99 – May 2008

Online Survival Kit

Trying to be practical, clear and objective I propose ten actions that can increase your security over Internet transactions.

1- Know where you are stepping.

The first and most important step is to know your risk "appetite". Making payments over the Internet is not 100% safe, so it is prudent to know the limit of your credit card, for example, so you can then evaluate your disposal and sensibility in the case of fraud. In practice, you should assess the potential of loss compared to the benefit resulting from the convenience of making the payment and the purchase itself from the comfort of your home or office.

2- Know who you are purchasing from.

In theory, purchasing on the Internet is to negotiate with a web server and an investment that, at times, we do not even know where it is located. However, in practice, knowing the company that is behind the market operation could considerably reduce your chances of loss. Search for references published on the Internet itself, especially on sites of complaints and certify the policies of privacy adopted by the company and commonly advertised on their e-commerce site.

3- Know how your information is transmitted.

The most critical moment of security is when you supply your payment details, and, for this reason, you should certify and identify the features of security in this environment. The simplest way of identifying the maximum level of protection is to look at the bottom of your Internet browser if there is a yellow padlock indicating that it is closed. This means that the communication between your computer and the e-commerce server is being encoded and, therefore, all the payment details being supplied are confidential.

4- Know the features of the means of payment.

When you make an online payment, there may be many models adopted by the e-commerce sites, but if you can choose, you should prefer those that operate in partnership with the credit card operators or with specialised sites, recognised publicly, which mediate the payment process from beginning to end, like PayPal. This is because there is no one more interested in protecting your payment details than the credit card operators themselves, which create a certain peace-of-mind in this kind of situation and prevent you from trusting the e-commerce sites and the practices of protection and confidentiality. These processes are usually well-automated and after they are concluded, the operator or the mediator communicates to the site that the payment was successful so that the purchasing process can be concluded.

5- Find out if your computer is compromised.

Many times fraud occurs not because of security failure in the transmission of data or the e-commerce site negligence, but the user's failure in not protecting their own computer. This vulnerability allows strangers to monitor, even remotely, the use of your computer and then "bugging" the communication at the time you supply your card details to the e-commerce site. Once they have obtained these details, third parties can forge legitimate operations and cause financial loss. This is why, you should check if your antivirus programme is up-to-date, if your computer is infected and especially, if your computer does not have any sign of suspect behaviour. In this case, do not use it to make payments.

6- Know how to choose a password.

It is always difficult to choose a password, and worse, having to choose a different password for each service or even, each e-commerce site. Nevertheless, this behaviour is critical and adopting "weak" passwords can jeopardise the security of your details and generate losses. This is why, respecting the limitation of each e-commerce system or site, try to form passwords that are difficult to decipher. Mix random numbers with letters and, if possible, special characters. However, do not try to be too creative so you forget it nor write it down to remember it later. For intensive users who have more than ten passwords, I recommend the use of special programmes that with a single cryptographic key, can store all the passwords safely.

7- Know how to choose the best means of payment.

Not always the most practical means is the best to be used on the Internet. If your choice of payment is credit card, choose the one with the lowest limit and use it only for online purchases, so this way you will have more control and you will run less risks due to the low loss potential defined by the limit. Alternatively, if the e-commerce site allows, you should use the service of well-known mediating companies, like PayPal, preventing you from revealing your payment details to every Internet site where transactions are made. Once you do this with one mediator, it will be responsible for confirming the payment without exposing and transmitting all of your confidential details.

8- Know how to back off even if your impulse tells you not to.

The Internet is still a no man's land, with no law, or better, without the same controls as in the real world. This is why it is possible to find everything on the large network. From traditional shops that are expanding their operations to those you have never heard of, God only knows where they are physically and legally established and at times, selling products at irresistible prices. In this case it is better to resist. It is not the case that you cannot make good deals with new companies safely, but in general, all of this obscurity can represent a fraud, a trap and, therefore, loss to the buyer. There are obvious frauds that are easy to identify where a payment is made and no product is ever received, but others are quite professional where the buyer is pleased with the payment and receipt of the product for an

honest price, when in fact, the fraudster benefits not from having made the relevant deal, but for having captured their payment details to use them subsequently without authorisation.

9- Know how to transform the online purchase into a positive experience.

There are online purchasing risks, like others that occur daily in the real world, but in a certain way, we know how to administrate the "real ones". Thus, do not make the decision of online purchase become martyrdom. The first step is to understand the risks involved and consider them with the benefits of this new model. After making the decision based on the analysis, follow the steps mentioned above you can rest assured that you have done the best that you could have. Purchasing online and losing hours of sleep does not make any sense, and is not worth it. Do not feel pressured by society if you do not feel comfortable in doing transactions over the Internet, or alternatively, you could start with small transactions. At first, with a special credit card with a small limit, used only on known sites and for small purchase amounts. Only time and your own experience may help you to overcome fears and inherent risks to this type of operation.

10- Know how to react if you are at risk of fraud.

Even after taking all the necessary measures, if there is a sign of fraud or information leakage, do not despair. The first step is to communicate the possible illegitimate operation or even, your perception of fraud to your bank or credit card operator. This will help them identify the fraud in progress and, at times, interrupt it even before it is happens. It will prevent new frauds from occurring with the same means of payment, also allowing you not to be liable for future responsibilities because of the communication of suspect behaviour. In these cases, it's a race against time and the longer you take to react, the more time the fraudster will have to increase the extension of damage. In the end, if you are affected, you must not think of the Internet as bad. It is different and you will not have been the first nor the last person affected by a fraud, which can now be done online.

Marcos Sêmola is Global IT GRC Manager at Shell International Limited Gas & Power in Holland, CISM, BS7799 Lead Auditor, PCI Qualified Security Assessor; Member and founder of the Institute of Information Security Professionals of London. MBA in Applied Technology, Professor at FGV with specialisation in Negotiation and Strategy by London School, Bachelor in Computer Science, author of books on information security management, governance and competitive intelligence. Visit www.semola.com.br or contact marcos@semola.com.br