Safe Internet Banking

Who Are We:

The National Telecom Regulatory Authority (NTRA) was established in 1998. The NTRA's legislative and regulatory framework has been defined pursuant to the Telecom Regulation Law No. 10 of 2003, that stipulated that the NTRA is a national authority competent to regulate and manage the ICT sector on the basis of fundamental principles, including, transparency, free competition, universal service, consumers' rights protection and non-monopolistic practices.

Chief among NTRA's goals are the provision of high-quality telecom services at the most affordable prices, in addition to the exertion of all efforts to enhance the services, keeping abreast of the state-of-the-art technologies and huge advancements in ICT field. Thereupon, and in implementation of NTRA's main goals, the Consumers Rights Protection Committee (CRPC) was formed in August 2004. It allows all telecom service users to communicate and interact directly with all telecom users by launching awareness campaigns and taking various measures. The CRPC, chaired by NTRA's Executive President, comprises notable public figures and convenes regularly.

In order to activate and fulfill the rights of every user to be provided with high-quality services, get clear and all-inclusive information about them and obtain health and environmental parameters, the NTRA established the Call Center. NTRA's Call Center receives complaints, inquiries and technical complaints of service failure from all users in the A.R.E., through the hotline (#155) and the free number (08003330333). It acts as a second-tier or second level for examining and solving such complaints, around the clock, in case the subscriber does not have his problem solved by the service provider.

To know the latest and most important ICT news on the local and international levels in addition to all issues related to the telecom market in Egypt, you can visit NTRA's website: www.tra.gov.eg. You can also address the NTRA through the following address: Smart Village, B4, K 28 Cairo-Alexandria Desert Road, Giza, A.R.E.,

Tel; (+202) 35344000;
Fax: (+202) 35344155;
Email: info@ntra.gov.eg
Youtube: http://www.youtube.com/user/CRPCNTRA
Facebook: https://www.facebook.com/CRPC.NTRA
Twitter: https://twitter.com/crpcntra

The ability to carry out online banking services has immensely changed persons' lifestyle. Ever since they became able to use these services, people have managed to save time and money such as the fees they used to spend for parking in front of banks. The ability to manage most banking needs without having to be present at banks has driven the success and popularity of online banking. However, swindlers and crooks have also followed the trend and banking-related cybercrimes have been on the rise too. Thankfully, any prudent internet user will be able to continue using online banking services if some tips and suggestions are strictly adhered to.

Here are some of best tips:

- **Use effective antivirus software and solutions and firewalls to protect yourself against hackers:** You should protect yourself from cyberattacks, for malware has become very sophisticated these days and any PC without an advanced robust antivirus system installed thereon will be at a high risk. Computer infected with viruses and malware are especially vulnerable. You may be typing and sending your banking instructions to your bank but that information may also be going, without your knowledge, to some criminal somewhere. The good news is that there are good free antivirus solutions available if you do not want to fork out money for these solutions. However, we do recommend you to consider buying a solution. If you believe that your PC has been hacked, call your bank immediately to have your online banking facilities suspended until you clean up your PC.

- **Update your browser:** You should update your web browser regularly. Simple measures like this can keep you safe online. Companies, that manage web browsers, update them once any vulnerabilities have been detected or when they have installed additional security measures into their application. Using an old version of a web browser is similar to walking out at night without being accompanied by guards to protect you from any attack.

- **Choose a safe place for online banking**: Do not ever carry out online financial transactions in public places. If you access the Internet from a local café, using the free Wi-Fi service, you might be at risk of being snooped upon by someone else on that same Wi-Fi network. You have to go online in safe places only such as your home or office (if you are certain that the network is safe).

- **Keep a sharp eye on the screen:** Do not click on a link that supposedly leads you to the bank you are dealing with. The link might look like your bank's url but it might be a fake website set up to capture your banking details and steal your money. Always look at the urls listed on the browser and make sure that it is the correct web address. That is why you must memorize your bank's web address and type it, on your own, every time you access its website. Most online banking systems have high levels of security. To access an online banking system, you should follow two login steps that involve pictures or phrases that are shown on the screen before you type your password, and you have selected previously. Make sure every time that the picture and or phrase is correct.
- **Ignore emails and SMSs:** Banks do not ask you the customers to re-verify their bank details or suspend accounts through emails, or even through SMSs. You can safely ignore

any such messages or requests. Moreover, do not ever send your login details to anyone by email.

- **Check banking transaction codes:** always check the third-party account number shown in the verification text message that you receive when you carry out a transaction. If your online account has been hacked or compromised, you will send money to a person you do not know. You might think that you are sending money to your son, for instance, but a malware on your PC could have secretly altered the account details when you typed them and instructed your bank to send the money elsewhere. By checking the verification SMS and your online transaction records, you will be able to stop the fraudulent attack before the crooks have the chance to steal your money.

- **Phone calls**: If you are unsure about any requests, instructions or communications you receive, do not hesitate to call your bank helpline to get more information. At the same time, be very cautious if you get calls from someone claiming that he represents your bank. Do not ever give out secret information (such as your password) to anyone including the staff of the bank you are dealing with. If you doubt the identity of the caller, end the call immediately and dial up your bank phone number.

- **When friends call for help**: Cybercriminals use all ways to get your banking information. One common way is to use the hacked account of one of your friends and request your banking information from that account. In addition, you may receive an email or SMS from one of your close friends, informing that he is stuck in another country and has no money. He asks you then to transfer money to a certain account number urgently. Do not fall for that trick! Another cunning trick is to inform you that one of your close friends has had an accident and needs urgent financial assistance. You should contact that person directly and if, in doubt, contact the police to report the issue.

- **Online purchase transactions**: You should make online purchase transactions from well-reputed websites. These websites have secure e-commerce systems and measures that create a safe environment for online shopping. You should be cautious of purchases from untrustworthy websites. Moreover, you should be wary of direct transactions with buyers and vendors found on forums and websites. When you make those sorts of transactions, be careful and do not share banking information with anyone, for swindlers want only to know your name and account number.

To sum up, keep your PC updated, install a powerful antivirus system, and ignore suspicious requests you receive. You have only to be connected to banks from safe places and deal with strangers cautiously. You must strictly adhere to the aforementioned steps and you will be safe from cybercrimes. Share these tips with your acquaintances and relatives that have an online bank account.

For Mobile, Internet and Fixed Service Users:

If you have encountered a problem with the service provider and could not solve it, call the Call Center hotline (155) and we will exert all efforts to solve your problem. The Call Center receives complaints and inquiries on a daily basis throughout the week.