Digital Starter Kit

Get Started: How to Register

You can watch the video here or follow these steps.

1. On your browser, go to www.hsbc.com.ph and click Register.
2. Click on Register Now.
3. After reading the Terms & Conditions, click the tick box to accept. Click Continue.
4. Choose your registration method:
    a. Phone Banking Number + Phone Banking PIN
    b. ATM/Debit Card Number (Primary) + Issue Number + ATM PIN
    c. Credit Card Number + Cash Advance PIN

    Click Continue.
5. Create your unique username, memorable question and password. Click Continue.
6. Set up two security questions and answers. Click Continue.
7. You've successfully registered. Now you can order your Secure Key.

Get Started: How to order a Secure Key

Free when you register to online banking, just follow these steps to have your own:

1. Log in to your account at www.hsbc.com.ph using your memorable answer and password (Without Secure Key type of log on).
2. Click on your name at the top Menu bar then click Manage Secure Key.
3. Follow the on-screen instructions to place an order and choose between picking it up at one of our branches or having it delivered to you.
4. Once you receive your Secure Key, prepare to set it up.

Get Started: Setting up your Secure Key

1. After you register for online banking, log in to your account at www.hsbc.com.ph and simply follow the on-screen instructions to begin setting up your HSBC Secure Key.
2. You will be led to the Activate your Secure Key page. Click on Generate an activation code now (this will be sent to your registered mobile number) and enter the code on the field.
3. Enter your device's serial number found at the back.

4. Create your Secure Key PIN.
    a. Turn on your device by pressing and holding the green button. New PIN will be displayed on screen.
       TIP: The Secure Key does not have an off button. After 30 seconds of inactivity, the device will automatically switch off
    b. Enter a 6-digit PIN of your choice. This PIN will be your password everytime you use the device. After you enter your PIN, PIN CONF will be displayed on screen. Press the yellow button to continue.
    c. Confirm your PIN by re-entering it into the device. You'll then see NEW PIN CONF and HSBC displayed on screen. Your device is now ready to generate a security code
       TIP: If unsuccessful, press the yellow button to return to Step 1.
5. Generate a security code by clicking on the green button while the screen displays HSBC. Enter the code on the field. Click Continue.

Get Started: Logging In

There are two ways you can log in.

With your Secure Key

Here you'll need your memorable answer and Secure Key PIN to log in.

1. Log in to your account at www.hsbc.com.ph with your username.
2. Click the With Secure Key tab.
3. Follow the on-screen instructions to input your memorable answer and security code.
4. Click Continue.

We recommend using your Secure Key when you log in so you can do any transaction that you need to do online successfully. Click here to find out what you can do with and without your Secure Key.

Without your Secure Key

Here you'll need your memorable answer and password to log in.

1. Log in to your account at www.hsbc.com.ph with your username.
2. Click the Without Secure Key tab.
3. Follow the on-screen instructions to input your memorable answer and password.
4. Click Continue.

Get Help & Support

Once you've logged in and you need additional support, hover on Help & support tab, and under support, click on Online Banking Demo. We have a series of tutorial videos to help you navigate your way through Online Banking.

Security Reminders

1. Browse smartly

- Download your applications from official app stores and check ratings to verify.
- Before doing any online transactions or sending personal information, make sure that the correct website has been accessed. Beware of bogus or "look alike" websites which are designed to trick you.
- Check if the website is secure by checking the Universal Resource Locators (URLs) which should begin with "https" and a closed padlock icon on the status bar in the browser is displayed. To confirm authenticity of the site, double-click on the lock icon to display a security certificate information of the site.
- 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.
- Be wary of dubious third party aggregators. Do not disclose any information like your online banking credentials to third parties.
- Only use trusted Wi-Fi networks or service providers, not free public WiFi.
- Use security protection, at minimum, such as Wi-Fi Protected Access (WPA), if possible.
- If possible, use software that encrypts or scrambles the information when sending sensitive information or performing e-banking transactions online.
- Disable Bluetooth if you are not using it or set your device so it is not discoverable.

2. Maintain your device

- Install a personal firewall, the latest anti-virus and anti-spyware software on your phones, computers and tablets, and keep it updated.
- Install updates and patches to your smartphone, computer and tablet regularly, including upgrades/updates to your operating system (OS) and web browser and other mobile applications in order to protect against weaknesses or vulnerabilities.
- Always check with an updated anti- virus program when downloading a program or opening an attachment to make sure it doesn't contain any virus.
- Install updated scanner softwares to detect and eliminate malicious programs capable of capturing personal or financial information online.
- Install apps on your phones or tablets from trusted sources only. Understand the permissions of mobile apps before you accept and install them. 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 that could hijack personal information, including password or PIN.
- Don't use security loopholes to log on to Online Banking on jail-broken/rooted handsets or tablets. HSBC mobile apps do not run on jail-broken/rooted devices for your security.
- Set up auto-lock and passcode lock to prevent unauthorised access to your phones and tablets and enable remote wiping.
- Log-off from the Online Banking site when computer is unattended, even if it is for a short while.
- Always remember to log-off when e-banking transactions have been completed.
- 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.

3. Be vigilant

- Don't store your username and password for HSBC Mobile Banking and other private services on your mobile handset or tablet.
- Avoid sharing your device with others and don't use other people's devices to log on to your private accounts.
- Some online services might request you to upload a scanned copy of your valid ID via their mobile apps. Protect your ID copy and treat it with the same caution as your physical ID card. Don't store your ID copy on your mobile device and don't share it with people you don't trust or know well. Don't scan your ID copy to any untrusted apps.
- If you have access to SMS service providers' app or portal, make sure to use complex passwords and change your password regularly to avoid fraudsters from intercepting your access and obtaining further sensitive details.
- Contact the Bank to talk about security concerns and remedies to any online e-services account issues.
- Refrain from doing mobile banking transactions in a place where you observe the presence of fraudsters trying to steal your confidential information by looking over your shoulder.
- If the phone is lost or stolen, report the incident immediately to your network provider so they can deactivate your SIM card. If bank details have been compromised, report it to us immediately.

What to do to keep your Online Banking safe

1. Accessing your account

- Avoid using public computers and public networks to do online banking.

- Never share your personal security details (password or security code/OTP) with anyone, especially if they claim to be from HSBC.
- If you find any unusual pop-ups or your computer starts running unusually slow, please don't input your personal details and/or credit card information.
- Do not open other browser windows while doing online transactions.
- Disable the “file and printer sharing” feature on the operating system if doing financial transactions online.
- Watch out for money-laundering scams. Be wary of any "business opportunity" that involves receiving or holding money for strangers.
- Only use secure and trusted wireless networks. Add a password and regularly change this password for your own home Wi-Fi network.
- Use the secure email feature of HSBC Mobile and Online Banking for general inquiries.

If you receive any email or SMS claiming to be from HSBC, remember that:

- We will never ask you to confirm or provide us with any personal data by replying to an email.
- We will not ask you for your PIN or password.
- We will not ask you to provide your CVV/CVC or OTP.

2. Monitoring your account

- Check statements, emails and SMS notifications as soon as you receive them. Review and reconcile statements for any errors or unauthorized transactions. If you spot any errors or unusual transactions, report them to the bank immediately. Use HSBC Online Banking or the HSBC Mobile Banking app to check transactions on your account more frequently.
- Always keep the electronic receipt for fund transfers and bill payment transactions to help you verify transactions.
- Check e-mail from merchants with whom you are transacting with. Merchants may send important information about transaction histories.

3. Protecting your PIN

- Memorise your PIN and never write it down.
- Never share your log-in ID password/PIN with anyone, even if they claim to be from the bank or a regulator.
- Use different PINs/passwords for different websites and channels (ATM, Phone Banking, Online and Mobile Banking).
- Remember that our representatives will never ask for your PIN.

Keeping your personal data safe

- 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.
- Create a separate personal email address from your banking email address.
- Do not click links from random text messages and e-mails.
- Destroy delivery labels that have your name, address and number.
- Do not share or let anyone else know your username or password.
- Transact only with established and trusted merchants.
- Take time to read the privacy notices and T&Cs, especially for sellers who will save your personal and credit card information, to keep your data safe. Check the security provided for the information divulged and determine how the information will be used or shared with others.
- Read and understand website disclosures specifically on refund, shipping, account debit/credit policies and other terms and conditions.
- Some websites' disclosures are easier to find than others — look at the bottom of the home page, on order forms or in the "About" or "FAQs" section of a site. If you're not comfortable with the policy, consider doing business elsewhere.

Protect Yourself from ATM Fraud

1. Stay vigilant

- Be aware of your surroundings when using an ATM. If there's someone or something suspicious, quickly cancel your transaction.
- When using an ATM, choose the one that you are familiar or that in well-lit and/or well-guarded areas.
- Have your card ready before approaching the ATM. Avoid having to go through your wallet or purse to find the card.
- Refuse help from strangers when using an ATM.
- Inspect the ATM. If there are signs of tampering, DO NOT proceed with your transaction. Report it to the Bank immediately.
- If the ATM is not working correctly, cancel the transaction and use a different ATM. If possible, report it to the Bank.
- If your card is captured and you suspect possible fraud, please report it to us immediately.
- Carefully secure card and cash in the wallet, handbag, or pocket before leaving the ATM.
- Do not leave the receipt behind.
- Do not let other people use your card.

2. Protecting your PIN

- Memorize your PIN and do not write it down.
- Choose a PIN that's hard to guess. Avoid using easily available personal information such as birthday, nickname, mother's maiden name or consecutive numbers.
- Cover the numeric keypad and make sure no one is looking while you are entering your PIN.
- Never disclose your PIN to anyone.
- Use different PINs for different channels (ATM, Phone Banking, etc.).

3. Keeping track of your transactions

   Regularly monitoring your account is important to detect any possible unusual activities.

- Always check your statements.
- Switch to electronic statements and get your statements faster.
- Immediately report unusual transactions to us.
- Sign-up to instant SMS notification so you get updates on movement within your accounts.
- Register through HSBC Online Banking so you can monitor your accounts anytime.

If you lose your card, call HSBC's Customer Service immediately at (02)8858-0000 or (02)7976-8000 from Metro Manila, +1-800-1-888-8555 PLDT domestic toll-free, (country code) +800-100-85-800 international toll-free for selected countries/regions.

How to report phishing/vishing/smishing

To report phishing websites, smishing texts or suspicious emails that requested your personal banking information, send an email to phishing@hsbc.com. You'll receive an automatic response to let you know we've received your email.

- Copy the full email, smishing text or website address (URL) and paste it onto the body of the email.
- Do not include your personal information in the email. This mailbox is processed by a third party on behalf of HSBC Global Services (UK) Limited and by HSBC Group companies (this also means we won't be able to give you personalised responses from it).

If you believe you've shared your confidential information either online, by telephone or any other means, call us immediately at +6328858-0000 or +6327976-8000 or +800-100-85-800 from overseas.

www.hsbc.com.ph

Issued by The Hongkong and Shanghai Banking Corporation Limited

 For inquiries or complaints, please chat with us via www.hsbc.com.ph or call HSBC's Customer services at (02) 8858-0000 or +63(2) 7976-8000 from Metro Manila, 1-800-1-888-8555 PLDT domestic toll-free, +(international access code)-800-1008-5800 international toll-free for selected countries/regions. If you want to find out more about HSBC feedback procedures, please visit hsbc.com.ph/feedback. The Hongkong and Shanghai Banking Corporation Limited is an entity regulated by the Bangko Sentral ng Pilipinas (Bangko Sentral) http://www.bsp.gov.ph. You may get in touch with the Bangko Sentral Consumer Protection and Market Conduct Office through their email: consumeraffairs@bsp.gov.ph; Webchat: http://www.bsp.gove.ph; Facebook: https://www.facebook.com/BangkoSentralngPilipinas or SMS: 021582277 (for Globe subscribers only). We maintain strict security standards and procedures to prevent unauthorised access to information about you. We will never contact you by email or otherwise and ask you to validate personal information such as your user ID, password or account numbers. If you receive such a request, please call our Customer Service on (02) 8858-0000.