

Summary

| | |
|------------------------|--|
| Email title: | 'Account Verification' |
| Scam target: | eBay users |
| Sender: | aw-confirm@ebay.com |
| Sender spoofed/hidden? | Spoofed |
| Phish 'punch line' : | 'Five password bruteforcing attems were performed on your eBay account. You must register and ID Verify certificate in order to remain in the eBay Community.' |
| Scam goal: | Getting victim's eBay username/password, credit card information |
| Phish link method | a 'Click here' type link |
| Link 'masked'? | Yes |
| Actual link to | http://www.lemondedegaetane.com/aw-cgi/ws2/SignIn.html |
| Phish website IP: | 212.85.153.6 |

E-mail

This is a fresh phish case, which uses a 'hijacked' domain - i.e. the phishers have obtained remote access to a legitimate site and placed the phish site there. This way they can use the whitelist entries for the legitimate domain, and get through a URL blacklist filter.

The email looks quite persuasive:


Five password bruteforcing attemps were performed on your eBay account.

You must register and ID Verify  certificate in order to remain in the eBay Community.

Dear eBay Community Member,

You (or someone else) has attempted to log in with your eBay ID and 5 diffrent wrong passwords.

According to our site policy you will have to confirm that you are the real owner of the eBay account by completing the following form or else your account will be suspended within 24 hours for investigations.

Establish your proof of identity with ID Verify (free of charge) - an easy way to help others trust you as their trading partner. The process takes about 5 minutes to complete and involves updating your eBay information. When you're successfully verified, you will receive an ID Verify icon  in your feedback profile. Currently, the service is only available to residents of the United States and U.S. territories (Puerto Rico, US Virgin Islands and Guam.)

[Confirm my account information and continue beeing a member of the eBay Online Auction Community.](#)

Never share your eBay password to anyone!

Regards,

Accounting Department,
eBay Inc.

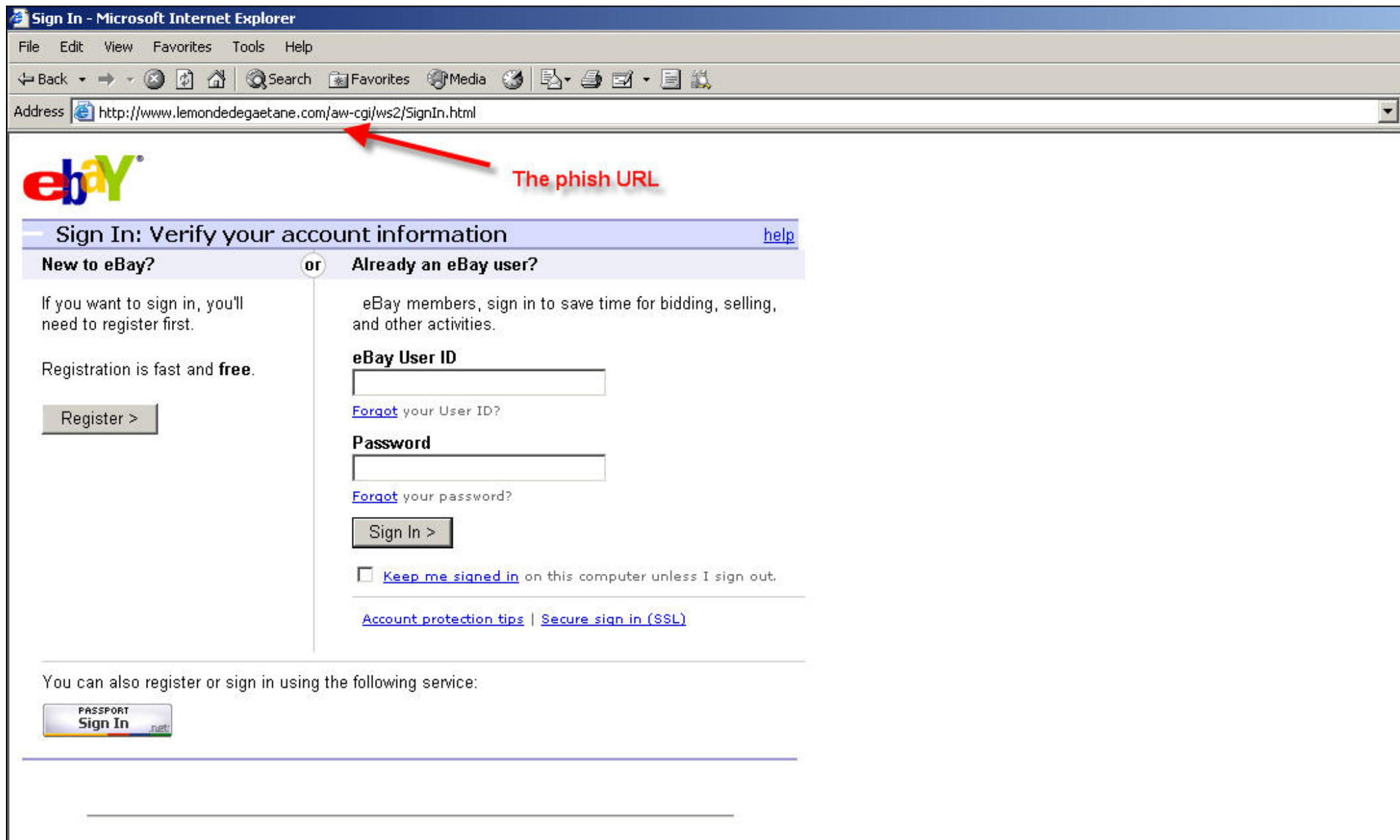
The tone is quite harsh and there is no eBay logo or legit header/footer. Otherwise it is well made - the sender is spoofed and the actual URL of the link is hidden.

Web Site

| | |
|-------------------|---|
| Link 'masked'? | Yes |
| Actual link to | http://www.lemondedegaetane.com/aw-cgi/ws2/SignIn.html |
| Phish website IP: | 212.85.153.6 |

The phish site opens up with a page that is an exact replica of the eBay login page, with only a couple of differences:

- The URL in the address bar is different (i.e. not an ebay.com derivate);
- The page is a 'http' one (unsecured). The legitimate page is on a 'https' secured site.



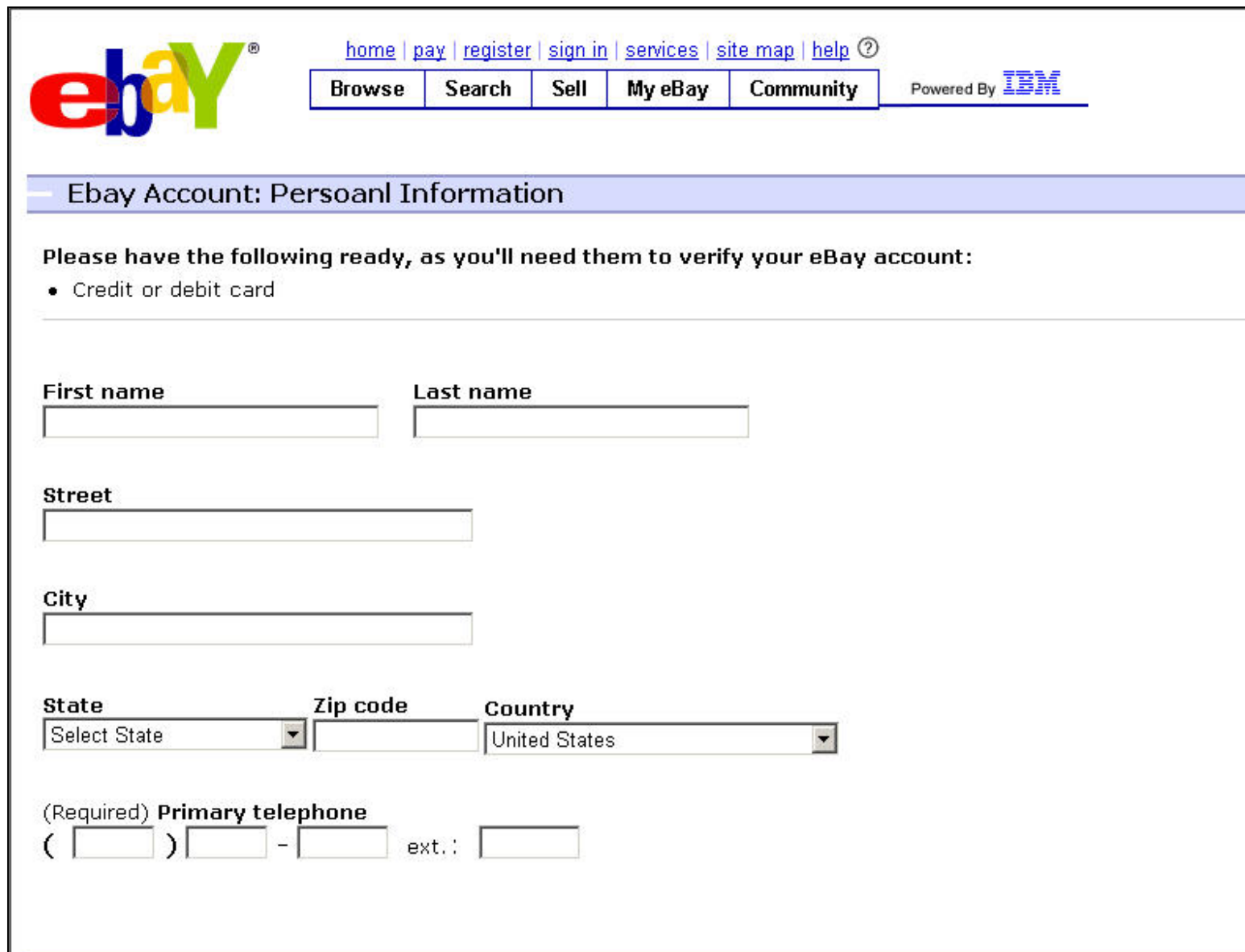
Copyright © 1995-2004 eBay Inc. All Rights Reserved.

Designated trademarks and brands are the property of their respective owners.

Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#).



After the initial 'login' page, a second one is displayed, demanding more information. The weaknesses mentioned earlier remain visible.



The screenshot shows the eBay website's account verification page. At the top left is the eBay logo. To its right are navigation links: home, pay, register, sign in, services, site map, and help. Below these are buttons for Browse, Search, Sell, My eBay, and Community, followed by a "Powered By IBM" logo. The main heading is "Ebay Account: Personal Information". Below this, a message states: "Please have the following ready, as you'll need them to verify your eBay account:" followed by a bullet point: "Credit or debit card". The form contains several input fields: "First name" and "Last name" (two separate text boxes), "Street" (one text box), "City" (one text box), "State" (a dropdown menu with "Select State" selected), "Zip code" (one text box), "Country" (a dropdown menu with "United States" selected), and "Primary telephone" (a form with parentheses, a hyphen, and an "ext.:" label, each followed by a text box).

Ebay Account: Credit Card Identification

(Required) **Credit card/Debit card number** Credit Card: MasterCard, Visa, American Express, Discover. Debit Card: MasterCard, Visa

(Required) **Expiration date** Month: Year:

Card type

(Required) **Credit/Debit card PIN**

(Required) **CVV** 3 digits for Visa , MasterCard , Discover | 4 digits for American Express

Copyright © 1995-2003 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#).

reviewed by
TRUST.e
site privacy statement

The site will check whether the fields are filled, and will check the credit card number using the Luhn formula. It is a simple mathematical formula, typically used for a first stage CC verification (i.e. - before connecting to a CC server). The function of this check is to reject a random bogus number, thus to imply legitimacy of the site. It will, of course, accept a bogus number conforming to the Luhn formula rule.


After accepting the information, a standard looking logout page is displayed:

You Have Signed Out - Microsoft Internet Explorer

File Edit View Favorites Tools Help


Back Forward Stop Home Search Favorites Media Print Mail News RSS

Address <http://www.lemondedegaetane.com/aw-cgi/signOutConfirm.html>



[home](#) | [pay](#) | [register](#) | [sign in](#) | [services](#) | [site map](#) | [help](#)


| | | | | |
|---------------|---------------|-------------|----------------|------------------|
| Browse | Search | Sell | My eBay | Community |
|---------------|---------------|-------------|----------------|------------------|

Powered By 



Information updated successfully

Sign in to your eBay account.

Get what you **Really** wanted!



- [Paintball](#)
- [Nike Golf](#)
- [Pool Tables](#)
- [Snowboards](#)
- [NBA Tickets](#)
- [Mountain Bikes](#)
- [Foosball Tables](#)
- [NASCAR Tickets](#)
- [Throwback Jerseys](#)
- [BowFlex Home Gyms](#)

[Announcements](#) | [Register](#) | [The eBay Shop](#) | [Security Center](#) | [Policies](#) | [Feedback Forum](#)
[About eBay](#) | [Home](#) | [My eBay](#) | [Site Map](#) | [eBay Downloads](#) | [eBay Gift Certificates](#)

[Browse](#) | [Sell](#) | [Services](#) | [Search](#) | [Help](#) | [Community](#)
[Overview](#) | [News](#) | [Chat](#) | [Library](#) | [Charity](#) | [eBay Gear](#) | [About eBay](#)

Copyright © 1995-2004 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#).



The hijacked legitimate server is located in France:

| | |
|--|---|
| WHOIS information (for IP 212.85.153.6): | IP Location: France domain: LEMONDEDEGAETANE.COM owner-address: Eric Ariaudo owner-address: Les Plantes owner-address: 24380 owner-address: Creyssensac owner-address: France owner-phone: +33.199999999 admin-c: GL736-GANDI tech-c: LO138-GANDI bill-c: GL736-GANDI nserver: ns1.lost-oasis.net 212.85.153.9 nserver: ns2.lost-oasis.net 80.67.160.54 reg_created: 2003-06-30 05:02:05 expires: 2005-06-30 05:02:05 created: 2003-06-30 11:02:06 changed: 2004-07-05 12:00:44 |
|--|---|