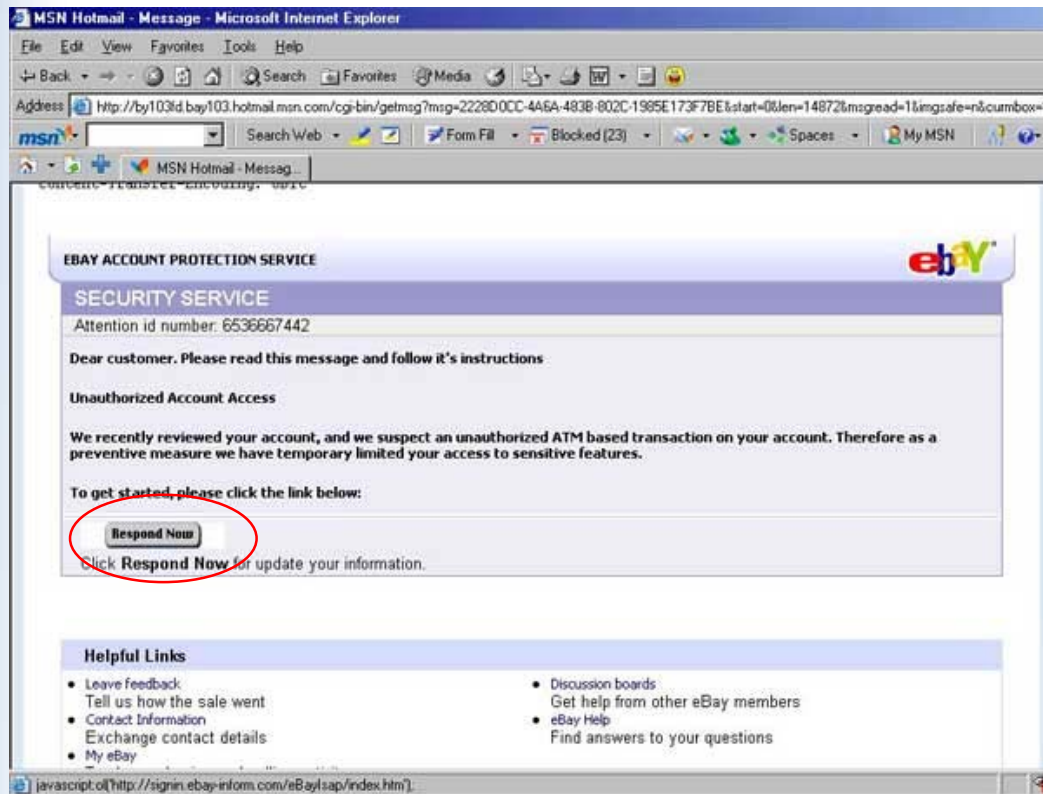


## Lesson 101 - How to detect phishing with ipGuardian?

In this scenario, you received an email from eBay Security. Apparently, eBay has detected an unauthorized ATM based transaction on your account. In response, it urges you to respond to update your information.

This is a scenario WITH ipGuardian.

1. You open the email and proceed to inspect the content.



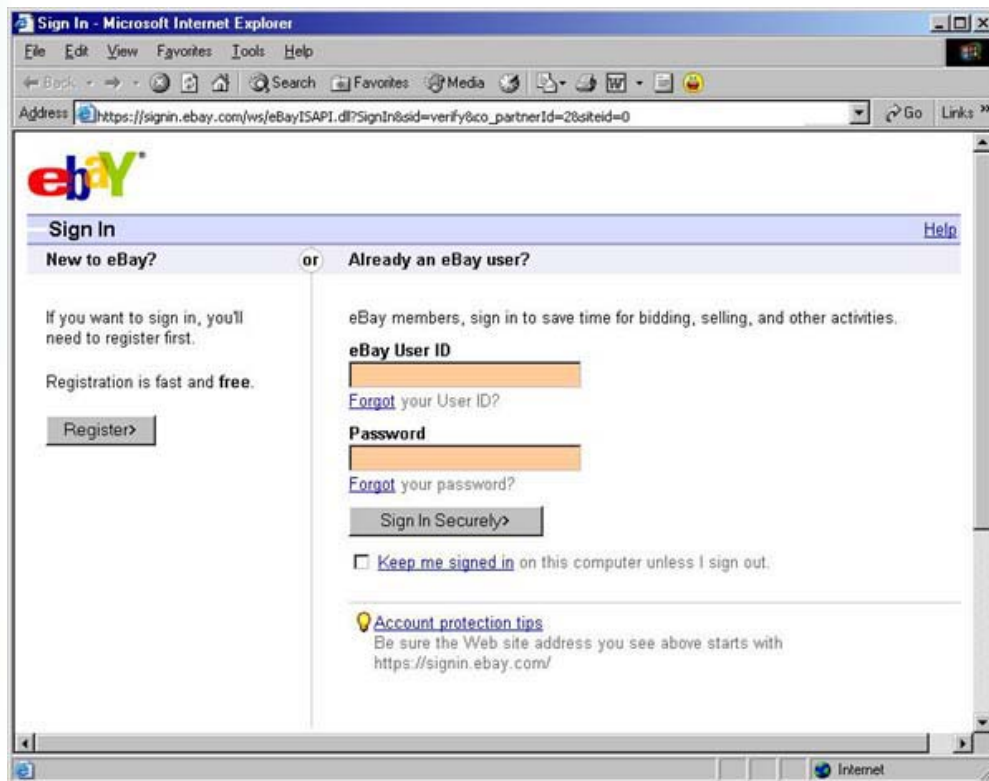
2. First, you place your mouse over the "Respond Now" button. It shows the following message on the status bar: -  
"javascript:ol('http://signin-ebay-inform.com/eBayIsap/index.htm');"  
The status message looks okay to you.
3. You proceed to click on the "Respond Now" button. ipGuardian immediately prompts you the actual page that you will be visiting.



**Benefit 1:** In the WARNING box above, ipGuardian shows you the real URL that you are going to. The revealing of the real URL defeats any obfuscation that you have seen in step 2 when you place your mouse over a URL. Who knows what is actually inside the "ol" JAVASCRIPT function?

**Benefit 2:** ipGuardian allows you to cancel the actual trip to the designated web site. This gives you the power to abort if you have made a mistake in clicking the link earlier. As an example, one can press the No button to cancel the trip if one realizes that ebay-inform.com is just a name obfuscation of the real ebay.com.

4. You press the "Yes button" and your browser brings you to the following page.



5. The browser "Address" line reads [https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co\\_partnerId=2&siteid=0](https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0).

That looks legitimate enough to you.

6. You noted that there is no "ipGuardian: country is safe!" on the status bar.

**Benefit 3:** The fact that you do not see the "ipGuardian: country is safe" on the status bar message show gives you more confidence that the web site is a phishing site.



7. You place your mouse on all links but you could not see anything on the status bar. You may not realize it but there is a clever JAVASCRIPT script running in the web page that clears the status bar every second.
8. You noted that ipGuardian did not bring up a POSITIVE WEBSITE VERIFICATION dialog.

**Benefit 4:** For eBay and a few other selected websites, ipGuardian shows you a positive verification<sup>1</sup> that you are on the real site; like the one shown below: -



If you see the above dialog, your confidence of you being on the real website should be very high (close to 100%). However, if you do not see the positive verification website dialog, it is more likely that the website that you have visited is a phishing site.

9. You select "Help+About ipGuardian" to check the real IP details. This further confirms your suspicion.



---

<sup>1</sup> Positive Website Verification is a new feature in ipGuardian v2.7

**Benefit 5:** The real IP details show that although the country is in USA (a safe country), the Host is not eBay. This should give you further confirmation that the website is fraudulent.

**Benefit 6:** The real IP details show that the "Is Secure" flag false. For a URL that is a https, it confirms that the Address URL as shown on step 5 is definitely fraudulent.

**Benefit 7:** The real IP details show that the URL is actually "signin.ebay-inform.com" instead of "signin.ebay.com" as shown in step 5. This implies that Address URL is fraudulent. In fact, this is a clever JAVASCRIPT trick that covers part of the real address bar with an image, which shows the fraudulent URL.

**Benefit 8:** The real IP details show that the IP address is 69.143.49.252. For those who are really in the know, he or she will recognize that this URL does not belong to eBay.

10. Given what you know, will you still sign in?