Security Features

It is our mission in Metrobank to provide you with banking services that address your needs and it is important for us that you feel secure and confident in your transactions. This is the reason why we're constantly developing, evaluating, and implementing advanced security measures in all our banking channels. Metrobank upholds the security and integrity of your online banking transactions.

We have provided you a list of security tips and information in this section.

1. How do we secure your online banking activities?
   The following are the norms, standards, infrastructure, and procedures by which we secure your transactions, your privacy and exchange of any information with your company.

   - Computer Virus Protection
     We use up-to-date virus protection software that protects our network system from computer viruses.

   - Firewalls
     To protect our system from risks of unauthorized electronic activity (spoofing, hacking, phishing, denial of service) we employ an integrated firewall system over our existing network backbone. This allows us to accept legitimate transactions and reject illegitimate ones.

   - Secured Transmissions
     We use 256-bit Secured Socket Layer (SSL) encryption on all our online transactions. This is the highest type of encryption currently used by all IBS (Internet Banking System) networks. Encryption is a communications process that scrambles private information to prevent unauthorized access as information is being transmitted between the client's PC and the Bank's server.

   - Authentication and Digital Certification
     Authentication is a means of verifying the identity of all parties communicating over the Internet. We use a range of technologies such as GlobalSign digital certificates, passwords and a Multi-Factor Authentication technique to ensure that during a secured Internet banking session, the parties involved are authentic and authorized.

   - Message Integrity
     As the Internet is the communications medium over which transactions are sent to and from the Bank, an e-mail authentication is in place to ensure that the transactions that are sent are not tampered with.

   - Monitoring and Log Control
     Non-repudiability means that the sender or receiver of a transaction done through the Internet is duly authorized and its validity cannot be denied. We ensure non-repudiation through the extensive use of transactional audit trails and comprehensive transaction logging.

   - Automatic log-out feature
     Our systems have an automatic log-out feature that is activated when your computer is left idle for 20 minutes. It is necessary for you to repeat the log-in procedure to continue using the system. This feature promotes the practice of properly logging-out from a system to prevent unauthorized access. A summary of your executed transaction/s is reflected on your Dashboard after logging in.

   - Corporate Code, Username, Password, and Multi-Factor Authentication (MFA) Security Code
     We assign each company and its users a unique corporate code and username and password, respectively, and a system generated MFA security code or one-time pin (OTP) to access Metrobank Business Online Solutions. This information, and/or account code should never be disclosed to anyone because it is the same as giving that individual authority to use your name in a transaction.

2. Why you need to secure your online banking activities?
   A compromised internet banking account can lead to identity theft. An internet banking account may be compromised in several ways.

   - Application-based threats
     Keylogging/screen logging – You may be at risk if you use a public PC (such as PC kiosks in internet cafés) to perform legitimate Internet banking transactions. There may be a chance that your Metrobank Business Online Solutions credentials have been secretly captured by a keylogger/screenlogger or thru an Internet banking Trojan in that PC.

     Malware – A software designed to engage malicious behavior on a device. If you have been recently downloading and installing free softwares/applications (e.g., screensavers, e-cards, games, software cracks, utility programs, rogue anti-virus programs, etc) from the Internet coming from untrusted/unverified sources, your PC can be infected with an internet banking trojan which captures username and password.

   - Web-based threats
     Browser exploits – Man in the middle attacks – Attack where the communication which is exchanged between two users is surreptitiously monitored and possibly modified by a third, unauthorized, party. If you have been using an open public WiFi hotspots, your Metrobank Business Online Solutions credentials can be compromised thru Internet banking session manipulation using Man-in-the-Middle (MITM) attacks.

     Phishing scams - The victim is tricked into providing information such as account log in information by sending an email links to an illegitimate site which looks exactly like the legitimate site. If you previously encountered a Metrobankdirect look-a-like phishing site and have entered/logged-in your MBDirect username and password in the fake site, your MBDirect credential will be captured by the phishing site and eventually be compromised.

- Network threats
  Network sniffing – A method used to capture and analyze data packets sent over WiFi or broadband connection using specialized hardware or software. It can be done maliciously or legitimately. Data being sent from a device may be intercepted by anyone listening across an unsecured wireless network.

3. How to secure your online banking activities?
   Always be mindful of your online transactions. Keep yourself informed.

   - Secure Corporate Code, Username, and Password
     i. Do not disclose Corporate Code, Username, and Password.
     ii. Do not store Corporate Code, Username or Password on the computer.
     iii. Regularly change password and avoid using easy-to-guess passwords such as names or birthdays. Passwords should be a combination of alphanumeric characters with uppercase, lowercase, and numbers. It should be at least 10-14 characters.

   - Keep personal information private
     Do not disclose personal information such as address, mother's maiden name, telephone number, social security number, bank account number or e-mail address – unless the one collecting the information is reliable and trustworthy.

   - Keeps records of online transactions
     i. Regularly check transaction history details and statements to make sure that there are no unauthorized transactions.
     ii. Review and reconcile monthly bank statements to make sure that there are no unauthorized transactions.
     iii. Check e-mail for contacts by merchants with whom one is doing business. Merchants may send important information about transaction histories. Immediately notify the bank if there are unauthorized entries or transactions in the account.

   - Check for the right and secure website
     i. Avoid responding and clicking on unsolicited email attachments and links from unknown/unverified sources especially if you are not expecting any emails from them.
     ii. Check e-mail for contacts by merchants with whom one is doing business. Merchants may send important information about transaction histories. Immediately notify the bank if there are unauthorized entries or transactions in the account.
     iii. Before doing any online transactions or sending personal information, make sure that correct website has been accessed. Beware of bogus or "look alike" websites which are designed to deceive consumers.
     iv. Check if the website is "secure" by checking the Universal Resources Locators (URLs) which should begin with "https" and display a closed padlock icon on the status bar in the browser. To confirm authenticity of the site, double-click on the lock icon to display a security certificate information of the site.
     v. Always enter the URL of the website directly into the web browser. Avoid being re-directed to the website, or hyperlink to it from a website that may not be as secure.
     vi. If possible, use software that encrypts or scrambles the information when sending sensitive information or performing e-banking transactions.

   - Protect personal computers from hackers, viruses and malicious programs
     i. Install a personal firewall and a reputable anti-virus program to protect personal computer from virus attacks or malicious programs.
     ii. Ensure that the anti-virus program is updated and runs at all times.
     iii. Always keep the operating system and the web browser updated with the latest security patches, in order to protect against weaknesses or vulnerabilities.
     iv. Always check with an updated anti-virus program when downloading a program or opening an attachment to ensure that it does not contain any virus.
     v. Install updated scanner software to detect and eliminate malicious programs capable of capturing personal or financial information online.
     vi. Never download any file or software from sites or sources which are not familiar or hyperlinks sent by strangers. Opening such files could expose the system to a computer virus/malware/trojan that could hijack personal information, including password.

   - Do not leave your computer unattended when logged in
     i. Log off from the Internet banking site when computer is unattended, even if it is for a short while.
     ii. Always remember to log off properly when online banking transactions have been completed.
     iii. Clear the memory cache and transaction history after logging out from the website to remove account information. This would avoid incidents of the stored information being retrieved by unwanted parties.

   - Check the site's privacy policy and disclosures
     i. Read and understand website disclosures specifically on account debit/credit policies and other bank terms and conditions.
     ii. Before providing any personal financial information to a website, determine how the information will be used or shared with others.
     iii. Check the site's statements about the security provided for the information divulged.
     iv. Some websites' disclosures are easier to find than others – look at the bottom of the homepage, on order forms or in the "About" or "FAQs" section of a site.

   - Other internet banking security measures
     i. Do not send any personal information particularly Corporate Code, Username or Password via ordinary e-mail.
     ii. Do not open other browser windows while banking online.
     iii. Avoid using shared or public personal computers in conducting online banking transaction.
     iv. Disable the "file and printer sharing" feature on the operating system if conducting banking transactions online.
     v. Contact the banking institution to discuss security concerns and remedies.

4. What to do if you have been compromised?
   Be alert and get in touch with us right away.

   - Immediately report to your System Administrator or to your depository branch. You may also call our Customer Care Desk Hotline from Mondays to Fridays except during bank holidays from 8:30AM to 7:00PM only at 898-8000 press 2, then 2, 1-800-10-8579727 for domestic toll-free, 0949-9942417 (Smart) or 0917-5233364 (Globe) or send an e-mail at **ibs.customercare@metrobank.com.ph**.
   - Have your Metrobank Business Online Solutions account credentials (i.e. corporate code, username and password) blocked or disabled temporarily until such time that you have cleaned (reformatted) your PC where you usually perform your Internet banking transaction.
   - Once you have cleaned and restored your PC from scratch by reformatting and reinstalling everything, install a legitimate anti-virus tool and perform an anti-virus and windows security updates.
   - Make sure that you have installed all the necessary security patches and hotfixes for your Microsoft Windows operating system before requesting for account enabling.
   - Call your System Administrator or your depository branch or Customer Cervice and request for account re-activation by requesting for new password mailer.
   - Upon issuance of your new password, change it immediately with a new set of password value to something that you can easily remember.