The Safe Route to Banking Online

Digital banking ushered in a new era of banking that translates into agility and convenience for today's customers, important considerations particularly for the modern fast-paced lifestyle.

However, another equally important consideration is peace of mind. Banks worldwide make significant investments to provide self-service banking channels and make them secure. That does not however exonerate the individual from acting responsibility. There are basic safeguards that one may, and should take, to avoid fraud and theft.

Credit and debit cards have evolved significantly over time, with enhanced security often being the driver for change. Chip and PIN technology requires the cardholder to insert the card into the reader at the Point of Sale and enter the PIN, thereby making it harder for thieves to use stolen cards, since they would need to authenticate the transaction by inserting the 4-digit PIN. The onus of the card holder here is to ensure that the PIN is not divulged to third parties, and definitely not stored with the card itself.

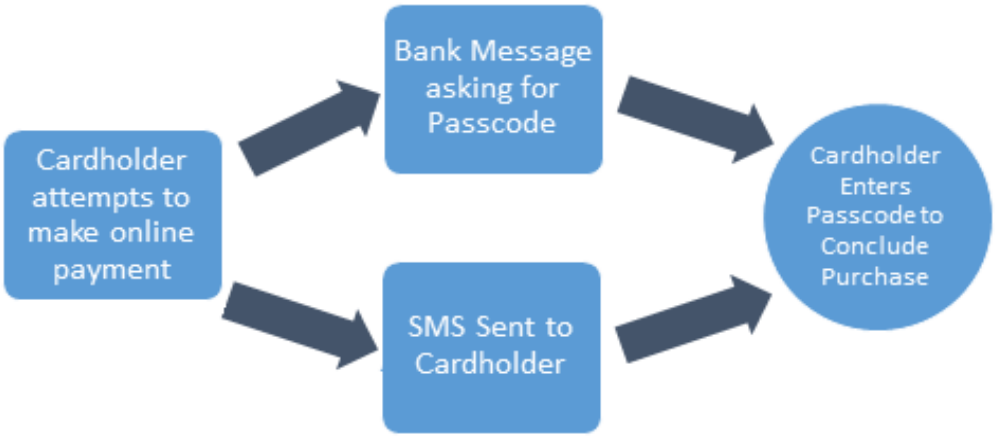
Another security measure embedded in cards is the number of times one can enter a wrong PIN. Generally limited to two, this measure acts as a deterrent for fraudsters who attempt to guess a PIN by trial and error. Cards also carry a daily limit. Effectively, this constitutes a ceiling beyond which one cannot withdraw from a given card in one day. In this manner, should the card be stolen, the third party would not be able to withdraw more than the daily limit in 24 hours, thereby giving time to the cardholder to report the card as stolen to his bank and have it cancelled.

Another measure taken by several banks is the requirement for a cardholder to activate new cards upon receipt. In such instances, one would need to carry out a simple procedure, which generally entails contacting the Bank by SMS or phone, to have the card activated. Thus, should a third party intercept both the card and its PIN in the mail, he would still not be able to use them. Several banks also offer SMS alerts. Cardholders subscribing to this service receive an alert when an activity deemed unusual is processed with their card. Every bank sets its own criteria for the alerts, but they often include country from where transaction is triggered and amount. Thus one should always inform the Bank when about to travel with one's cards, so they are not flagged for unusual activity should one use them to buy croissants on Champs Elysees.

Cards are the perfect tool for online shopping, and who can resist shopping online? However one should never put down one's guard, particularly vis-à-vis phishing

attacks. In simple terms, these refer to attempts by thieves to swindle an individual out of his sign-in credentials and credit card information.

There are basic steps one can take to ensure that one is safe whilst shopping online like sticking to trusted sites and checking the online statement regularly so as to take prompt action should there be irregular activity on one's card. Banks also take measures in this regard. For instance, some banks offer *3D Secure*. This is a programme which links the seller's website to the seller's bank and the bank card issuer. Thus, when the cardholder is processing a transaction, he is provided with a one-time passcode on his mobile phone which he must use to authenticate and authorise the transaction, thereby safeguarding him from the unauthorised use of his cards.



Banks invest in the security features of their electronic channels. However customers play a very important role in ensuring they remain safe online. Taking simple precautions goes a long way in ensuring a reasonable level of security. Thus, for instance, when using electronic banking, it is good practice to type the site's URL directly on one's browser. Phishing emails often contain links to a website which would look similar to the original but would really be fake, intended to steal one's login credentials and other confidential information. As a general rule, banks do not send emails to their customers requesting personal information, so one should exercise caution in such instances. It is also good practice to ensure that one's PC, tablet or mobile phone is regularly updated with a good antivirus software and that this software is active at all times.

Online banking spells convenience, and banks go to great lengths to provide their customers with secure systems. By remaining vigilant and exercising caution, customers may make the most of the convenience that these channels provide.

Victor Borg
Manager Multi-Channel Banking
Electronic Banking Unit
Bank of Valletta p.l.c.

7 April 2017