

## Re: https question on popular email providers

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.misc/2003-06/0140.html>

---

**From:** Skulking Rogue ([anon\\_at\\_cheshire.hopto.org](mailto:anon_at_cheshire.hopto.org))

**Date:** 06/07/03

Date: Sat, 07 Jun 2003 07:22:36 GMT

On 6 Jun 2003, richard2008918@yahoo.com (richard) wrote:

>I have seen hotmail and yahoo email providing https connection for  
>login. However, once the user is authenticated, the page is  
>re-directed to non-secure http. Does that mean all the data (i.e. the  
>content of email) in transmission are not protected? If this is the  
>case, why bother to protect userID/password?  
>Maybe I am missing something here.

It is not a useless as it initially seems. Included in the attacks that this prevents are:

1. An attacker cannot send mail from your account, posing as you.
2. An attacker cannot read your mail any time he wishes, instead he must wait for you to download it, and passively sniff it as it passes.
3. An attacker cannot log on as you, and delete your mail before you see it (so now he would read it and you would not).

What it does not do is provide you with privacy, but you didn't have any of that anyway. All of your mail is sitting in plain text on yahoo's servers, available to anyone at yahoo, or anyone who can compromise anyone at yahoo, or anyone who can make a deal with yahoo,... The list goes on. The email was also in the clear as it made it's way to yahoo, and so visible to the attacked at that time.

You have no privacy unless the email is encrypted. In that case, there is little need for protecting it in transit.

>I am going to set a web-based email application to my company's IMAP  
>server. I am evaluating to what extent of implementation https  
>communication assuming user can access their email account using  
>browser anywhere and anytime. How big is the overhead if implementing  
>https through the entire session? Are there any other solutions that  
>can increase the security in such a scenario?

comp.security.misc: Re: https question on popular email providers

The overhead in https is in the public key computations to set up the session key. The symmetric encryption under that session key involves negligible work; it would be overshadowed even by disk access speeds, much less network transmission. So there is no significant overhead in using it for the whole session.

>*You comment is greatly appreciated!*

>

>*richard*