Google yourself

BY CAROLYNE REGAN

It is not the punch line of a juvenile sex joke. It's a reality check. You have just gone viral. You want to be the new sensation exploding exponentially through e-mail, and the entire chain of social media and networking sites. Instead, you are the victim of a prank gone horribly wrong as you gaze at the image of yourself in one of those mock inspirational posters. You are a humiliating embarrassment. Okay, maybe not, but you could be if you don't read this.

Google yourself. Make a habit of it every 6 months, or so. When daylight savings time comes, we remind ourselves to change the batteries in our smoke detectors, change the filter in the A/C or furnace depending on the season. Why not give your reputation a check-up as well?

Trust me, I know.

A well-known colleague of mine was the victim of internet extortion. Why? Because of a Facebook account. That account has since been closed, the slander removed, the damage – which was considerable – has been repaired. It is amazing how quickly one libelous comment can mess up your life. And that mess took hours and hours to clean up. In a world where time is money, you just cannot afford that kind of destruction to your reputation.

So go on, do it now, and Google yourself. After you type in your own name and hit enter, you may be very surprised, even shocked, at what you may see. Your whole life is up for grabs, by anyone, anywhere. You have potentially placed yourself, your family, friends and even your coworkers in danger at the hands of scam artists, hackers and extortionists.

We willingly place the entire contents of our lives on our social media accounts. On Facebook, for example, how many "friends" do you have? How well do you really know these people? All of them have access to your birth date, your address, the name of the company you work for, photos of your children, photos of your drinking binge at a nightclub party. Your information can be used and your photos copied, by anyone who you have included in your network of friends.

All of these bits of information have the potential to go viral, globally. In less than a nano-second, the entire Earth could have access to every detail of your personal and private life. The chances of you being scammed, extorted or used as the butt of a sick joke, have just skyrocketed.

You, however, are smarter than that. Or so, you think.

Perhaps you see no need to worry because you have changed your privacy settings so that only your friends can see your information. Or maybe you are even more sophisticated and have created customized lists of who can see certain information. You may have even blocked your accounts from being "discovered" by search engines. And all of your accounts are accessed through anonymous e-mail accounts from services like Hotmail or Yahoo! mail.

Well, you are wrong. You should definitely worry. In fact, be very afraid. Because for every sophisticated social media user, there are 20 internet hackers who can break through all your precautions before you can figure out how to delete your account. Most of those hackers don't even hack. More often than not, no hacking is involved. Instead, you have been offering yourself up as the sacrificial lamb.

I probably should not pick on Facebook. Twitter is just as much to blame. I have never used Twitter personally, but the means and the results are the same. In either site, every commercially represented page you join, comment on, every group you subscribe to, potentially shares this information with other "profile networks" such as ProfileEngine.com and Pipl.com.

And make no mistake. If you have a Facebook or Twitter account, you are on there. So was my colleague, who although well-known, is just one of us regular people – not a famous personality or spokesperson or corporate figure.

The ProfileEngine and Pipl sites are not the ones you need to worry about. There are other parasite networks and links that use your information for more sinister purposes. These sites do not have privacy policies or codes of conduct. Their sole purpose is to gather any information that can be used against you.

But why would anyone want to do that, you ask? Maybe

someone wants to get back at you for a bad break-up or messy divorce. Maybe someone wants to ruin your career in order to advance their own position. Or maybe they just want your money.

Do you even realize that you have been the victim of an internet extortion scheme? Most victims don't. And you won't know either until you Google yourself.

Internet extortion sounds like something that happens to large corporations or that is funded by underground political groups. It brings to mind images of sophisticated code-breakers, secret files, encrypted documents, ground-breaking scientific technology and millions of dollars. That is a possibility, but closer to home it is much simpler than that.

Would you be willing to shell out $19.95 plus tax to clear your name of slanderous comments that could potentially ruin your career and destroy the sterling reputation you have built for yourself? If you answer yes, you have just become a victim of the kind of thinking that internet extortionists count on. Which is worth more – one theft that nets $100,000, or scamming thousands of people out of $20 each. When you consider the more than 800 million people who use Facebook and Twitter, the potential is staggering.

My colleague, who is in the process of changing careers, wanted to make sure that that road ahead was clear. She performed the Google-check that I am urging all of you to do when you finish reading this. She discovered her own face on another website. Beside her face were the comments "is cheating .....", "don't trust this person!!!!!!!!" and "yes be aware.." Quite understandably, she panicked. She was convinced that her sleazy ex-boyfriend was out to get her, especially when she saw that the comments had gotten several thousand hits.

That is exactly what the creators of this website were counting on. So when my colleague noticed the link to "Remove this profile" she clicked on it. The link took her to a PayPal payment page. For just one payment of $19.95 to a PayPal account, the slanderous profile and all its horrible comments would be removed. Sound easy? Of course it does, it is supposed to. The simpler and less expensive it is for you to fix your life, the more likely you are to hand over the money first and ask questions later.

The website advertises itself as a website where you can submit "Anonymous comments about every facebook and twitter user." Apparently, you are free to bash ▶

anyone you want without fear of discovery or retribution. Sounds like every teenagers dream.

The truth is this website and others like it are scams. No one submitted malicious comments to this website. The comments were generated by the websites creator in hopes that their victims would be willing to pay a paltry $20 to protect a reputation. At a rate of almost 5,000 hits per day, the potential pay-off is not so paltry. The reason it is all so believable, is because of the valid and current profile picture from the Facebook account of the victim which is accompanied by the url for that Facebook account.

Even if you are not on Twitter or Facebook, you are still not completely safe. If I have not quite convinced you of the potential danger, read on.

After I did a little bit of digging, I discovered just how far the tentacles of extortionist websites reach. This website is owned by a company based out of Los Angeles, California. I had never heard of it.

But I had heard of Amazon.com. Amazon is the hosting company for the website. I am not suggesting that Amazon is in anyway responsible for the activities of an internet extortionist. I shop on Amazon and I will continue to do so. Amazon is one of the safest internet companies I have ever dealt with and I deal with them a lot. I just want you to be aware that these people are not just computer geeks who live in their mother's basements. The connection between you, hundreds of multi-national internet corporations and every scam artist in the world, is only a click away.

The purpose of this company (according to its website) is to "Protect Your Privacy" from spammers. Ironic, isn't it? And if that is not enough, the company is the owner of many other websites (I saw a list of only the top 10), each of which have different hosting companies. And those companies are in countries all over the world. The content of these sites includes games, online stores, news services, cartoons, porn and much more. At least one of those sites has more than 7 million visitors on a daily basis.

Those tentacles reach far and deep.

Don't cancel your Facebook account just yet. There are good reasons to have one. I use mine to keep in contact with distant relatives. If you are starting a business, it is a good way to network and get noticed. But you also need to be aware that you are not in control. They are.

The way for you to take back control, is to know what is out there. You need to find out exactly what the world knows about you. If you know how and where your personal information is leaking, you can clean up any potential mess before it does irreparable damage to your reputation and your life.

After you find out just how global your personal life has become, do a little housekeeping on that social media account you pride yourself on. Get rid of those 873 "friends" you don't even know and keep only the 97 you actually do know. Take down the photos of your 4-year-old on her first day of kindergarten with the name of the school in the background. Think twice before twittering the intimate details of your weekend activities. Don't display your birthdate or where you work – people who are actually in your life will already know that. Remove any attachment to commercial sites, links or "likes" that are partnered with other sites. Learn more about the privacy options available to you – and use them.

When you are finished tweeting or posting, log out of your account and clear your cache, which will remove the cookies stored in your browser. Logging out of your account disengages your browser from web applications; however, those informative little cookies including your account number are still available to be passed along to all requests through facebook.com – yes I mean all requests. It's called frictionless sharing. Every page you visit that is integrated with Facebook continues to be tracked by Facebook even after you have logged out of your account. The only way to stop this is to delete the Facebook cookies in your browser or to clear your cache.

Web based scam companies are just one example of the potential harm that the internet can cause. Scams and extortion can come in many forms from anywhere at any time. And keep in mind that not all schemes are designed to come after you for your money. Sometimes those schemes are created to wreak havoc simply because they can. Internet parasites are everywhere. We will never escape them completely, so let's not make it easier for them by providing them with ammunition. At the very least, we can arm ourselves with the knowledge of how our information is used and distributed, and cut off that flow of information before it comes back to haunt us.

Six months from now when you change the clocks for fall, remind yourself to give your reputation another check-up… And Google yourself. WLM