

Identity Theft and Bank Fraud all Rolled Up into One Nice Little Package

May 18, 2012 - For more than one year now, there has been a nice little malware program floating about the internet called Tatanga. But the people distributing it probably refer to it as "cha-ching". This is one nefarious little piece of software that can entice victims to give up all of the information needed to commit identity theft, drain their bank account, and more.

Tweet

```
(function() {  
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];  
s.type = 'text/javascript';  
s.src = 'http://widgets.digg.com/buttons.js';  
s1.parentNode.insertBefore(s, s1);  
})();
```

```
(function() {  
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;  
po.src = 'https://apis.google.com/js/plusone.js';  
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);  
})();
```

In short, if your compute is infected with Tatanga, the latest version of the program will insert a new screen in your browser when you do online banking. The screen will tell you that your bank is offering free credit card fraud insurance to all of its customers. It also claims that the insurance is offered in conjunction with Visa and MasterCard.

As if that's not bad enough, since you are already logged onto your bank's website, the program then grabs all of your account balances and offers you an insurance package that will cover all of them.

To make a long story short, anyone who agrees to sign up for the insurance will be presented with an insurance policy number. But that number is really a bank account number. You'll be asked to authorize a transaction through your account to activate your insurance policy. What you are really doing is transferring funds from your bank account to someone else's. The amount transferred can be as high as \$6,500. In addition to the account transfer, other personal information will also be provided to the crooks running the scam. Bottom line is that once you become a victim of Tatanga, you may be victimized more than once.

There are some things to look for if you find yourself presented with a similar offer. Bad grammar, words in foreign languages, or misspellings are all clues that the offer may be a scam. So far, researchers that have looked at the program have only seen a Spanish language version but it is known to have been distributed in both the United States and Europe. English versions are almost certainly already in place.

Trusteer, the organization that discovered the latest version, is advising that if you do get solicited by your bank with any special offers, not to respond online. Instead, pick up the phone and call your bank to ask if the offer is legitimate.

byJim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, [click here](#).

Registration is easy and free.
Follow me on Twitter:

Follow ACCESS