop, mobile, and tablet versions. Viber uses a color-coded system to show how protected a conversation is, and allows you to attach files.

 **Telegram** (<https://telegram.org/>) is another secure messaging app with E2EE and a desktop version. You can send text and video messages, and attach documents. Messages can be set to “self destruct”.

Facebook Messenger allows E2EE messages that can also be permanently deleted, but you have to remember to turn on the “Secret Conversations” option to encrypt them.

Apple’s iMessage is also end-to-end encrypted, but Apple also allows users to send messages as a text if the iMessage won't go through, and text messages are not end-to-end encrypted.

Skype (<https://www.skype.com/en/>) recently upgraded to E2EE, but it is not the default setting. Users must enable “Private Conversation”.

Zoom (<https://www.zoom.us/>) recently upgraded to E2EE video calls, but E2EE is not the default, and must be configured at the account or user level.

Do you need to send private information securely using email? NoteShred (<https://www.noteshred.com/>) was created to provide an easy way to send and receive sensitive information over the internet. It does not require the recipient to create an account or to install any software to receive the information.

You create a “note” and assign it a password. You then send a link to the note to the recipient, and a separate message with the password to allow them to open it. You can select how and when you would like the note to “shred” or delete itself. NoteShred will email you once your note is deleted, so you will know the sensitive information is no longer in anyone’s inbox.

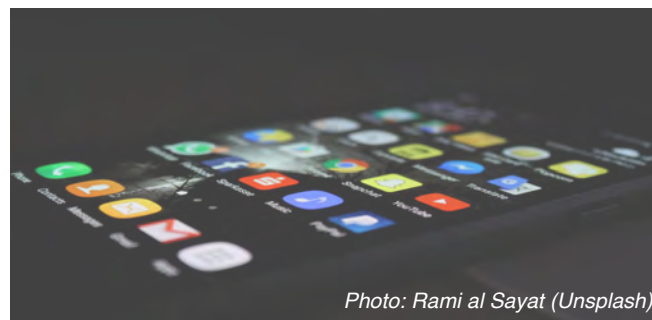


Photo: Rami al Sayat (Unsplash)

Additional Resources:

Questions to Consider: Technology Safety for Programs NNEDV Safety Net Project
<https://www.techsafety.org/resources-agencyuse/techsafety-for-programs-considerations>

Using Technology to Better Support Survivors: Literature Review Nicole Pietsch
http://www.vawlearningnetwork.ca/sites/vawlearningnetwork.ca/files/LN_Brief_33.pdf

Standard for the Use of Technology in Counselling BC Ass. of Clinical Counsellors
<https://bc-counsellors.org/wp-content/uploads/2015/09/7BCACC-Standard-Use-of-Technology-2011.pdf>

Ditch All Those Other Messaging Apps: Here's Why You Should Use Signal Wired.com
<https://www.wired.com/story/ditch-all-those-other-messaging-apps-heres-why-you-should-use-signal/>