

HOW TO SEXT SAFELY

Category: Commercial Law, Privacy Law, Infosec, and POPIA
written by Darren Epstein | June 8, 2016



How many of us have ever sent sensitive information or a password with someone over a text or email. Perhaps, you have had the need to send a rather 'saucy' photograph to someone.

The internet has changed the way people act. A new found confidence and a sense of unfounded safety has led people into serious hot water.

It is important that everyone knows some method to share sensitive data and information with people they trust.

The following methods are not perfect for every situation and depend on the type of data that is going to be sent.

- For passwords and simple information, the simplest and one of the most effective methods is to break the message up into chunks. This works well for usernames, passwords and other line text (like a credit card number).
- Obscurity is the key and the sensitive data should be sent over separate channels (i.e. half email, half text message).
- This method works as someone intercepting a message would not have the context for what it applies to. The key element for this method is that there must always be a separation of context and information.
- This method is not foolproof and is extremely tedious, but is a simple way to add some extra security.
- For full documents or those 'naughty' photos, a great idea is to use an external service.
- Dropbox is one such service and has the benefit that the recipient does not need to have signed up for the service to receive the content. Dropbox encrypts everything you upload and download over a secure HTTPS connection, meaning your file transfer should be secure from start to finish.
- A big drawback is that the mobile application does not use an encrypted connection, so there is a risk if it is used over a Wi-Fi connection.
- To add further security to the Dropbox method, employ the 'half and half' method, described above, as well. Split the link, with half in email and half in text message. Of course it may cause a slight hassle, but the extra security afforded greatly outweighs any hassle.

- For those who like to risk reputation and careers by sexting, certain 'self-destruct' applications offer a slight benefit. These applications automatically delete your photo from a recipient's phone after they have seen it for a few seconds. The issue with this is that if something can be seen, it can (and more often than not) be copied. For photographs, this method is not recommended as it carries a great risk. To demonstrate this risk, one just has to browse the many websites devoted to screen-grabs of Snapchats and the like.



Another issue is trust. Can you really trust the person you are sending that photo to will not show anyone else? Can you really trust these random third party applications with your drunk texts and dirty images? Security extends only so far as you trust the recipient of that private info

In the end, the best option is the old-fashioned person-to-person hand-off. There is no risk of anything getting intercepted while it travels through servers or the like and there is a guarantee it reaches the person that was intended to receive it. The only issue is, would that person be the only one to see it...