



TEN MYTHS ABOUT IDENTITY FRAUD

Think ID fraud is running amok over the Internet? Are online credit card thieves your worst fear? Here's a dose of reality that may change your mind

FEBRUARY 12, 2008 | 5:38 PM

By Tim Wilson, Site Editor, Dark Reading

Identity fraud is running rampant. Between corporate breaches and online exploits against individuals, hackers are stealing identities in record numbers and posting it to the Web from all over the country, right?

Wrong on all counts, according to new studies of the ID fraud space. The reports -- one released yesterday by Javelin Strategy and Research, and one released by ID Analytics a few months ago -- offer data that debunks many of the current myths about identity theft.

If you think you know what's happening in the ID fraud space, take a gander at some of the data offered by these new reports. You may find you don't know as much as you thought you did.

1. There is a higher incidence of ID fraud today than in past years.

Javelin Strategy and Research, which has conducted a mega-study on U.S. identity theft and fraud annually for the past five years, has definitely recognized a trend. But it's downward, not upward.

According to Javelin's 2008 survey, some 3.58 percent of respondents reported experiencing online fraud during the previous year. That's down from 3.74 percent in the 2007 study, 4.0 percent in the 2006 study, and 4.7 percent in the 2003 study.

In fact, Javelin says, the identity fraud incidence rate has decreased every year since the research firm began doing the report five years ago.

2. There are more victims of identity theft and fraud today than there have ever been before.

If it hasn't happened to you, it's happened to someone you know. And with so much personal data being exposed every day via corporate security breaches and cunning hacker exploits, there must be more victims than ever, right?

Wrong, according to the Javelin study. The research firm estimates that there were approximately 8.1 million victims of ID theft and fraud last year, but that number is down, not up, from the year before.

In fact, just like the incidence rate, the number of ID theft victims in the United States has dropped every year since Javelin began conducting the study. Approximately 10.1 million people reported experiencing fraud or theft in the 2003 study; that figure had dropped to 8.4 million by last year, and 8.1 million this year.

3. Identity fraudsters are stealing record amounts of money from their victims.

Despite reports of big-dollar thefts and a booming black market for credit cards and other personal information, the cost of identity fraud and theft underwent its most precipitous drop last year, according to Javelin.

After hitting an all-time-high of \$58 billion in the 2007 study, ID fraud and theft totaled just \$51 billion in the U.S. this year, Javelin says. The \$7 billion drop was the largest in the history of the research.

The drop also is the first that Javelin has seen since it began publishing the study in 2003. From 2003 to 2007, the fraud damage figure has been on a steady incline, going from \$56 billion to \$58 billion and increasing slightly every year.

4. Most identity theft and fraud occurs online.

Now that everybody's doing business via the Web, the criminals must be moving there too, conventional wisdom says. Many enterprises have responded to this wisdom with improved sign-on and multi-factor authentication schemes designed to protect the online consumer.

Rather than fight this trend, however, criminals are simply moving to places where the pickings are easier: telephone and mail fraud. According to the Javelin study, identity theft via phone and mail order fraud have skyrocketed in the past year, going from approximately 3 percent of cases in the 2007 report to 40 percent this year.

The difference is primarily in the defense, Javelin says. As of 2007, only 48 percent of the top 25 U.S. financial institutions had instituted a multifactor authentication scheme for telephone banking, making it a much easier approach for criminals than the increasingly armored Website.

5. Online attackers are the greatest perpetrators of identity fraud and theft.

In the TV cop shows, they always cite statistics to show that murder is often committed by someone you know, rather than a stranger. Apparently, this is true of identity theft as well.

In the Javelin study, approximately 14 percent of thefts occurred through traditional "hacker methods" such as Trojans, viruses, or phishing. Data breaches accounted for another 7 percent of thefts -- but even taken together, these account for less than a quarter of all ID fraud.

So where does the rest of it come from? About a third (33 percent) comes from physical theft -- a lost or stolen wallet, purse, or credit card. But a surprising 17 percent of identity theft is perpetrated by friends, relatives, or in-home employees, the study says.

"Often, consumers find it hard to believe that a close friend or family member would perpetrate identity theft against them, but it is these very individuals that have the easiest access to one's private information," the study says.

6. Large security breaches, such as the ones at TJX or the Department of Veterans' Affairs, are the most dangerous to users.

The TJX case has been held up as one of the most egregious breaches in online history, and there have been some incidences of identity theft arising from it. But according to a study published in November by ID Analytics, you're more likely to be victimized by a small data breach than one of the much-ballyhooed gaffes such as TJX's.

Smaller breaches have a higher misuse rate, according to ID Analytics. Misuse of personal data ranged from one in 200 identities for breaches of fewer than 5,000 individuals to a misuse rate of less than one in 10,000 identities for breaches of more than 100,000 individuals. (See What You Don't Know About ID Fraud.)

7. Identity thieves distribute their booty widely, selling or publishing it wherever they can.

Once a criminal has your personal information, you're history, right? It's just a matter of time before the whole world has it, too.

That's not necessarily true, according to the ID Analytics study. In fact, many identity thieves apparently protect the data they steal, just as a bank robber will protect his bags of money.

The study found no evidence that fraudsters who misuse breach data were selling the data broadly or distributing it over the Internet. "This finding is significant because one of the greatest potential risks of data breaches is the broad dissemination of personal information to others with criminal intent," ID Analytics says.

8. Valid credit cards are an identity thief's primary target.

While a nice fat batch of valid credit card numbers is a good haul for an identity thief, there are many other ways to use personal data that can be just as dangerous to the consumer, researchers say.

According to the Javelin study, virtually every category of "card not present" fraud and theft has shown an increase over the past year. Among these are attempts to create new accounts using stolen personal data, as well as efforts to break into existing bank or credit card accounts through means that don't require a card.

Address changes are among the most popular methods of attack, Javelin says. A criminal may call or email a company and claim that he wants to change the address on a card or account. Then, using stolen data to verify his identity, he may gain access to the account without ever possessing a card.

9. Fraudsters steal as much personal data as they can, storing it up until they are ready to use it. Many consumers -- and even some IT people -- have an image of an identity criminal who hoards personal information like Ali Baba's 40 thieves. Even if your data was stolen years ago, this notion says, it might be used any minute.

But according to ID Analytics, in most cases, online fraudsters don't store up stolen ID information, but cycle through it quickly. Fraudsters misuse a breached identity for no more than two weeks before moving onto the next identity, researchers found.

The Javelin study confirms this conclusion. In the study, data collected via viruses, Trojans, or phishing was misused for the shortest period of time, usually between 21 and 41 days. By contrast, data obtained from a physical theft or by a friend or relative may be misused for an average of 112 to 130 days.

10. The incidence of identity fraud is pretty much the same from state to state.

We're all on the same Internet, so we all share an equal risk, right? Computer users are no safer in one region than another.

According to the Javelin study, that's not so. In fact, over the past three years, consumers in California, Delaware, Idaho, Illinois, and West Virginia have experienced a higher rate of identity fraud and theft than their counterparts in other states. On average, New England and the Plains States reported the lowest incidence of fraud.

Generally, states with the most populous metropolitan areas, such as California, are more likely to have higher rates of fraud activity, thanks to higher incomes and more frequent use of online commerce, the study says.