Article from

Reinsurance News

July 2018
Issue 91

Don't be Naive About Social Media

By Mairi Mallon

Do you know what access social media companies have to your personal data? Use your smarts to continue using this useful tool, while keeping your information safe.

I'm assuming if you are reading this publication that you are smart, that you have at least one degree and have had to use those brain cells a lot. So, let's assume none of you are at the bottom of the class (and never have been).

So why is it that when it comes to social media, so many clever people lose their smarts? They not only post away, allowing people to know when they are abroad, (it really is silly advertising that your house is lying empty), but on a much more sinister level they give away information that you wouldn't pass on to family members.

Those Facebook tests? The ones that say, "post your favorite albums of all time," or "what your Game of Thrones character would be called?" These are blatant phishing exercises designed to get you to tell them valuable pieces of personal information such as your first pet's name, your middle name or your mother's maiden name, your first street name and mix them up to come up with some meaningless name. While taking these tests, you very often also have to give the app access to not only your photos, data, posts, but also those of your Facebook friends.

Would you do this in any other situation? If you need it explained, many of these apps are simply finding out the answers to your security questions. I actually saw one quiz last week that not only asked for your mother's maiden name, your date of birth (in various stages), the first street you lived on, and, wait for it … the last four digits of your credit card. If I could print the emoji with wide open eyes, I would. The crooks no longer have to go through your bins looking for your details, they create apps that gamify data harvesting, and we happily walk into these traps.

To be honest, the recent scandal with Facebook sharing data should come as no surprise. Social media sites make money by collecting data and selling it, usually to advertisers.

Just to jog your memory on the Facebook story, the Cambridge Analytica privacy scandal erupted on March 16, prompting the hashtag #deletefacebook. Reports in newspapers from *The Observer* to *The New York Times* said Cambridge Analytica, which is a political data-mining and consulting firm, collected and accessed over 50 million Facebook users' private information without their knowledge.

The data, originally claimed to have been collected for academic purposes, reportedly was later used to target Facebook users for crafted ads and messages for President Donald Trump's 2016 election campaign.

Facebook CEO Mark Zuckerberg spent two days testifying before Congress because of the outrage at what the legislators saw as the irresponsible use of personal data. Cambridge Analytica has since shut down.

What makes this story so different from many other breaches is that Cambridge Analytica didn't steal this information, instead it was given to the company.

And we willingly gave it to Facebook. One good thing to come out of the scandal is that, finally, the general public has woken up to the facts that a) Facebook (and other social media) make money from selling your data; and b) that whirly tab at the top right for settings should be looked at and access restricted.

I recently helped a friend from the U.S. look at her settings on Facebook. What was amazing was how hard it was to get to the granular information they had stored—and then how detailed it really was! It had a list of her interests, from mommy groups, to age ranges, to the kinds of houses she likes. It even had an analysis of what political party she voted for (she is quite political in her posts, so in fairness, not that difficult to tell). What was interesting is that she had left the door open for apps that had access to her friends' accounts, as well as finding that her friends had unwittingly allowing apps to access all her data as security doors had been left open.

So, it is really important to go through your Facebook settings, particularly the apps that others use, and switch off everything you can, unless you want to give away all your personal data when a friend plays one of those quizzes. They take everything you ever posted and everything your friends posted unless you've gone deep into your settings and switched it all off.

And it is not just Facebook. Have you checked your LinkedIn settings recently? I train people in LinkedIn, and more often than I would care to admit, when I have a look at what LinkedIn is now accessing on my account there are several new buttons, each one set to its most open setting by default. It is the way they get around you shutting it all down. While it can be great to be able to spy on rivals, bosses and work colleagues (and who

has not done this, to be honest), remember that, generally, if you can find out that stuff about someone else, they can find it out about you.

If you look at the detailed analytics available on Twitter about your followers, you know they have the access to a great deal of your data. Settings can also be set to restrict this access. They have lists of your interests, what you buy, estimate how much you earn and can find out exactly where you have been. Have a good look, and check you are happy to share this information.

So, just how dangerous is it to not have closed everything down? I'm not a person to be overly-worried about being found. I've not been stalked or harassed and work in the rather tame world of insurance and reinsurance where I actually want people to know who I am. That is why I am on social media, to promote myself and my company.

In today's inter-connected world, there is so much data being harvested about us, most of which I could not care less about. What I do object to, however, is social media companies taking this data without me realizing I may have given permission by mistake, or it has been assumed.

There is more damaging data that can be harvested, however. Health data—this comes from apps accessed from gyms, or from smart watches which monitor our heart rate, exercise … even our breathing. We have our banking apps on our smart phones.

Below I've listed top tips on how to keep safe on social media. Remember that you need to, on all your social media platforms, go in and play around with your settings—and take the time to delve deep.

Reuters recently said that Facebook executives "have apologized for the data-harvesting, pledged to investigate others who collected Facebook user data and reduced the amount of data available to similar app developers now."

The power to really restrict access, however, lies in our hands. If we learn how to make our data more secure, then we can prevent it from being harvested in this way.

Just use your smarts. You have plenty of them.

TOP FIVE TIPS ON KEEPING SAFE

1. **Don't panic.** The world will not fall on your head because of social media. Go to your settings and take your time to shut down the access they have to your information and how they share it with third parties. It is not hard and there are many, many articles on this on the internet. Set your settings to a level that is comfortable to you. Really think about it and give it some time. For an example, see here: https://www.zdnet.com/article/facebook-private-data-settings/

2. **Secure the most important stuff.** I would not bother with a two-step verification on sites like LinkedIn, but you should use two-step verification for your most important sites, like banking and health apps. These should have a code or fingerprint after the pass codes. Facial recognition is really useful as a way to secure your device against unwanted access.

> What you put on the web can last a lifetime. You can delete a tweet or picture, but there is always a record of it somewhere.

3. **Ask questions.** Ask why you're giving certain information. If you're taking an online quiz, it doesn't need to know your address and phone number. Be careful if you feel uncomfortable disclosing information. Scammers can be putting together a profile on you based on the info you give. That whirly little cog at the top right is where you look to see what access apps have to your data and your friends' data.

4. **Share with care.** What you put on the web can last a lifetime. You can delete a tweet or a picture, but there is always a record of it somewhere. It does not disappear completely. Before putting up a post about yourself or yourself with friends, think about how it will look. Tequila shots may be OK at college, but may not be taken to too kindly in our sober working environment.

5. **Spring clean.** Look at all your apps often and have a look at what they are trying to find out about you. Get rid of the apps you aren't using and question free apps that seem to want to know too much. Watch what access they have to your social media and other data.

HOW I BECAME @reinsurancegirl

Ten years ago, I set up a public relations firm, rein4ce, with Stephen Breen to service the global insurance and reinsurance market.

What we understood from the get-go was that in order to be a communications firm of the future, we had to master social media. At the time, there were hundreds of self-appointed "social media gurus" and I spent a lot of time reading up on what they were saying. A lot of it was based on business-to-consumer promotion or self-promotion. Almost nothing had anything to do with business-to-business communications, let alone our small, rarefied world of insurance and reinsurance. I spent a lot of my time almost giving up, sitting with my head on my keyboard.

To say I'm not a digital native is an understatement. I was born in 1968, and have just turned 50. I read real newspapers, and prefer real books over my Kindle. I'd still rather pick up the phone or meet in person than send an instant message.

So, this new way of communicating did not come easy. But I had to master it, and master it I did. I remember picking @reinsurancegirl as a handle as I thought it was funny, getting my 50th Twitter follower and being super excited.

I remember connecting with others who were trying all of this new-fangled media out in our world. Stand-outs were Alicia Montoya at Swiss Re and Tom Johansmeyer at Guy Carpenter (he's now at Versik, and both are now doing very different jobs). Conversations with other communicators with many more years' experience than myself were key to learning—James Peavey at A.M. Best was a great sounding board and then willing Guinea pig. Friends such as Alayna Francis, then Swiss Re, now Marsh Group, and Harvey Smith, who is doing something super-clever and InsureTechy now, have helped me wrap my old head around new communications ideas.

But the biggest revelation is that there is nothing really new about this kind of communications revolution. Yes, it is much faster. Yes, it is much more public. But good communication is still the same. Work out what you want to say, and who you want to say it to, and you will win every time. Know your audience. Know your subject. Know how to write. The rest is just really learning new technical skills, which is about the same as moving from a Blackberry to an iPhone, a fax to an email, telex to a fax, a telegram to a phone call. Maybe once I wrap my old brain around Snapchat, that will be the next thing I will find a use for and will have to show clients how to use. What I do know is that technology never stands still, and to stay relevant we all have to keep up. ■

@Reinsurancegirl, aka Mairi Mallon, CEO of specialist insurance and reinsurance PR firm rein4ce. She can be contacted at *mairi.mallon@rein4ce.co.uk.*