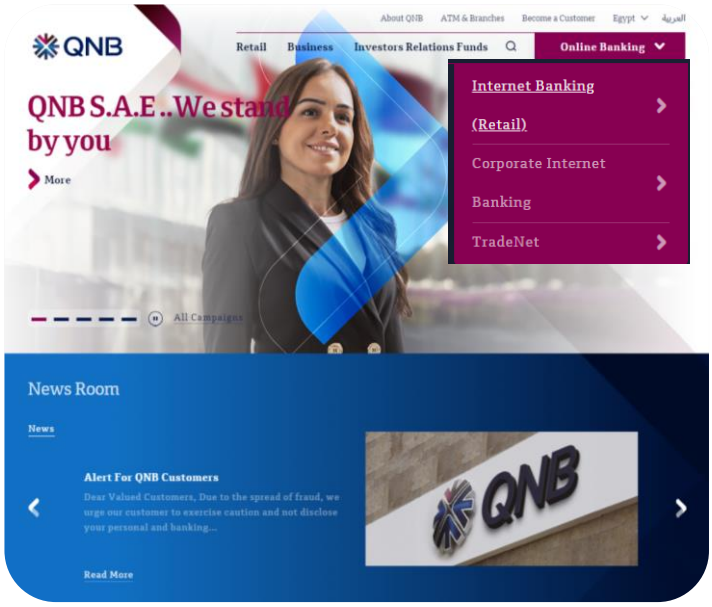
Internet security message:

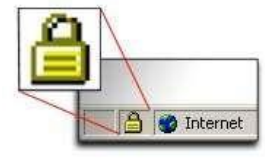
Protect yourself from fake web sites:

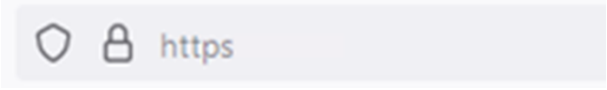
1. When you want to access our website, enter the address of the QNB (QNB) online https://ib.qnb.com.eg
   You can access it from our main web site. https://www.qnb.com.eg
   Never access it from untrusted links.



2. To make sure you're on a secure Web server, check the beginning of the Web address in your browsers address bar - it should be "https://" rather than just "http://"

3. Always look for the padlock icon at the bottom of the browser window for secure online transactions/banking.





Protect yourself by following the below tips:

1. Keep your password safe through the following:
    1- Avoid using the same password for different systems that are important to you.
    2- Choose a strong password with complexity requirements (Letters, Numbers, Special characters, …)
    3- Do not use passwords less than 8 characters in length.
    4- Do not use passwords used for four previous trials before.
    5- Change your internet banking password periodically.
    6- Choose a password that is non personal or difficult to be guessed (away from user name, birth date, …)
    7- Never write your passwords down.
    8- Do not disclose your password to any person whatever the reason.

2. Regularly log into your online accounts and check the last successful or failed log on attempts displayed on the top left of the application.

3. Do not disclose any information personal or business. Keep your user name, password, card details confidential.

4. Keep your computers, portable devices (i.e. laptops, mobile devices, …) safe by installing the last security patches/updates, anti-viruses, anti-malwares, anti-spyware, …

5. Use data encryption on your device to protect it in case of theft or loss.

6- Do not access QNB internet banking from public PCs (i.e. Internet café, etc …) or through public Wi-Fi connections, this is to keep your confidential data secure. And in case you have to, please follow the below instructions:

- Turn 'off' sharing on your device through the 'Settings' options before accessing public Wi-Fi connections.
- Use VPN connections while using public Wi-Fi connections.
- Avoid connecting to Wi-Fi hotpots 'Automatically'.
- Use secure protocols 'HTTPS' when accessing any of your browsers.
- Turn on firewall on your device.

Be aware of: Fraudulent Emails:

Fraudulent email messages appear to come from legitimate sources 'QNB web site for example' indicating that you have won a prize, purchase order you never made or asking you about confidential banking information. The Email invites you to click on links that redirects you to a fake web site or to download an executable file (Malware, Virus, …) to your computer/portable device. If you receive any e-mail from an unrecognized source, you should delete it without opening it and contact directly QNB call center 19700.

Beware of: Scam Email:

Scam Email is an unsolicited email that claims the prospect of a bargain or something for nothing. Some scam messages ask for business, others invite victims to a website with a detailed pitch. Many individuals have lost their life savings due to this type of fraud. Scam Email is a form of email fraud.

Beware of Phishing attack:

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. Communications could be from popular social web sites, auction sites, banks, online payment processors. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users and exploits the poor usability of current web security technologies. Phishing takes advantage of the trust that the user may have since the user may not be able to tell that the site being visited, or program being used, is not real. Therefore, when this occurs, the hacker has the chance to gain the personal information of the targeted user, such as passwords, usernames, security codes, and card numbers, among other things.

Note: IF you have any concern about an email that appears to have been sent by Legit source and you think it might not be legitimate. Please do the following:

- Do NOT click on any URL/Link in the email received.
- Do not reply to the email.
- Contact QNB call center 19700 to validate the email received and to advise you on further Instructions.