COMPUTER NEWS from the

JANUARY 2018 Volume 6 NO. 1

As found on the web and other sources

HAPPY NEW YEAR to one and all.

I hate to start the new year, but…

Is it real or Photoshop?

Fake News and Fake Photos

Category: Reference From “askbobrankin.com”.

Social media of all kinds - Facebook, Twitter, Instagram, etc. - is rife with disinformation spread by people with ulterior motives. It’s a huge problem; you never know if what you’re looking at is real or fake. Many users react emotionally to provocative fake photos and posts, sharing and commenting on them, perpetuating the false impressions and outright lies. Read on for my tips on spotting a fake photo...

Verifying Authenticity Of Photos

In a recent study, I read that lots of people pass along these bogus items on social media without bothering to venture beyond the photo or the headline. You don't want to be one of those people, right?

Doctored photos are a favorite tool of propagandists. There are many free photo editing tools online, making it dead simple to alter or create a fake photo. As an example of this sort of disinformation campaign, we can turn to the widely circulated photo apparently showing a Seattle Seahawks football player burning an American flag, while his teammates cheered him on.

The player in the photo was one of those who "took a knee" during the playing of the national anthem at NFL football games, and the image was modified in an attempt to besmirch him. The original photo, which showed Michael Bennett doing a victory dance in the locker room, was taken almost two years earlier. But the doctored photo was shared on social media tens of thousands of times.

The same thing happens when people with a political axe to grind create fake photos. One recent example shows President Trump rescuing cats after the flooding in Houston. There were also fake photos of former president Obama, supposedly kissing the Prime Minister of the United Kingdom.

And then there are the hoaxsters, who create fake or outlandish images by using photo editing tools such as Photoshop. The "Giant Squid on Santa Monica Beach" photo (shown here) is one such example. The Gallery of Fake Viral Images has many more examples of doctored and misrepresented photos that have been passed along by lazy or unthinking people. (See also the Field Guide to Fake News Sites and Hoax Purveyors.)

You don't want to be one of those people, and you don't want to be their unwitting tool by falling for and spreading their manure.

Unfortunately, a lot of people fall for it and spread it even further. If they had the knowledge and had taken the time, they could have discerned that the photos they shared were entirely bogus. Here is how you can do it, and avoid being a pawn of hoaxsters and propagandists.

How to Identify Fake Photos

Check when the photo was taken. Doctoring a real photo of a tragedy is a complicated and time-consuming process. It's much simpler to take an older photo out of context and link it to a news story about the tragedy. If you can determine that an image was made before a tragedy, but it claims to depict the actual event, you can be sure it's fake.

One way to check a photo's age is to look for prior use of it. Google's reverse image search feature will find matches and near-matches to virtually any suspect image. If you use the Chrome browser, the simplest way to perform a reverse image search is to right-click the image you see on a website, and then click "Search Google for this image." You can also search using the image URL, or drag and drop the image. See the reverse image search help page for instructions.

TinEye.com is a dedicated reverse-lookup image index. Just right-click on the suspect image, select "copy image address," and paste that address into the search box at TinEye. If you find a suspect image in a context that puts it clearly before the date of the real event, consider it fraudulent.

This BBC article has some tips on identifying the signs that can reveal a fake photo. Checking the reflections, and even the color of a person's ears in a photo can be telling.

Videos can also be misrepresented, and can have even more powerful disinformation effects because video is more "credible" than still imagery. There is no reverse-lookup site for videos; the technical challenges are greater. Researchers at the University of Washington have created a tool that uses artificial intelligence to create fake videos. In this example, the software is used to put words into a synthetic Barack Obama's mouth.

Amnesty International has partnered with YouTube to create a YouTube DataViewer but its limitations make it unreliable. First, it only covers videos uploaded to YouTube; contrary to appearances, that does not include every video ever made. Second, if a video is edited in any way, even by trimming off a few seconds, its metadata will no longer match the original and it won't be found in a DataViewer search.

Take a Look Under the Hood

Sometimes the most reliable information about a photo is stored in the photo itself. Called EXIF Image Data, this hidden text includes such valuable information as when a photo was taken; what kind of camera took it; and even the geolocation coordinates if it was taken with a smartphone that had "location services" enabled. You can right-click on the photo and click "Properties", then "Advanced", to take a look at the EXIF data. Jeffrey Freidl's Image Metadata Viewer can even pin a photo to a map, if it includes geolocation data.

If you find that a heartbreaking photo of a little girl covered in mud and holding an equally sad puppy was actually taken in Australia, you can be sure it is not a photo of a Bosnian war orphan.

EXIF data can be altered to deceive, but most of the people who spread disinformation this way are not that technically savvy. You can catch a lot of fake images by looking at EXIF data.

Also, consider the source of an image. If someone in New Jersey is feverishly posting outrage-inducing photos “in real time” of an incident taking place in Germany, it just doesn’t make any sense. As Judge Judy loves to say, “If it doesn’t make sense it probably isn’t true.”

Twitter’s Advanced Search enables you to rule out such frauds by restricting searches to the location where you know the event is or has occurred. Facebook can also tell you the location of a user.

Finally, you can Google it, or use Snopes to check out things that seem odd or salacious. If you don't like Snopes, use another myth-busting site such as Hoax-Slayer or TruthOrFiction.

Bottom line, don't believe everything you see online. You can avoid looking foolish, or playing into the hands of ill-intentioned scoundrels by doing a few seconds of research before passing along a photo or story.

Your thoughts on this topic are welcome. Post your comment or question to “askbobrankin.com”.

..----------

Download YouTube Videos As MP3 Files

toggle-button

Submitted by rob.schifreen | Last update on 28th November, 2017 - 6:44am

I'm always interested in new sites that allow you to download a YouTube video as an MP3 file, as it's a great way to be able to play a music track on your PC. My latest discovery is something called GreenMP3, which you'll find at www.greenmp3.com

.

Just paste in the YouTube video URL, wait a few seconds and your MP3 (or MP4 video if you choose that option) is ready for downloading.

NOTE: When you first visit this web site your browser will ask if you wish to grant it permission to display notifications. To avoid any unwanted adverts, say no. The site will still function just fine.

New Google Tool Makes Snoopers Vomit Rainbows

By John Lister on November, 29 2017 in “Infopackets.com”.

Google researchers are working on a way to warn users when someone else might be sneaking a peek at your smartphone. They say it can spot a gaze in just two milliseconds.

The project is the work of Hee Jung Ryu and Florian Schroff, who'll demonstrate their work at a conference on Neural Information Processing Systems. It's based on a remarkably simple concept with some smart technology.

Front Camera is Key to Tool

In its current form, the system runs on a Google Pixel phone and takes advantage of the front-facing camera - the one typically used for face / video conferencing before it became dubbed the "selfie camera."

The system not only detects human eyes in the picture, but figures out the precise direction they are looking in and the person's position. The idea is to decide if they are intentionally looking at the phone's screen or merely looking in that general direction.

If the system detects two sets of eyes (that is those of the phone user and somebody else) it can give an alert. In a demonstration video, this involved the phone switching to a camera view with a crude message reading "STRANGER is LOOKING ALERT!!!", a red box around their face, and an animation of rainbow vomit falling from their mouth. (Source: **theverge.com**)

Suffice to say, this particular alert is for the cultural amusement of the researchers and would be somewhat refined if the software was released publicly.

Older Phones Might Struggle

There are a couple of things needed to make this feature a viable tool on Android phones. One is that the detection would have to accurately distinguish between a person deliberately looking at the screen, compared to merely happening to glance at it by accident.

The other issue is that artificial intelligence is needed to accurately calculate whether or not a stranger is in fact looking over your shoulder. This is often done by sending data over the Internet to remote servers for processing. In the demo, this was possible but in reality this would likely add too much of a delay to be useful. (Source: **qz.com**)

That said, the processing power needed to run the application means it will only run on high end smartphones. And, since it's an app that is constantly running in the background, it also means that it will drain battery and eat bandwidth constantly. That may be enough to make it not very user friendly unless you have exceptional battery life, a cutting edge phone, and lots of bandwidth to spare.

What's Your Opinion?

Would you find such a feature useful? Thinking of the way you use your phone in public, do you ever have data or information on the screen that could be embarrassing or threaten privacy or security if somebody else saw it? Can you see this becoming a real phone feature or is it more of an experiment?

This subject has been in the news a lot!

Former Exec Slams Facebook for 'Destroying Society'

By John Lister on December, 12 2017 in “Infopackets.com”.

A former Facebook executive says the site is responsible for "ripping apart the social fabric of how society works." Chamath Palihapitiya says the problem isn't restricted to the US.

Speaking at the Stanford Graduate School of Business , Palihapitiya said he felt "tremendous guilt" about his role as Facebook's vice president of user growth. Talking about the way Facebook tried to get users to stick around on the site, he echoed the comments of former colleagues in likening it to psychological manipulation.

Social Media Works Like Drug

He referred to "dopamine-driven feedback loops", referring to the way users get a small burst of pleasure from seeing a new post or getting a notification of a "like" on their content, then come back to the site in the hope of repeating that pleasure. Dopamine is a chemical in the brain that acts as something of a reward system and is often associated with addictions.

Palihapitiya said the problem is that the emphasis on these feedback loops takes priority over Facebook being a genuinely useful tool for fostering civil discussion and sharing accurate information.

He noted how this can lead to false but eye-catching and provocative 'information' being more likely to get shared and spread, with the problem occurring this way even before organizations start deliberately trying to manipulate the news people see.

Tech Investment Under Fire

He said he no longer uses Facebook at all, claiming that it is "eroding the core foundation of how people behave by and between each other." (Source: **gizmodo.com**)

Palihapitiya also aimed at the wider tech business community, particularly the way new companies get investment through venture capital. Typically, investors risk their money in the hope that their share of the business becomes valuable when it takes off. He said this approach meant investors were chasing quick profits, meaning companies that are more likely to benefit society in the long term struggle to get started. (Source: **theverge.com**)

What's Your Opinion?

Do you share Palihapitiya's views? Do sites like Facebook have benefits that outweigh their cultural negatives? Can any tech company or Internet site still improve society once it becomes a huge business?

THOUGH FOR THE MONTH.