999

SECURITY AND SAFETY FOR ALL

ISSUE 43 AUGUST 2015

SMOKING AND KIDS DON'T MIX
BUTT IT OUT WHEN KIDS ARE AROUND

DANGEROUS ROADS DECODED
WHY SOME ROADS KILL MORE

THE GREAT PHOTO SCAM

SPOTLIGHT ON ABU DHABI
HERITAGE HOPPING IN ABU DHABI

STOLEN ONLINE IMAGES CAN WRECK LIVES AND FLEECE VICTIMS

UAE	5.000	AED
KSA	5.000	SAR
Kuwait	0.500	DK
Bahrain	0.500	BD
Qatar	5.000	QAR
Oman	0.500	OR

6 291100 752126

IN THIS ISSUE: CASES OF MISDIAGNOSIS, INSIDE A BLOOD BANK

When all of the UAE was enjoying spring this year, Dubai resident Ruth Palmer, a British citizen married to fellow Briton Ben Graves, was trying to recover from the shock of discovering her own double life, one that she never knew existed.

There was this person called Leah Palmer, a stylish young woman with a horrible ex-partner. A Brit expat in Dubai, Leah knew people in the celebrity circles, flirted effortlessly with men, and hooked a few of them. Quite a rocking life... for someone who was a work of fiction. All the photos used for Leah's social media accounts were stolen from Ruth's accounts. The scam only came to light when a friend sent Ruth a screenshot from another person's Instagram account – the so-called Leah's – and she saw herself and some friends. Dozens more photographs thus stolen were discovered. In Leah's universe, Ben was marked as a psycho. One fake account was taken down; another one popped up. The person behind the fiction named Leah was certainly persistent.

As snapshots of our whole life begin circulating online – photos from parties, time spent with friends or one special person, graduation ceremony – online infringement of photography rights becomes common. It can be a web of lies spun for personal advantage, as in the Leah Palmer case, or a racket being run for monetary gains, as in the case of a fake school offering fake jobs and charging a visa fee.





In its April issue, ***999*** exposed the modus operandi of Middle East Office of Academic Regulation and Examination (MEOARE) where people were offered master's degrees only by paying $500 (Dh1,836), and without even studying. Among other indications, a clear proof that MEOARE was a sham is that: the photo of its "chairman" was bought from Shutterstock, ***999*** found out.

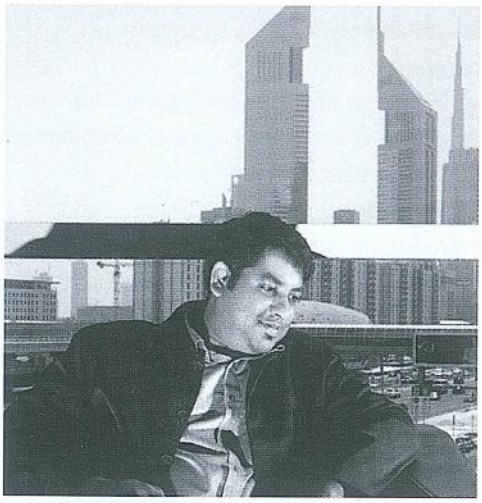
Last year, UAE media reports and a vigilant school advisory website brought to light the school scam. It targeted teachers by offering them jobs in a non-existent institution in Abu Dhabi; the basis for the scam was a set of photos stolen from another school website. The fake school invited

"As snapshots of our lives begin circulating, infringement becomes common

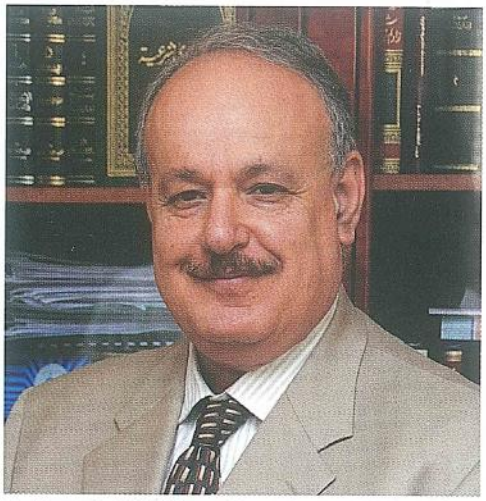
online applications for teaching and administrative posts, and candidates would need to pay $1,250 (Dh4,587) towards the visa processing fee.

The interesting thing was the fallout of the two cases. In Ruth Palmer's case, her photos stolen to create another identity couldn't be investigated as fraud by the police in Britain, as her photos were not strictly copyrighted and, therefore, were available to all. In the school case, a crime had obviously been committed, as people had paid money on the basis on false promises.

It's important to understand that not only are our photos out there, but that we have little control over who uses them and how. Someone else can not only take your online photos, but can also make money from them in entirely legal ways – in addition to the illegal ways. One such instance is the recent widely covered exhibition by the New York artist Richard Prince. He took screenshots of pictures he liked from other people's Instagram accounts, 'modified' them artistically, printed them out in giant sizes... and sold the prints for $90,000 apiece! He never bothered to inform the owners of those Instagram accounts that he was using their photos, let alone ask if they wanted to be featured in the exhibition.



John Thomas, Head of Social Media, Unveyl Technologies



Dr Reyadh Al Kabban, Founder and Managing Director of Al Kabban & Associates

Motives and methods

Misuse of photos posted online can happen for various reasons. As we've seen already, someone found an attractive woman's face and used it as a mask; someone used another institution's façade to con people; someone took artistic licence with other people's captured moments. It may be safely assumed that these photos were easy to steal. Most people don't take detailed steps to guard personal pictures; only professional photographers use watermark and prominently displayed copyright information.

Socia media websites do have privacy settings, e.g. you can control on Facebook whether your photos are visible only to friends or to the public; and Instagram has no sharing button at all. But any kind of



Photo identity theft and celebrities

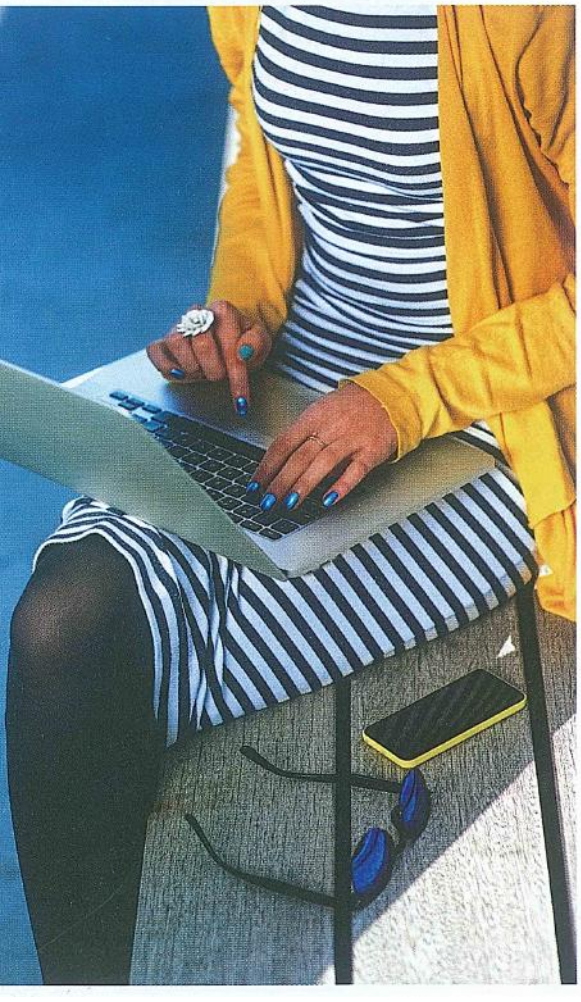
Hollywood celebrities Jim Carrey and Meryl Streep have recently been in the news as victims or perpetrators of photo misuse. In the case of Jim Carrey, in July this year, he posted a series of photos of children as a warning to those who support vaccination; the actor is part of the anti-vaccine fringe group in the US. Alert users found that photos of crying children having a meltdown were mostly stock photos. One of them, however, was a screen grab of a video of a boy who suffers from tuberous sclerosis complex, a genetic disorder, the symptoms of which include seizures and cognitive impairment. His family runs a blog to spread awareness of the condition. It caused them much distress to see their visual used without permission for a cause they don't agree with. Carrey had to apologise and remove the photos.

Meryl Streep, on the other hand, was seen dishing out advice that she never gave. Facebook users are notorious for posting seemingly inspirational messages randomly attributed to celebrities. This quote about no longer having patience for things that displease her was actually written by a Portuguese life coach, José Micard Teixeira, who in September last year asked his readers on Facebook to publicise the misattribution. Snopes.com, which is a great source of checking the veracity of so-called Internet facts, says, "As far as we can tell, the earliest Facebook reposting of Teixeira's words that incorrectly credited them to Meryl Streep occurred on the page of Tuncluer Textiles on 15 July 2014, and the quote went viral in that form after being combined with a photograph of Meryl Streep... ."

protective measures, such as using hidden layers, tiling, disabling right clicks and using flash, can be bypassed by taking a screenshot. Only a watermark in the middle of the picture can thwart the photo thieves; unfortunately the watermark also kills the visual appeal of the photograph.

Lawyers say that when it comes to photos, the first line of defence is the user. Dr Reyadh Al Kabban, Founder and Managing Director of Al Kabban & Associates, says, "It is important to note that when people upload their pictures on social media, they may be impliedly consenting to their images being shared. As such, it is very important to check the privacy terms and conditions on the website prior to uploading photos. Additionally, the privacy settings need to be checked as well."

Most social media websites allow you to choose how public you want your image to be. However, do note that the original website where you posted the photo may have rights to it. Dr Al Kabban says, "With regards to copyrights on images uploaded on social media, you need to check the terms and conditions of the website. Most of the time, by uploading your image on [any] social media website, you impliedly grant the owners of the website a non-exclusive, transferable, sub-licensable, royalty-free, worldwide licence to use any content that you post."



Once your photo is out there for all to see, there's really no telling who will copy it and use it. John Thomas, Head of Social Media, Unveyl Technologies, Dubai, says, "Of late, there has been a spate of scams online, where photos of people were stolen from social networks and misused to create fake profiles for job scams and database thefts. Prevention is always better than cure, and it does a world of good to think well before uploading one's pictures online. It, however, becomes necessary to upload one's photo in certain situations. For example, while creating a profile on professional sites like LinkedIn or Viadeo. In such cases, I would recommend that people make full use of the privacy settings available within the network."

Spotting a scam

While prevention is the first step, vigilance is the next. Scam websites promising jobs, services or degrees may use fake photos stolen from here and there. If you're going to use a service based on the glowing reviews provided by seemingly real people, it's best to test it via a website that offers reverse search. This means that if you upload an image, the search engine will find images that fit the parameters on the Internet. Stock photos are likely to show up in this search. Similarly, if you've been careless in leaving your image on a public platform, a reverse search reveals whether it has been stolen.

A good marketer uses genuine people for product or service testimonials, while copyrighted stock photos from websites like Shutterstock and Getty Images are used for representative visuals. Thomas says, "The easiest way to get anyone's attention is through photographs. So, we use a lot of photos, in our ads, social media posts and marketing and promotional material for our clients. Usually, we source images from image banks. However, when usage of a real photo is required, particularly when showcasing customer testimonials, we use actual images of the customers. Typically, we source the images by getting in touch with the customer himself and asking for permission to use it for promotional purpose. Otherwise, [the photo] is client-supplied, but we ensure that the client has got the necessary permission from their customers to publish their photos in print or online."

> **"When it comes to photos, the first line of defence is the user**

He adds, "If one wants to know if his/her profile [picture] is misused online, he can do a reverse image search of that photo. A reverse search reveals all the websites and pages where the particular image has been used. This is one way of finding out if your photo has been misused by anyone and uploaded anywhere without your permission."

The law in the UAE is very particular about protecting the privacy of individuals. Dr Al Kabban says, "If you come across any incident of image theft in the UAE, you are entitled to file a criminal case against the individual who has committed the act. One can refer to Article 378 of the Penal Code which states as follows: 'Whoever invades the privacy or family life of individuals by committing any of the following acts in



Locking out the photo thieves

Here are some measures that make it harder to steal one's photo posted online. These tips are from www.cambridgeincolour.com, an online community for photographers.

Hidden layers: Place the actual image behind a transparent foreground image. The online image will appear completely normal, but whenever someone tries to right click and save it, the resulting file will be the blank foreground image, not the background.

Tiling: Another option is to break your photo into smaller image tiles. These will appear as a continuous image, but anyone trying to copy your image will end up saving only one tile piece at a time. However, the tiling approach also means that your web server will have to provide several files instead of just one – this may make the web page load more slowly, and can potentially increase your server requirements. Separating each photo into smaller tiles can also be quite time-consuming, so this option isn't commonly used.

Disabling right-clicks: This method can be a very effective way of letting your visitors know that you're serious about image protection, and of ensuring that they receive a copyright notice whenever they try to save your image.

Using flash to display the image: This prevents any kind of right-clicking or saving in standard browsers, and can be implemented using a programme called swfIR. However, the visitor can still access the original image if they view the page's HTML source code.

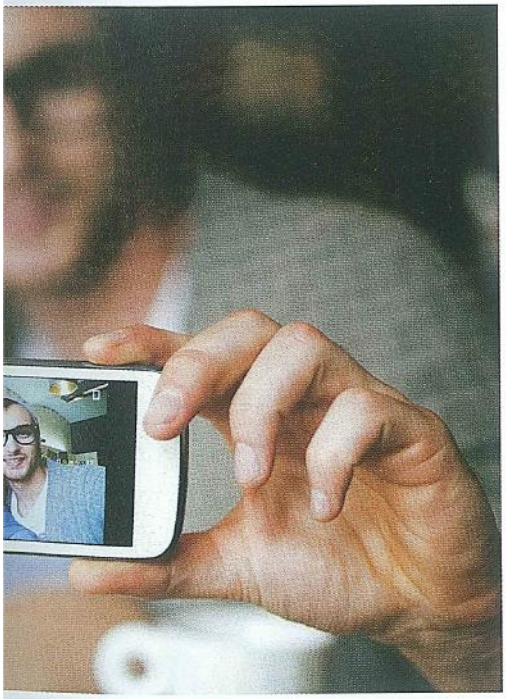


Watermarking: A good way to make it clear that you're serious about copyright protection. Watermarks also make it more likely that you'll receive credit even when an image has been copied without your permission. A software called Digimarc digitally encodes the watermark as image noise that is imperceptible to our eyes, but detectable by a computer with the appropriate software. The Digimarc watermark can still be removed, but only if the violator knows it's there in the first place. A disadvantage is that this increase in noise may also increase your image file size. Digimarc is built into Photoshop by default; however, this feature isn't free.

Putting digital image frames: An alternative to watermarks is to create a frame for your image, upon which you can list your name and other photo details. This would give you immediate credit even when the photo is used on another site, but it's also the type of attribution easiest to remove.

circumstances other than those permitted by law or without the consent of the victim, shall be punished with detention and a fine.'"

The law stipulates that "any person who publishes, in a public manner, news, pictures or comments relating to the secrets of the private or family life of individuals, even if they are true, shall be punished with the same punishment."



Dr Al Kabban says that as per the law, "detention for a period not exceeding seven years as well as a fine shall be the punishment to be imposed on any public official who commits any of the acts stated in the Article, depending on the authority of his post".

For those who find that images that belong to them have been used without their permission, he says, "If you are the owner of a website and if someone has copied images from your website and used it for his/her benefit or on social media, you are able to take legal action against him, provided the images on your website were copyrighted."

The next time you post a picture online or see a testimonial accompanied by a photo, be alert – when it comes to the Internet, photos do lie.

Prevention and cure

DO

- Check and use the privacy settings on photos that you post online.
- Search your name/image on popular search engines to see if your identity has been compromised.
- If a professional service that you are a member of uses your photo without permission, you are within your rights to request its removal.
- Take legal recourse if you find unauthorised use of photos.

DON'T

- Leave your photos online visible to everyone.
- Be careless about tagging photos.
- Trust each testimonial you read without verifying via reverse image search.