# Three ways your personal photos are vulnerable to hackers

September 2 2014, by Andrew Smith

Recent reports of celebrities having nude or risqué photos of themselves leaked online highlights the serious risk of hackers getting access to our personal pictures.

While many of us take inane and uninteresting photos that we wouldn't mind anyone seeing, some of us do like to share more interesting pictures with other individuals that we wouldn't wish to be seen on the twitter feeds of millions. I am not personally interested in value judgements around taking nude pictures but I do appreciate the impact on those who have seen their intimate moments shared without their permission.

How were these pictures hacked? The reality is going to be the work of cyber-security and forensic experts to discover. But as there are now so many private photo streaming services, the potential for exposure becomes very likely.

There are three main ways your photos could be vulnerable to hackers.

## Sharing passwords across different sites

One vulnerability is if you use the same password for more than one account online. Taking a look back to the Oleg Pliss hack in May, cyber-criminals managed to compromise iCloud by using indirect hacking, social engineering and innovative thinking.

Assuming people used the same password on more than one service, the hackers attacked another unrelated system then managed to systematically test each @icloud email account to see if they could get into the cloud with the same password.

The same applies to any other private photo storage or cloud-based account. The technology by itself is secure, but if you use the same passwords for multiple services and have been unknowingly part of an attack, then the rest is quite obvious.

## Targeted attacks

Alternatively, you can fall victim to a targeted attack by being sent targeted emails, files or even given a memory stick with compromised files on it. It does not take too much effort to get a trojan keylogger onto someone's computer if you really want to.

Once the keylogger is at work, it will send screen-shots of each mouse click, key stroke and other activities back to the hacker. Internet speed is now so advanced that you would not notice the traffic.

## Public hotspots

Finally, if you have a laptop or smartphone with personal photos on it and use it on a public hotspot, there is the potential for compromise. Firesheep, among other applications, allows hackers to compromise any device on a public system.

The man-in-the-middle attack is an old compromise taught to many network engineers as a way of defending networks. It is not a complex process, and it deceives a wireless access point into letting one computer become the gateway for all devices on the network. This would allow

hackers to see all traffic and therefore images being sent across the system.

## What can you do?

There are steps you can take to reduce your vulnerability to attack. Consider where you store any pictures that you wouldn't want the public to see. Consider how up-to-date your anti-malware software is and also what passwords you use on different systems. If you are using photo streaming services, check now to see if private photos are already at risk of being exposed to the internet.

If nothing else, the story of this mass leak of images has exposed how many of our own photographs are being unwittingly shared with cloud services which may be compromised. Whether we're celebrities or nobodies, we must all be vigilant in protecting our private data in these increasingly insecure times.

*This story is published courtesy of* The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation