

FIRST CYBER SECURITY: PROTECTING YOUR BRAND ONLINE AND CREATING GREATER CUSTOMER CONFIDENCE

Traditionally, when we use online banking or e-retail sites, one of the very first things that we need to do is authenticate who we are. Various permutations of mothers' maiden names, dates of birth, pin numbers or difficult to remember number sequences given to us by our bank or e-retailer are requested in various forms to ensure that we really are who we purport to be. A necessary evil to ensure the fraudsters who would like to release us from our cash or steal our ID, find this information difficult to obtain: or do they? Sadly, the fraudsters are often one step ahead (at least) and they have developed a plethora of techniques to overcome even the most difficult of antifraud precautions.

Phishing is probably the most common, where the customer is duped into believing they are at an authentic site and happily input their data, to be collected by the fraudster and used at a later time to relieve us of our hard earned cash. APACS the UK payments association, estimate that 18% of us are still selecting URLs from emails that we receive, which often initiate this type of fraud, despite the huge effort by all website owners to educate customers not to do this. But in order to trap the more IT literate users who do not fall for this type of approach the fraudsters have developed more sophisticated techniques like DNS poisoning or frame spoofing, which are almost impossible for the customer to recognise when using a website. If not complex enough, newer types of fraud such as cybersquatting and typosquatting not only lead to customer confusion but also sales of counterfeit goods and perhaps most importantly it damages the online brand. Interestingly, it is not just banks and retail organisations that can be damaged by this type of fraudulent activity. Media organisations have fallen foul of misinformation being communicated supposedly on their sites as have software organisations, whose latest anti-virus or new printer drivers have actually proven to be malware. It is no surprise that every organisation whether in the private or public sector has to consider the implications of all of these types of fraud in their online offering.

Given these difficulties how can we instil confidence for online customers and protect website owners from increased fraud and causing harm to the brand?

Fraudsters are often one step ahead and they have developed a plethora of techniques to overcome even the most difficult of antifraud precautions.

First Cyber Security reports

First Cyber Security has developed a technique which authenticates the website on behalf of the customer (not the website owner). Whilst this concept may not be entirely new, the philosophy behind how it works certainly is. Previous website authentication mechanisms have all been "in browser"; a logo on a website is supposed to give "authentication" by its mere existence, but in reality it is easy for a fraudster to replicate, or a certificate which again is not difficult to compromise. These certificates can also be confusing as often the certificates and the websites they relate to, have different names.

First Cyber Security has developed an online identification mechanism for customers to have assurance that the website they are visiting is the one where the website owner wants them to go. Designated "SOLID Authentication™"; or Secure OnLine IDentification, the technology is independent of the browser and appears as a separate "always on top" window which the customer can place anywhere they wish on the screen. When they visit a website belonging to a subscriber to the FCS service the subscriber's logo appears in the SOLID Authentication window and the window turns green. There is no user intervention required at all, we call this innovation, Security at-a-glance™ and the customer can take confidence that should this website be attacked by any of the fraudulent techniques that are becoming commonplace, the SOLID Authentication™ service will not

Figure 1: Example of a positively authenticated site for Southern Stone Bank, with the logo appearing in the SOLID Authentication™ window



show the website owners logo and the window will turn yellow. This positive authentication is a major step forward in introducing a dynamic, fast and simple to understand mechanism for safe internet usage.

Behind the positive identification is an eight stage process which is applied on every separate page view, from the first to the last. Not only is each page authenticated but also any frames that appear on the page such as dynamic advertisements. It allows the customer to have multiple windows in use, reporting only on the current active window or tab and deploying a number of innovative security techniques to ensure that compromise is extremely difficult. It doesn't matter to the customer at which stage the authentication process has failed (it could be different depending on the type of fraudulent activity), what matters is that the process failed, meaning it may not be safe to enter personal details to the website. This is particularly important where the customer normally sees the website owner's logo in a green SOLID Authentication™ window as it is an indication that something on the site has changed.

An extension to the First Cyber Security subscription service allows subscribers to request that a particular

website is blocked to their customers. In this case customers visiting a typosquatting or phishing site for instance will see a red SOLID Authentication™ window and a large red form appear on the screen telling them that the website they wanted has been reported as fraudulent or fake, and as such any download from the site has been disallowed. This is to ensure any malware that might be present on the site does not get downloaded on to the customer's computer, further protecting the customer from losing personal data. Whilst there is always an option for these sites to be closed down by the ISPs, they are more commonly hosted in foreign countries where the ability to close these sites down takes time. Although many companies claim that the average time to get fraudulent sites closed down and inaccessible to their customers is a couple of hours, in practice this is much longer. The SOLID Authentication™ service will indicate such unsafe sites to the customer immediately (there will be no company logo showing in a yellow SOLID Authentication™ window) and within 30 minutes of a site being reported as fake those subscribers to the extended service will be presented with a red SOLID Authentication™ window and the website will be inaccessible, protecting them far quicker than waiting for the website to be shutdown. Companies who reimburse their customers' losses from fraudulent activities also reduce their cost of fraud and all companies using the service benefit from improving their corporate responsibility.

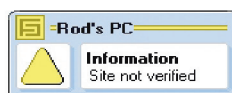
The subscription service is available with an unlimited licence to download the client software. The client software can be deployed in either the home or in a corporate environment.

For further information or a demonstration, please contact:
 First Cyber Security on 08450 564232 or email info@firstcybersecurity.com

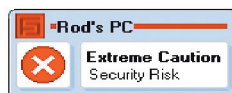
Figure 2: FCS guide to symbols



When you see the green symbol and the bank's logo you know that you can trust the website and that it is SAFE to use.



When you see the yellow symbol, FCS cannot verify the safety of this site although this doesn't mean it's unsafe. You should exercise caution on whether to use the website.



When you see the red symbol, FCS has identified this as a security risk and you should exercise extreme caution.