|  |
| --- |
| **USING THE NEW CYBERCRIMES ACT TO PROTECT YOURSELF** |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  | | --- | --- | |  | ArticleImage | |  |  | |   ***“…cybercrime has increased by over 300% during the COVID-19 pandemic - making it one of the biggest threats to businesses around the globe.” (Property 24 report)***  The Cybercrimes Act, which has been years in the making, is now (with effect from 1 December 2021) at last largely in force. Although some provisions still remain on hold (most notably some of those relating specifically to “revenge porn” and the granting of protection orders), a whole range of unlawful cyber-related activity has now been specifically criminalized.  The police have also been given wide powers of investigation, search, access and seizure, and the penalties for contraventions are substantial.  The pandemic-forced shift to a “work from home, shop and communicate online” culture has reportedly seen cybercrime rocketing by 300%. As always our best protection from online criminals is prevention, but for anyone unfortunate enough to fall victim to them at least the new Act now provides us all with a layer of legal protection we haven’t had before – but only if we actually use it and report cybercrime.  ***The new crime categories***  The Act’s provisions are detailed and complex, so this is of necessity just a very brief summary. But for most practical purposes what you need to know is that both individuals and organisations now face prosecution for any –   * Unlawful access to a “computer system” or “computer data storage medium” (i.e. “hacking”). * Unlawful interception of or interference with data, computer programs, data storage mediums and systems. * Unlawful acquisition, possession, provision or use of passwords, access codes and the like (PINs, access cards and devices included). * Cyber fraud, forgery, extortion and theft. * “Malicious communications” (which would by definition include messages sent by email or via Social Media channels, WhatsApp and the like) to the general public, individuals or groups that –    + Incite damage to property or violence to a person or persons,   + Threaten a person or persons with damage to property or violence,   + Disclose a “data message of an intimate image of a person” without that person’s consent, and regardless of whether the victim is identifiable in the image itself or only from a description or other related information. Moreover the image can be “real or simulated”.   ***A particular warning to Social Media users***  Posting or sharing anything prohibited by the Act – perhaps particularly any of the types of “malicious communication” referred to above – could land you in some extremely hot water. **Think before you post!**  ***What about “revenge porn”?***  As noted above, some of the Act’s provisions relating specifically to “revenge porn” are not yet in effect, but there are already prohibitions against it in other legislation, plus the offences mentioned above relating to disclosure of “intimate images” should at least partially assist victims in the interim. |