Personal Data For Sale – In time for the Holidays!

Peter Silva, 2010-04-11

Come one, come all! Are you tired of using your own money for those big holiday purchases? Are you wary of entering your own personal & financial information to get that special gift? Would you rather spend a stress-free holiday season impersonating various folks? Just in time for your holiday shopping, get your very own unlocked identity profile!! Why go through the hassle of protecting your own information when you can just pretend you are someone else? For a limited time we are offering everything you need to create your own shopping character – name, address, bank/credit card info – and if you act now, we'll include the user names and passwords for 5 social media profiles!! Call Now! Operators are standing by…

I got a call yesterday from a well-known national bank letting me know that there may have been some fraudulent activity on my account and to enter my info to verify the charges. First, I don't have an account with this institution but played along. The automated system gave me the name of the person they were trying to reach but I couldn't go any further since I didn't have their info. I tried to zero out but the annoying prompts kept scolding me that the info I entered does not match their records. Initially, I thought that this might be a phone scam attempting to get sensitive info but upon further investigation it was the actual bank. I called the 800 number back and finally got to a human. I explained the situation and got connected with the fraud department. Apparently, my number is still associated with a customer (actually 3 customers) and they will correct the database. But it got me thinking that I might have been able to pretend I was that customer and through a little social engineering, get their info. I already had their name and associated phone number, it doesn't take much more to create a persona and demand that I am who I say I am.

Just this past week, I also got a nice email from another financial institution alerting me that my account's Online Access Agreement had been updated and I need to logon to confirm my identity, over a secure connection of course, to read & accept the new agreement. I was urged to partner with them to prevent customer fraud. What a great idea… unfortunately, I don't have an account with them either! The link to the 'security update' went to tiktak.com.br (intentionally left out the rest) and the source showed that it was also sent from Brazil. I sent to the abuse department of the bank and to the FTC. Not surprisingly, the bank's reply did confirm that it was a scam.

While many of us are aware of the dangers of clicking on an email link that looks suspicious, crooks are still using this method to pilfer and even if only a few fall for it, it's still a success. According to the Identity Theft Resource Center (ITRC) as reported this past June, data breaches are up in 2010. 498 total breaches were reported for the entire 2009 calendar, including those high profile exposures and for the first 4 months of 2010, 245 breaches were reported. Well on the way of breaking 2009's numbers. The scary part is that only 8% of all breaches are reported, according to the Australian Crime Commission. In the states, I've seen statistics saying that 89% of security incidents go unreported. Either way, reported statistics for electronic fraud are well below the actual damage. And it'll probably get worse as more and more mobile devices are used to conduct sensitive transactions. And don't get me started on social media. I'm still amazed that just 10-15 years ago when we all had answering machines (remember those?) we were warned that you never say as part of your outgoing message, '*We're not home right now….*' since that tells criminals that the place is ripe for the pickings; the message should say, '*we can't get to the phone right now…*' Yet, just a decade later, thousands of people are telling the world, '*Hey we're a thousand miles from home having a wonderful time – check out the great photos*,' all with GPS info included. The profile has their hometown, kid's schools, latest expensive purchases and a picture of the new addition to the house. I realize social media is a great way to share with family and friends and has many benefits both business and personal but we do need to be aware of the type of information we choose release. And with the holidays coming, that data is extremely valuable to outlaws. This is just a friendly reminder to protect yourself, reduce your risk and pretend you have an old answering machine before the madness of the holidays is upon us. I guarantee we'll be seeing a number of data theft stories at the peak of the shopping season and wanted to get a jump on it now – before all the clutter arrives in a few weeks.

ps

twitter: @psilvas

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com