

[Click to view this email in a browser](#)

Identity Theft Resource Center



ITRaC News - Q4 2009

A Message from the ITRC

As we enter into the New Year, it is vitally important that consumers and businesses alike remember the need to be continuously diligent about protecting personal identifying information. The ITRC predicts an increase in identity theft and related crimes over the next two years unless significant changes are made in information security ([2010 Trends](#)). Many of us are growing tired of hearing about it. But, the fact that we are tired does not make the impact of the crime any less significant on either the victim or our society at large.

There have been several studies conducted over the past few years reporting on the annual number of victims of identity theft – with results reported ranging from 8 to 15 million cases a year. The ITRC has always felt that these studies largely focused on financial identity theft issues, and didn't accurately reflect the whole gamut of cases, especially the tough to repair governmental and criminal identity theft cases. We also felt that these difficult cases were largely under reported, since there was no effective manner of even determining how many victims had criminal and governmental problems with their cases.

Since July 1, 2009, the ITRC has responded to more than 4,400 identity theft victim cases. At that time, the ITRC began tracking a variety of attributes attached to these identity cases (other than financial), such as "governmental", criminal, child identity theft, internet takeover and medical identity theft. These attributes are not "self reported" by the victims, but are recorded by knowledgeable victim advisors as they help the victims mitigate their cases. This is a much more accurate method of determining just what types of identity theft are involved in a particular victim case. Nearly 38% of the victims (7/1/2009 to 12/21/2009) were identified as having serious non-financial attributes to their case. Six months of data, over 4400 cases is certainly enough to see some trends. The ITRC sees this as a strong indication that more complex cases of identity theft are



In This Issue

[Identity Theft - What's it all About?](#)
[The Sandbox](#)
[Social Networking](#)
[ITRC Gratitude List](#)

The Sandbox

increasing as a percentage of all cases. If this is the case, we can state that these cases will not be as easily mitigated by the victims without expert assistance.

ITRC expects that our tracking of actual victim case data will provide a new insight into the fabric of identity theft victimization, and we are anticipating some surprises concerning the relevance (or not) of some types of cases which have had significant press focus. Remember, these statistics are being compiled from identity theft victims only. They are referred to the ITRC by a variety of methods, and are located all across the U.S. They represent a reasonable account of what is happening across the country as a whole.

Identity Theft - What's it All About?

American citizens, businesses, legislators, law enforcement, media, and privacy advocates have spent an immense effort in the past five years pursuing a wide variety of interests in the field of identity theft. We have reported, regulated, legislated, prosecuted, expostulated, argued, denigrated, and even cooperated in the name of identity theft. Different parties have held differing viewpoints about many of the things that might affect identity theft. You had best be prepared before bringing up biometric identification with a group of law enforcement, business and privacy folks in hearing distance.

Sometimes the din has been deafening as we agreed or disagreed on quite basic things, like the definition and even name of the crime (identity fraud, identity theft, or ID theft, or ??) It is difficult to even reach agreement on whether the crime is increasing, as some study or another will point out the specific areas where the incidence is decreasing while not discussing those that are increasing. Taken altogether, America is fortunate to have so many talented and energetic people involved with identity theft. And, most of them are involved with integrity and good intention (but often differing viewpoints). All this activity, without argument, is a massive undertaking in the field of identity theft. So, what's it all about?

ITRC might be considered fortunate in one way. Since a big part of our effort is in mitigating identity theft cases for victims, we are constantly reminded of the importance of continuing our effort. A recent email from Lisa S. was one of those reminders. She wrote, "Finding the ID Theft Resource Center was such a gift during that time. Initially,



Wilma Burt was my contact. She was friendly, straightforward, and funny. She made me feel normal in the midst of the chaos because she could relate to the emotions, stress, confusion, and loneliness. I appreciated her truthfulness, even though at the time some of the guidance I was given I questioned. Ultimately, in the long run, I did experience the emotions and experiences she described. I am grateful to her and the ID Theft Resource Center for the guidance and direction to assist me in coping with and managing the fraud."

"I remember when Linda told me I wasn't alone. I was walking to my car parked in a garage a few blocks from the hospital where I worked," she continued. "I was passing the Chief Medical Examiners office at the corner of the extremely busy intersection at the height of the afternoon traffic. Linda and I were speaking about the fraud, emotions, etc. and we were talking about me participating in a 60 Minutes exclusive. During our conversation, as I shared how lonely I felt, I remember

Identity Theft Is Really No Big Deal. Idiot.

by Robert Siciliano
Identity Theft Expert

I make a portion of my living talking about identity theft. Admittedly, I profit from the crime. I don't steal identities of course, but I get paid because others steal. I'm not FBI, CIA, Secret Service or a cop. But you wouldn't disparage any of those entities for doing their jobs to protect you from bad guys.



I talk about this issue all day, every day to whoever will listen. I'm obsessed with this and all issues regarding personal security. It's what I do, and it seems to be "my purpose." I may sometimes go a bit overboard in my take on these issues and what people need to do to protect themselves, but sometimes that's what it takes for people who think it can't happen to them get off their duff and be proactive.

All that said, it bothers the heck out of me when someone looks me straight in the eye and tells me that identity theft is no big deal, that I should get over it. That's exactly what Julia Angwin does in this Wall Street Journal article. And she uses a prominent industry professional as the anchor of her article, to confirm her beliefs and trivialize this heinous crime.

The fact is, crime happens all day, every day. Some crimes are more or less common. Some are more or less invasive. All crimes have victims and all victims suffer the consequences of others actions. To trivialize those victims and make little of their burden is a completely incomprehensible act.

I responded to this article with the following comment:

"A person is more likely to be a victim of some form of identity theft than to be injured in a motor vehicle accident. But I'll bet she wears a seat belt and doesn't

when she said "Lisa, you are not alone". I needed to hear that so badly that day and it was so overwhelming that I dropped to the ground, sat down on the corner and cried. I just cried. I cried because I could breathe; because no one around me could say they understood; but Linda could and did understand. Both Linda and Wilma were and still are the only two people I have met during this time that were able to truthfully say, "I know how you feel". I am grateful for the resources the site provided, the direction, and the counseling; but I most thankful for the times when I heard Wilma or Linda say the words "you're not alone".

It is very easy in the pressure and tempo of our lives, with deadlines, conference calls, computers, webinars, websites, sponsors, media, and all the other activities that fill our days to lose sight of the most important reason for all our efforts against identity theft. What Lisa wrote brought me right back to the reality that this crime destroys lives, careers, and families, and creates a sense of isolation and loneliness that is overwhelming to many. In her brief email Lisa makes clear to all of us the most important reason for our work. Whether we work for identity theft prevention or identity restoration, we must not ever forget that what we accomplish can affect many lives in a positive manner. Now, go out there and do something good for somebody!

By: *Rex Davis*, Director of Operations, ITRC

Social Networking

Just because that link was tweeted or messaged to you by a colleague doesn't mean you should click it (in fact when I discovered the latest variant of Koobface spreading on Facebook, it was because the infected account of a former colleague, incidentally a VP of a global security company had sent it to me). Just because your friend published a list of 25 previously unknown things about themselves doesn't mean you need to reciprocate. Just because a celebrity that you respect tweeted a link, it doesn't mean it's safe to follow it, particularly when the real destination is obscured through a URL shortening service.

Social networking has rapidly gained acceptance in all walks of life, Facebook boasts close to 300 million users, MySpace doesn't advertise its figures but it is certainly Facebook's closest competitor in terms of user numbers and Bebo can count in excess of 40 million users. The customers of these social networking providers are not exclusively the school or university aged either, in fact two-thirds of the world's Internet population now visit social networking or blogging sites, accounting for almost 10% of all internet time, according to a Nielsen report dated March of 2009. It's not just about social networking sites though, the professional networking site LinkedIn has a new member joining almost every second and has over 50 million members, and the micro-blogging service Twitter grew a staggering 1382% year on year in February 2009.

With explosive growth and user populations of this order it's hardly surprising that these services also appear to be coming of age as attack platforms for cybercriminals. Web 2.0



with its user-generated, rich, interactive content and social networking with its interlinked trust-based networks of people and groups, offer cybercriminals great scope for leveraging the capabilities offered, both to disseminate traditional forms of malware through new channels and also to carry out

trivialize that. A person is more likely to be a victim of identity theft than have their home broken into or car stolen. But I'll bet she locks up. A person is more likely to be victim of identity theft than be sexually assaulted. But she dare not trivialize that. A person is more likely to be a victim of identity theft than have their child abducted. But I'll bet she watches her kids close at the park.

Sister, just because you don't understand something doesn't give you the right to make little of it. Identity theft victims suffer the consequences of fraud every day. Some much more than others.

For the victims, identity theft is a living hell. I wouldn't wish any of the above on anyone and hope identity theft never happens to you. If it does you will sing a different tune and be appropriately empathetic to the victims of this heinous crime. But really, identity theft is no "big deal."

ITRC Gratitude List

Yes, It is that time of year when ITRC will be contacted by more and more victims needing help on a new identity theft case. As of 12/15/09, ITRC has responded to 6391 identity theft cases this year. Being able to assist this many victims would not be possible without the support and contributions of many other people, businesses, and agencies. So, ITRC would like to take a moment to fill out our "Gratitude List".

Our ITRC advisors and support people simply rock! What's not to like about a bunch of people who work hard, laugh a lot, and yet are willing to dive into a new bunch of identity theft cases each and every day!

social engineering attacks for the purposes of target profiling or identity theft.

Among the more traditional attacks, facilitated through social networking, that we have seen over the past few months through social networking sites you can count the following:

- Several outbreaks of (so far) non-malicious worms on Twitter, using cross site scripting vulnerabilities or clickjacking.
 - Fake Bebo and LinkedIn profiles containing links that lead to malicious downloads.
 - Rogue applications that appear to be designed for information harvesting and the infamous Koobface worm on Facebook.
 - Hijacked profiles being used to scam money under false pretences, directly from one friend to another.
 - Scam advertisements leading to bogus multi-level marketing schemes, or worse.
- You can also be sure that the information publicly available has been used to create targeted attacks such as spear-phishing, whaling, and to facilitate credit card fraud.

There are several entry points available for cybercriminals into the interactive playground of social networking: fake or compromised profiles, malicious applications, malvertisements, cybersquatting, spam and phish masquerading as legitimate notifications from social networks, information harvesting through group memberships, cross-site scripting vulnerabilities and direct messages just for starters. Victims are at risk of identity theft, fraud, infection or simply of becoming an attack platform to infect or defraud their own friends and colleagues.

The one thing that all of these attacks have in common though is the very thing that binds social networks together: trust. Because the attacks, messages and links come from friends or colleagues, they appear far more credible than the average Spam email from a stranger. Even the Koobface worm with its almost textbook standard Spam messages such as "You are very ggood at pposing to a spy cameeral!" becomes that little bit more believable when it comes from someone you know. And of course, when we choose to join a community, by default we naively choose to share all of our personal information with any other member of that community simply on the basis of a mutual shared interest.

Most of us are guilty of being far too trusting and far too free with our personal information online, we give away little snippets (or great chunks in some cases) of our personal lives in what is essentially a public or at best only semi-private forum, making the work of criminals such as carders and ID fraudsters far more simple. In fact I have seen social networking sites spoken about in underground carding forums as a "free date of birth look-up service" along with a wealth of tips on how best to exploit these kinds of platforms.

We need to become far more aware of the value of our personal information and importantly the information we have about our friends. We also need to become far more conversant with the privacy controls available on social and professional networking sites and actually use them. There is no need to fill out that questionnaire "25 Things About Me" and post it on your profile, there is no need to share your entire employment, educational or address history. There is no need to share your "Porn Star Name" (first name = name of your first pet, family name = mother's maiden name), isn't that exactly the kind of information needed to reset your email account password, or access your financial data? And there is no need to volunteer the email addresses of friends and family when asked to recommend a "joke" website or application to 10 friends.

When your personal information becomes public it is out of your control and soon out of sight. Criminals can and do use this stuff to break into your online accounts, just ask Sarah Palin or Salma Hayek.



We are grateful to all the law enforcement officers and others, who help provide victims with the all important police report. Those who do this with understanding compassion are our heros!

There are a some very good people in the trenches, in a variety of U.S. government agencies, who continuously search for ways to make people's lives better. Notable are the DOJ/OVC and FTC for their efforts. These are mostly unsung hero's in this war. You know who you are, and so do we. Thank You!

We are thankful for the support from the Rose Foundation and California Consumer Protection Foundation, who continue to believe in what we do, and help keep us centered on the need for personal and business privacy. You are fundamental to our balanced viewpoint, and we thank you.

We certainly appreciate our public spirited business sponsors! These are companies and people who put aside time and financial support to further the ITRC mission. They constantly surprise us with new avenues of collaboration and public support. Muchas Gracias to:

Debix, Fellowes, First Advantage, ID Analytics, Identity Theft 911, InfoArmor, ProtectmyID.com (part of Experian), Salesforce.com, ShopShield, TrendMicro,

Next time, before you hit "Post", ask yourself this "If a stranger called me on the telephone asking for this information, would I tell them?" If the answer is "No", then step away from the mouse.

By: *Rik Ferguson*, Senior Security Advisor, [Trend Micro](#)

Refer to the new [ITRC Fact Sheet138 - Social Networking and Identity Theft](#)

[ITRaC News Q1 2009](#)

[ITRaC News Q2 2009](#)

[ITRaC News Q3 2009](#)

*TrustedID,
and Uni-ball.*

We have developed partnerships with some of the best industry experts and agencies including, National Foundation for Credit Counseling (NFCC), and the American National Standards Institute (ANSI). Thank you all!

ITRC wishes each of you a Happy Holiday Season, and hopes that you will take time to make your own "Gratitude List."

ITRC New Hot Link!

Over the past few months, the ITRC has implemented a number of new website features, including a new Data Breach Home Page, a "Scam Home Page" and a Document Catalogue button which allows users to directly find ITRC Fact Sheets, Solutions and Letter Forms in seconds.

[Document
Catalogue](#)

ITRC Online

Find the Identity Theft Resource Center on:

[facebook.](#)

[myspace.com](#)
a place for friends

[twitter](#)

[itrc](#)
Identity Theft Resource Center

[To Subscribe](#)

If you no longer wish to receive these emails, please reply to this message with "Unsubscribe" in the subject line or simply click on the following link: [Unsubscribe](#)

Identity Theft Resource Center
9672 Via Excelencia, #101
San Diego, California 92126
US

[Read](#) the VerticalResponse marketing policy.

