

# Why you Need Calling ID

*Not a day goes by without hearing about someone who has had some sort of identity theft related incident. Most of these incidents were possible because mail to the victim was intercepted or the thief was able to get enough personal information to create a new account, change the address or capture a userID and password. While there are no easy ways to avoid incidents associated with mail and opening accounts there is some relief available to help you protect your interests on the Web. This paper describes a way to help you decide whether you want to do business with or provide personal information to a site.*

## Identity Theft is Big Business

According to a recent US FTC report, one out of every five Americans was a victim of identity theft in the last 3 years with an average cost of \$600 per incident. The problem is that until you are victimized it isn't real because you know the things that you need to do. For example you know that you should tear up credit card receipt carbons and that you should try to keep track of your credit card when you give it to a waiter in a restaurant to reduce the odds that the waiter might make a duplicate. This is tough enough. But what about information you pass on the Internet when you make queries, buy some items or simply use online banking and/or online investing? Watching your credit card is relatively easy, since you can see or at least try to see what the waiter is doing with your card, whereas when you deal with an Internet site you have very little visibility as to what is going on and who you are dealing with.

When you send your personal information over the Internet it is your responsibility to make sure that you know who owns the site receiving the information. As a result the FTC's primary recommendation is: "Don't give out personal information over the Internet unless you are sure you know who you're dealing with".

## Phishing and Pharming to Get your Information

When using the Internet, unless you are very inquisitive, skilled and have a lot of time you don't know anything about the site other than the name displayed by the site. Scammers work very hard to mask themselves from you with websites that appear legitimate. In fact, the setting up fake sites to steal your personal information has become significant enough and widespread enough to warrant labels like "phishing" and "pharming" and daily references to attacks. Phishing usually uses an email to entice you to go to their site. The enticements range from unbelievably tempting deals to emails that cause you act emotionally such as in response to "there has been an unusually large purchase on your VISA card – please visit our fraud site to validate". Pharming is an even more subtle approach. It uses technical tricks available on the Internet that actually change the destination of the URL that you see on your browser and points to another site under the covers. In other words, you could think that you are accessing your bank while actually entering a scam site.

## Normal Information Protection Measures aren't Working

Web presentation technology and access flexibility have made it very easy for fake sites to gain your confidence to the point that even well trained professionals are having difficulty in being sure that a site is legitimate. Web thieves' technologies are so sophisticated that they can actually capture your keystrokes before you submit the information that you have entered.

The most prevalent answer to address identity theft problems such as phishing and pharming is to educate the user. The problem is that the guidelines offered conflict with many of the Web premises regarding ease of navigation and challenge their ability to make meaningful decisions with such advice as:

- *Do not follow links that cross sites* - But shopping comparison sites like shopping.com, pricegrabber.com etc. always use redirects to sites for shopping.
- *Do not disclose any information to un-bona fide sites.* - How does one verify that the site is bona fide?
- *Confirm that the session used is secured with a valid certificate and verify the owner of the certificate* - Who knows how to do that?

Something more reasonable is needed.

### **Can IT Solutions Help?**

IT organizations have a lot of experience in protecting their users from the bad guys. They focus on prevention technologies that filter phishing email attacks using anti-spam approaches and block outbound web access to blacklisted sites. Some organizations block web access to all sites except to those on a white list. The latter approach is often out of desperation when the prior approaches aren't comprehensive enough. For an IT organization with their own network these techniques can be implemented in a proxy server or firewall. If the company being served by the IT organization also uses the internet, special software installed in the desktop is needed in order to force connectivity to their proxy server first.

For users outside of the "internal company network," that need more web access "freedom", special software is installed on the users' systems. This software is like anti-virus and anti-intrusion detection and blocks or warns when access to blacklisted sites is attempted. The problem is currency; the update of the black lists is not immediate. It usually takes several hours to detect the site and update the list. Like most burglaries, the scam is usually highly effective and reaches most of its victims during the first few hours. Scam sites are usually shut down or detected after a few hours of effective activity, so the blacklist is typically only as good as the rapidity of the detection and currency of the list.

Home PC users are ill prepared to deal with the rigors of access control and typically don't have the interest or skill to deal with them. They get frustrated and either take the risk or go somewhere else..

### **Desktop/Laptop Protection Technology is Needed**

As would be expected, there are a lot of software vendors working furiously to help the masses of home users with desktop and laptop software to help protect them from scammers since they don't have the benefit of network access control that companies with internal networks offer.

Some tools

- Analyze the content of the site to determine legitimacy by comparing the content and the address.
- Make users aware that they are sending passwords and personal information like credit card info to unknown or inappropriate sites.
- Either block or warn the user when they attempt to submit a password or data previously defined as "confidential".
- Try to tell the user where he goes and if the site is safe for browsing.
- Examine the site content to ensure the real address of the site is not different from that shown

The primary problem is that each tool tends to provide a partial solution which is really not viable as a home user solution since they cannot deal with being "half protected" or "protected most of the time". What is worse is that the bigger the upside potential benefit to the thief the more sophisticated the extraction of the desired information.

What is needed is a way to engage and educate the user proactively on an ongoing basis. We saw such a phenomenon with Caller ID. When we were inundated with phone calls from sales people and other undesired solicitations, Caller ID offered a way to know who was calling before picking up the phone. Now most US homes use the caller ID feature.

We believe that a similar, easy to understand mechanism is needed for assessing websites before accessing them and especially before providing the sites with passwords, personal or confidential information.

## CallingID's Calling ID

CallingID is a comprehensive solution that empowers web users to protect themselves and provides them decision making information they need.

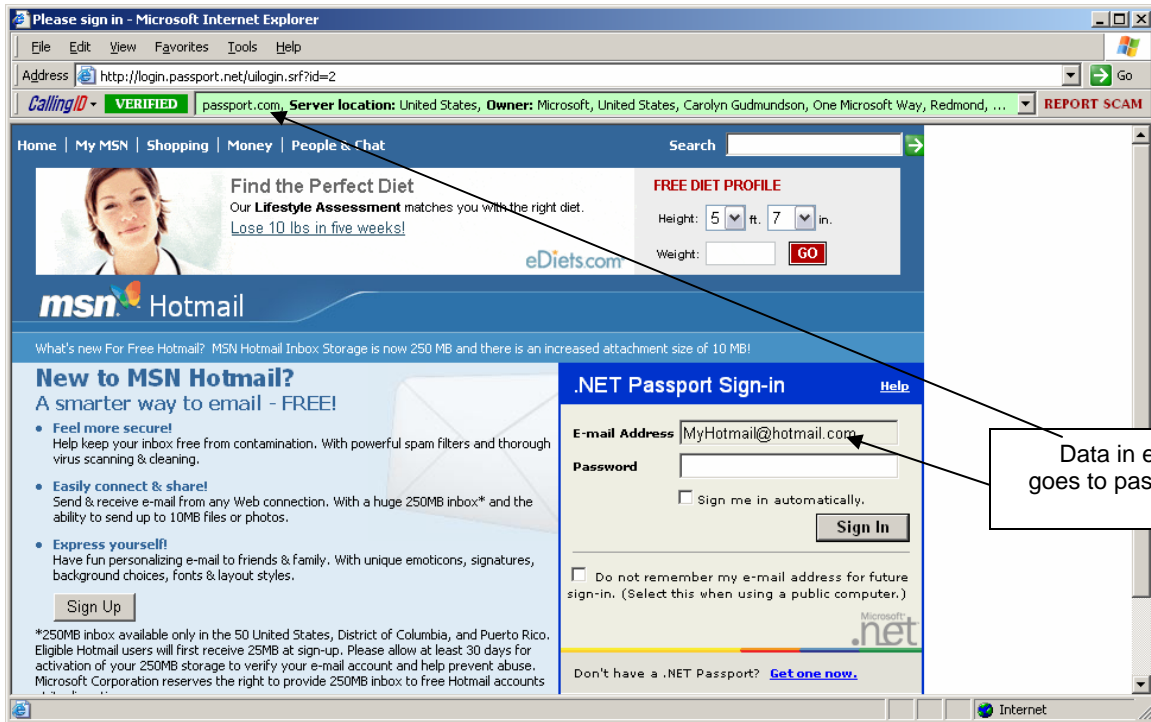
It alerts them to all types of identity theft and scamming threats and informs the user about the site being accessed. Like "caller id" on the phone, the CallingID panel shows the user who is being called. Unlike "caller id" the CallingID software includes a lot more. It provides a risk assessment (verified, low risk and high risk), identifies the site being visited, the location of the site and the owner's address. CallingID was designed with end-users in mind and watches for extremely sophisticated information theft techniques including dealing with sites hidden within verified site pages.

For example, if you were to visit [www.hotmail.com](http://www.hotmail.com) (see example below) you would actually be going to a page on the passport.net site, moreover:

- If you enter some data in the search field this data goes to msn.com
- if you type your email address and password the data goes to passport.com

CallingID immediately identifies the site being visited or where data will be sent before you press enter, and it automatically provides a risk assessment. It often exposes some surprises, for example the login to hotmail and its associated sites are all identified by CallingID as owned by Microsoft from Redmond, Washington.

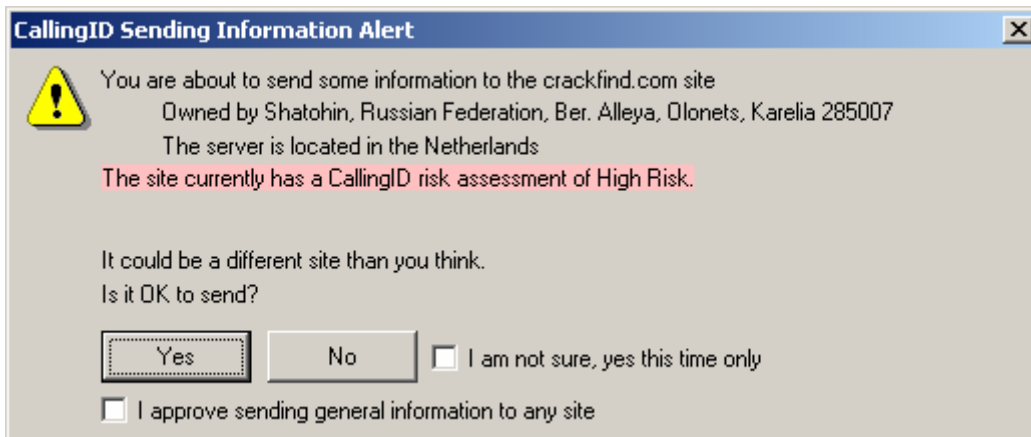
The screenshot shows a Microsoft Internet Explorer browser window. The address bar displays <http://login.passport.net/login.srf?id=2>. A CallingID overlay is visible at the top of the page, showing a green bar with the text "CallingID - VERIFIED" and "Server location: Israel, Owner: Microsoft, United States, One Microsoft Way, Redmond, WA 98052, Redmond, WA". A "REPORT SCAM" link is also present. Below the overlay, the browser displays the eDiets.com website. A search field is visible on the page, and a callout box points to it with the text "Data in search field goes to MSN.com". The browser window also shows the "NET Passport Sign-in" form with fields for "E-mail Address" (lyoramjunk@hotmail.com) and "Password".



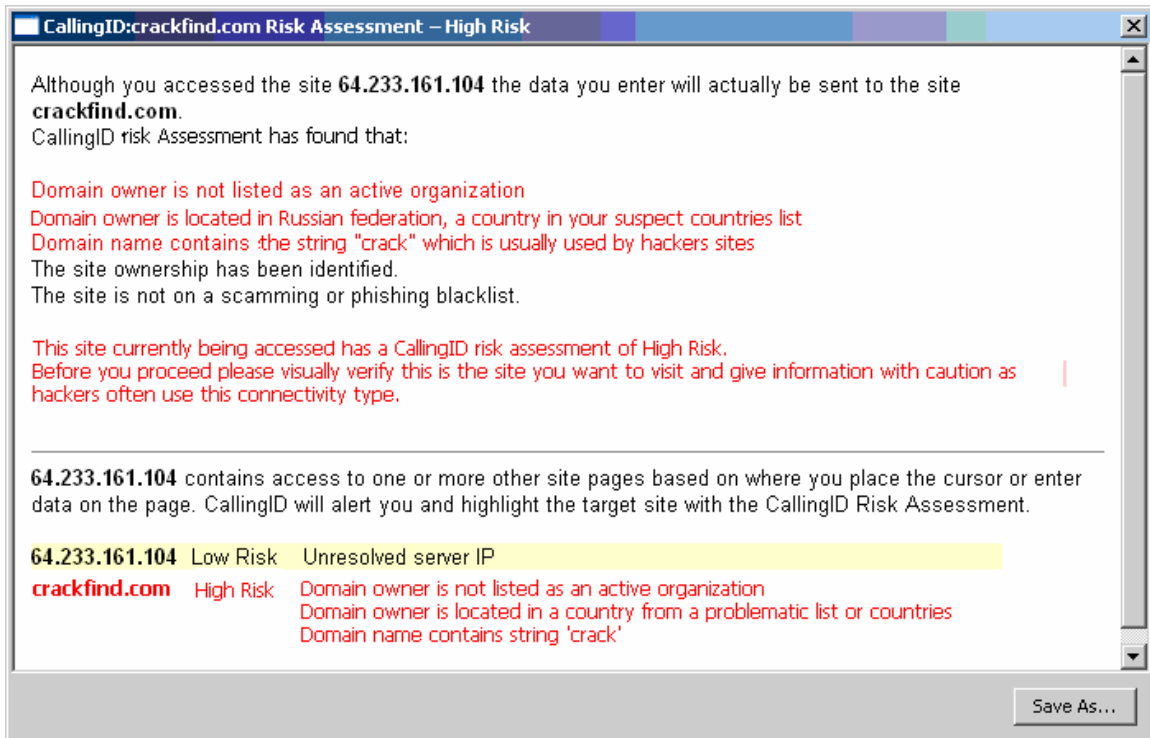
Now let's look at a CallingID identified High Risk example, a Google search for "crack find" results with [www.crackfind.com/](http://www.crackfind.com/). However, when you press the text cached for [www.crackfind.com/](http://www.crackfind.com/) you will see a new page that has a strange address:

[http://216.239.63.104/search?q=cache:px4PfrzmOYJ:www.crackfind.com/+crack&hl=en&lr=lang\\_en|lang\\_w](http://216.239.63.104/search?q=cache:px4PfrzmOYJ:www.crackfind.com/+crack&hl=en&lr=lang_en|lang_w).

CallingID informs you that the page is owned by Google, but it also shows you that data will go to crackfind.com, a site located in the Netherlands and owned by Shatohin from Russia and there is high-risk in sending information to that site, before you send it. While this is all interesting it is very confusing to most users. To help sort this out, CallingID issues the following alert and information if you try to send any data to that site:

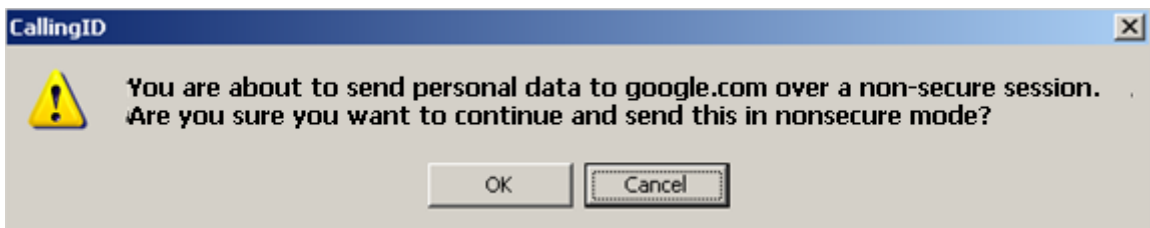


The alert lets the user decide what he or she wants to do. If the user knows the site he may choose to approve it. Approving the site eliminates subsequent alerts when accessed. As a general rule, however, sites assessed as "high risk" should be avoided. To assist any questionable judgment calls, the user can click the CallingID risk assessment (verified, low risk, high risk) this provides a comprehensive list of the criteria that should be considered and how they apply to this page. See the example:



As can be seen from the CallingID Risk Assessment above, this provides a very specific list of considerations and guidance. This helps users become knowledgeable of the considerations and enables them to proceed based on an educated and informed judgment.

CallingID also provides an alert to make the users aware that they may be sending credit card information in a session that is not secure and encrypted by a valid certificate even if the site being accessed is verified.



In summary, CallingID provides a comprehensive yet very user friendly identity theft and fraud detection assistance mechanism that is easy to understand and use without training. CallingID makes the Internet safe to do business again.

*CallingID is based on unique patent-pending technology. It includes more than 50 algorithms that analyze the pages and the sites behind the page in order to identify exposures, phishing, pharming, key-loggers and other risks. CallingID Site Owner Verification includes over 250 constantly reviewed sources to ensure the most meaningful information possible about the site ownership.*