

ZEST Digital social media case study on identity theft through social media

Steven Lewis:

Hello and welcome to another ZEST Digital social media case study. I am Steven Lewis and I am a director with ZEST Digital. ZEST Digital is a social media consultancy based in Australia and this podcast series looks at how social media is being used in Australia particularly in a corporate environment. In this episode I talk to Anton van Deth from Symantec in Australia. Symantec is well known for their range of protection software for consumers and companies. We talk about identity theft which is growing at a frightening rate and is particularly an issue for users of social media. Social media invite us all to put a lot of information about ourselves online and some of that information if not carefully used and protected can lead to identity theft. I started by asking Anton whether identity theft was a particular problem in Australia.

Anton van Deth:

Identity theft world wide is an issue and the internet is a worldwide network of tools and applies equally here in Australia and the Australasian consumer fraud task force recently in March this year did a study and their results came back that in Australia alone sorry in Australia and New Zealand it is over a billion dollars worth of fraud committed through loss of identity and that's a significant number from people losing their passwords, having their identity stolen etc. Once that information is gone it is very, very hard to get back so protecting our identity is really key to our online safety as we go forward.

Steven Lewis:

So banking details are probably the most obvious one to people, what other sort of personal data are necessary to steal identity?

Anton van Deth:

Oh look it is fairly easy to do if you are really good as a hacker and Facebook and some of the social networking sites where people are putting a lot of personal information up, they're putting their age, their mother's maiden name, their favourite pets, their hobbies, where they'll be and that kind of information can be used either in terms of a predator trying to find you or a cyber criminal trying to hack into your passwords. Passwords are a good example, most people if you forget your password on a website, you'll say email me my details or they'll ask you a private question, what's your mother's maiden name or what's your dogs name; there are a standard set of those and if you're putting that kind of information up its very easy for somebody else to work that out. So any information that involves you personally can be a risk to you if you're not careful with that.

Think about it in the real world versus the online world. If somebody walked up to you in the street and said g'day can I have your name and your address and oh actually where do you do your banking and I've got this great thing down the side here if you want to spend five bucks on it I'll guarantee a \$300,000 return, you wouldn't fall for it for a second. Applying the real world skills and techniques that we have to the online is a really good way of helping protect ourselves.

Steven Lewis:

So we've got a situation now with social networks, lets take Facebook as an example because I get very excited about Facebook myself at the moment you've got a lot of opportunity to put up a lot of the sort of information you were talking about; has social networking increased the opportunity for identity theft?

Anton van Deth:

I think there are two ways of looking at this, the tools like Facebook in themselves are terrific and they really encourage that greater sharing and community to take place particularly with this new generation who actively will spend more time on a Facebook site than they will at a shopping mall. The downside to that is that there's no guideline, there's no tools for people particularly those who have not grown up in a situation where they've had their identity stolen or at risk to just put anything up there. To put comments about people that they don't like or to be very aggressive with that sort of stuff or to put photographs, photographs are a really good example if you were putting a photograph of yourself doing something strange and unusual. A teacher for example in the United States put a photograph of herself drinking, unfortunately she did that when she was in training and was underage, instantly she couldn't

get a job, couldn't get her degree that kind of thing can come back to haunt you.

Children these days will put up all kinds of information in the belief that a) they're anonymous or b) that they can take it down; and the reality is that you can't. You might be able to take it down from on that website but that may have already been searched and crawled over by a number of different search engines, not just the big ones, it maybe backed up somewhere or somebody else may have copied it and linked it and once it is up there its up there permanently. So applying rules like don't put something up there that you wouldn't put on the front page of the major newspaper and that you'd be comfortable with your grandmother reading, just thinking about that beforehand will prevent a lot of that kind of information coming up.

Steven Lewis:

Now this is back to a more philosophical point of view. If a company puts up some sort of social networking site as many of them are doing now so that their customers can share photographs and experiences, whose responsibility is it do you think if somebody puts up a photograph that might get them into trouble or make a comment?

Anton van Deth:

I think there are always two sides to this, when you have two players involved both are responsible, for example Symantec is very careful, we're running a photo competition, we did last year, encouraging people to use these sorts of things but we will vet those to make sure that there's nothing criminal or dangerous to put up because we take that sort of responsibility very seriously. Other websites probably won't they just allow you to continue to post. For example UTube is quite conscious of this and if there's something that comes up that they feel is inappropriate they will pull it down but it is equally incumbent upon the person putting it up to think about it because you can't necessarily always trust the person you're putting it up to and you may trust them but that might be copied or used by somebody else so it really is a two way street and we all need to work together on this to combat this kind of abuse.

Steven Lewis:

What can be done?

Anton van Deth:

If you look at it from the point of view of deal with reputable sites, deal with organisations who have a privacy policy that you can log up to, deal with organisations that you know you can reach in the real world, that's the first

step. The second one is to actually look at the content that you're putting up there and apply that real world principle, if I had two people sitting in the room, one person I trusted and the other one I didn't know and looked kind of dodgy would I be happy showing them both the same thing and if you're feeling still comfortable at the end of that double check it one more time, is there anything in there that may be used against me later down the line and if there's not go for it and enjoy the net; the net has lots of positive things to explore and to use but we need to just couple that with a little bit of common sense.

Steven Lewis:

So flip that round for a company building its social network or a site of this kind, they need to have that stuff very much in mind and they need to make it easy for users to check what they're doing?

Anton van Deth:

Absolutely and security software these days, both ours and the industry that's out there at large, can be very good at analysing websites and predicting and picking up when things are not right. So as an organisation if you're creating a shopping site or a social networking group that contains tools or a code in it that is going to set off alarm bells, your customers are going to stop coming to you. This is very much the self serve generation where customers will go online to buy from you directly, I mean for myself I went online just recently to buy a headset for my flying directly from the US because it was cheaper and quicker but I was able to look at the site first, I knew who I was dealing with before I gave my credit card. If I didn't feel comfortable I wouldn't have bought there and that's becoming a pattern of behaviour.

Steven Lewis:

So if you're a company building a site you really ought to be running your own site through these checks?

Anton van Deth:

Very much so. Run both your own internal security software using your firewalls and so forth but look at it from your customer's point of view, log on through a system that has internet security installed and if it does set off alarm bells look at it and if you still have problems and you don't know what's setting off alarm bells contact that security agency such as ourselves and we'll be able to help you identify where those issues are.

Steven Lewis:

In terms of companies whose employees are using social networks possibly while at work, there are a lot of corporate or business related social networks, is there anything you think a company should be doing with their employees?

Anton van Deth:

The social network, instant messaging tools are really good examples of advanced that help people communicate far more effectively over quick topics etc. You always take two approaches, one you can turn it off or you can put a wall around it but the trouble is that will reduce your productivity and make you uncompetitive. So how do you combat that? Well first of all you install the relevant security software but talk to your staff, talk to them about what they're putting up. Symantec for example internally will constantly be talking to us saying hey look this is what's going on out there, don't put this up, be careful of this, so we have this whole process of constantly educating ourselves. The same thing needs to go as consumers, just keep tabs on what's going on. What a lot of organisations are doing now, and what we would recommend them to do, is to have an internet user policy which staff sign when they join outlining what's appropriate, what's not appropriate, so it is clearly communicated and for tools like instant messenger or new ones that come up have one for those as well, don't make it too onerous, too difficult for them to understand the top key points and you'll make the security and safe transactions and data much better by simply having clear communication to your staff.

Steven Lewis:

You wouldn't encourage people to stay away from Facebook or MySpace?

Anton van Deth:

No no, look really the net is a fabulous place and the opportunity for us to grow as both a nation and our children and to improve things overall is most definitely beneficial by using the net. I think the real world is full of crime, the real world has bad people in it but we still go about, we still drive a car and we still go to the movies because we apply the basic behavioural tools and we equip ourselves with the relevant things to protect ourselves. Apply those same principles online and you'll enjoy the benefits of it and so will our children.

Steven Lewis:

I would like to thank Anton van Deth from Symantec Australia for coming in and talking to me about identity theft from a social media perspective. If you'd like to talk to me about how ZEST Digital could help you with your corporate social media campaigns either from a consultancy point of view or from an execution point of view, you can find me at steven.lewis@ZESTdigital.com.au, that's



Steven with a 'v' and L E W I S. This podcast is available from our website ZESTdigital.com.au where you'll also find examples of the work that we've done for other companies. You can leave a comment on this podcast on the blog page or the podcast page at our website and I'd like to thank everybody who has commented so far. Also do please subscribe to the podcast which you can do automatically and for free just by clicking through the appropriate links on the website and that will make sure that you receive all future episodes of this podcast automatically and absolutely for free. Of course you can unsubscribe as well at any time that you like.

Thank you for listening to this ZEST Digital social media case study.