

LOGIN INFO secure at www.americanexpress.CA?

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.inetexplorer.ie6.browser/2007-03/msg0034>

- *From:* Mister.Fred.Ma@xxxxxxxxxx
 - *Date:* 17 Mar 2007 05:24:05 -0700
-

On Mar 15, 9:59 pm, Gary Smith <bitbuc...@xxxxxxxxxxxx> wrote:

Mister.Fred...@xxxxxxxxxx wrote:

On Mar 14, 7:41 pm, Gary Smith <bitbuc...@xxxxxxxxxxxx> wrote:

...When I typewww.americanexpress.com inthe address bar and press enter, I'm immediately redirected tohttps://home.americanexpress.com/home/mt_personal.shtml, which is secure by virtue of the "https" protocol. That's where the login boxes are, on a secure page which causes the lock symbol to be displayed in the status bar. Does that not happen for you?

Yes, it does. I missed the part where you use .com as the suffix rather than .ca. That is the difference which caused the login page to be secure. Weird, eh?

I suspect that the difference is in the waywww.americanexpress.ca is set up. Evidently the target of its redirect is not a secure page. I'll call that a page construction error

I'm not an web-type person, but perhaps that login region is somehow made secure, even though the page itself is not https. It has been speculated among office people that this is hinted at by the picture of a lock in the login region. To me, this way of setting up the web page has 2 drawbacks.

First, it isn't clear whether the speculation is even true. For example, the intended message might be that the session is secure *after* login (which is true, since it becomes https after login). It's hard to tell from a simple icon.

Second, even if it was true, the use of a non-https page removes all the standard security indicators that a (duly diligent) user is taught to look for -- namely, the https on the URL, and the lock at the corner if IE (or whatever the equivalent is for firefox, since that's what I normally use). Due diligence, therefore, requires a user to not use that page.

Amex front line support is reluctant to even recognize the problem and escalate it, though I did insist. Their position is that they "try hard" to make "things" secure (though they couldn't say how) and if I didn't like it, I shouldn't use it. Since this boils down to inaccessibility to online services, I appreciate your pointing out the .com alternative, which doesn't have this problem.

2nd line support left me a voicemail assuring me that he went through a session, and all was secure. No mention was made of the fact that the particular point of concern was securing the login info itself, as well as the clear indication of having done so using standard security indicators. So it isn't clear that the problem was properly communicated; I would tend to think not, based on the misunderstanding at front line support. An erroneous return phone number was provided. The frustrating thing is that there is no email address to raise this issue in documented manner, including documentation of the tenuous communication. Hopefully, their anti-phishing email address (the only one I can find) will forward this message to the right department.

The surprising thing is that most users I spoke to didn't even notice the problem because they don't pay attention to the security aspect, particularly at login (or they had faith in the picture of the lock in the login region, and decided to forgo the standard indicators). This means there will be very little demand for a change to bring it in line with standard security indicators.

In any case, I believe that I've done what I can to respond to the issue, and I now leave it in their capable hands. Thanks once again for pointing out the properly coded .COM webpage so that I can avoid the problem on the .CA webpage.

Fred

Fred

.