

# Extortion via Facebook on the rise in the UAE

Take these steps to remain safe online

By Rachel McArthur

Published Saturday, August 21, 2010



Personal information is at increasing risk on the internet. (FILE)

There is not a week that passes by without a story about an online crime or court case being reported on the news. From individuals being jailed for blackmailing a 'friend' on Facebook, to millions of users' information being hacked into, it's safe to say that the world of online social media isn't, well, as safe as you think.

And despite the UAE having more control over the World Wide Web than other parts of the world, users in this country still are not 100 per cent safe. Basically, if you post information or a photograph of yourself online, there is a chance of that content reaching someone you did not expect.

Even Dubai Police have raised the alarm regarding the situation. Last week, the General Department of Forensic Sciences and Criminology announced that the number of criminal cases involving online abuse has

already passed 50 this year, of which nine involved defamation cases from social networking websites. Forty-two involved extortion, threats or insults.

Captain Rashid Ahmed Lootah, Head of the Department, told Arabic media: "People are using blogs and social networking websites to collect information and defame people for revenge purposes. Facebook has a technical fault that allows it to be hacked into easily and used for extortion."

Compared to last year, a total of 62 cases of defamation were recorded by Dubai Police. Seventy-four cases were recorded in 2008.

According to Alexa.com, the top 20 websites in the UAE include eight websites that are social networks or incorporates a social media element.

They are Facebook (the second most popular website in the UAE; number one being Google); YouTube (ranked number four); Yahoo! (fifth); Windows Live (sixth); Blogger.com (eighth); Twitter (number 15); LinkedIn (16th); and Dubizzle.com (17th).

Not surprisingly, most of the online crimes reported to police in the UAE have involved Facebook.

One man admitted before the Dubai Court of Misdemeanours that he uploaded several pictures on Facebook of the victim, an Arab lady, and posted libellous comments. And in another case, a woman claimed that a man she did not know was forcing her to send him compromising pictures of her and her friends.

In another recent incident, a women described how she kept on receiving sexually explicit messages on her Facebook wall from an alleged stalker.

Meanwhile, other cases noted involved men hacking into computers of female friends/co-workers and stealing personal photographs for revenge purposes.

Out of all the cases reported in the past year, most users that were targeted were women of Arab or Asian origin; making it highly probable

that many do not even report such incidents out of fear of ruining their family's reputation or causing them trouble, for example.

The key, therefore, is to avoid landing in these situations from the beginning.

Here are some tips on how to stay safe online:

- When you sign up with a social networking website, make sure you know how your information is going to be used and how it is going to be shared. Read the terms and conditions carefully. At the end of the day, social media is business, so more info equals more money for the owners!
- Make sure you are on top of any privacy settings. On Facebook, only share some information (including wall posts) with friends. Don't share your e-mail, street address, and phone number with anyone. Avoid joining networks.
- Avoid uploading each and every single photo of you – keep it simple. Don't feature photos of you with people you don't necessarily want friends/employers seeing or that crooks could use to their advantage.
- But it's not just about protection against crime. Think of your normal life too. Imagine calling in sick on Monday, only for your boss to see an album entitled "Dubai Monday Madness" uploaded on Tuesday? Chances are that will be your last day in the office.
- If you are job-hunting, remember that potential employers will want to check you out. If they see a Facebook or Twitter profile picture of you looking worse for wear being carried by a friend who looks even worse, they'll probably think twice before inviting you for an interview.
- Unless you're a major celebrity or politician, chances are you don't really want to be found on Google.com. On most social networking websites, there is an option for your profile to be publicly available in Google's search results. Disable that option.
- Do you work for a bank or an insurance company? Make sure this is not mentioned anywhere in public forum – or you could be targeted by criminals interested in making some illegal money.

- Give false (but memorable) answers to “reminder questions” – who’d guess that your mum’s maiden name is MohamedAhmed06?
- If you are unhappy with the service or privacy, change your details on it and delete the account.
- And finally, if you suspect someone is using your photos or information or you are being blackmailed or threatened, report it to the police immediately.