MiVision Security Advice

Keep your passwords, credentials and personal information secure
Fraudsters use personal information from different sources to steal people's identities.

Viruses are one way to do it. But they also use paper documents containing personal details, such as receipts and bank statements.

Fraudsters use many methods such as searching in dustbins to obtain these documents.

You should take simple precautions to keep your details safe and to dispose of these documents safely, such as shredding them before you bin them.

Your HSBC MiVision password, together with your other HSBC MiVision credentials, permit access to your user profile. When creating passwords, remember the following things:

- Keep them to yourself: No one at HSBC will ever ask you for your HSBC MiVision user credentials
- Make them hard to guess. It should not be based on guessable information such as user-id, personal telephone number, birthday or other personal information
- Use different passwords for different websites, applications or services
- Change your passwords regularly or when there is any suspicion that it has been compromised or impaired
- Never write them down or record them anywhere
- Don't let your browser remember your log on details

HSBC may send One Time Password (OTP) to you via SMS as an authentication measure for your MiVision activities. Watch out for notifications sent by your telecommunication provider about activation of the SMS forwarding function of your mobile device. Check with your service provider and report any suspicious notifications if you haven't authorized the activation. Don't let anyone tamper with your mobile device. You should not reveal the OTP generated to anyone.

Please inform HSBC immediately on the loss of your mobile phone or change in your mobile phone number.

Install anti-virus, anti-spyware and firewall software
Anti-virus, anti-spyware and firewall software protects you and your privacy.

Viruses are bad news. They steal personal information, take over your PC, pop up unwanted adverts and they can even use your computer to attack other people's computers.

You may also hear them called malware, trojans, spyware or adware.

Anti-virus, anti-spyware and firewall software protects you against all of them.

To work properly, anti-virus, anti-spyware and firewall software has to download updates regularly over the internet. Out-of-date software will have flaws.

Any file with no extension (e.g. just named 'file') or a double extension (e.g. file.wow.jpg) is almost certainly a virus and should never be opened. Also, never open an e-mail attachment that is unknown to you and in particular contains a file ending with .exe, .pif and .vbs because these are commonly used with viruses. Always delete junk or chain emails. Do not open email attachments from strangers.

It is a good idea that you install anti-virus, anti-spyware and firewall software if you don't have any already. There are many effective programmes to choose from, but the most common commercial products include McAfee†, Trend Micro, Sophos, Symantec and F-Secure.

†McAfee® software download is only available to PC users.

However, be sure to visit the genuine site because there are many fake products claiming to protect your computer but which may actually infect it with viruses. Do not install software or run programs of unknown origin.

Make sure you have the latest security updates and patches
From time to time, weaknesses are discovered in programmes running on your computer. These weaknesses can be exploited by virus writers and hackers to gain access to computers. As such, publishers will release 'patches' from time to time to correct these weaknesses.

To check for patches and updates you should visit the publisher's website, typically their 'Download' section. Generally, the latest versions of an operating system family (like Microsoft Windows) or browser (like Internet Explorer, Google Chrome, Apple Safari, etc) is the most secure.

Microsoft users can visit: http://windowsupdate.microsoft.com, which can automatically check what is required for both your operating system and browser and then download it at your request.

Apple Mac users can visit: https://www.apple.com/downloads and navigate to Software Update where a list of the most recent security updates is available for download. Alternatively by clicking from the Apple Menu on your Mac device and selecting Software Update you can also be sure you are running with the latest security updates available.

Keep your software and browser up to date
It is harder for viruses to infect updated software.

The criminals who create viruses take advantage of software bugs to infect computers. Software companies fix bugs with free downloadable updates. Most modern software will check for updates automatically. It is a good idea that you install updates for your software as soon as they become available.

Be wary of fake e-mails about bogus updates. Use the update software that comes with your computer – don't click on links in e-mails. You can check if your Windows computer is up to date in the Security Center in Windows Vista and in the Action Center in Windows 7 and Windows 8.

To be sure you are running the latest software on your Apple mac, you can click from the Apple Menu and select Software Update.

As well as your computer software, other programs need updating. The program you use to look at websites is called a web browser. Modern web browsers warn you if you visit fake websites and it is harder for viruses to infect them. It is a good idea that you install an up-to-date web browser. There are several to choose from and they are all free.

If you have updated your computer regularly, it is likely that you are already running either Microsoft Internet Explorer 11 (on Windows PCs) or Safari 7 (on Macs).

How HSBC protects you online
We are constantly reviewing the ways we can help and support you. Our proactive approach includes meeting some of the world's leading security experts to discuss key issues and sponsoring joint initiatives to improve your online security.

We protect you by:
1. Ensuring your online transactions are safe and secure. We use industry-standard security technology and practices to safeguard your account from any unauthorised access.

2. Using logons and passwords to make sure we're dealing with you. Online access to your user profile is only possible once you have authenticated yourself using the correct user credentials and security details.

3. The SMS OTP is an additional layer of protection that will help protect you from internet banking fraud. It is designed to make sure only you can access your personal information.

4. The SMS OTP is commonly being used for secure transactions all round the world. With this layer you can enjoy far more secure online banking services and it's one of the simplest to use. This means you not only need a password or PIN, but you also need unique number to carry out some critical functions, making it more secure for you.

5. Creating secure online sessions. When you log into HSBC MiVision you are said to be in a secure session. You know you are in a secure session if the URL address begins with https:// and a padlock symbol appears at the top of the page as part of the address bar.

6. Using session timeouts. If you forget to log off after banking online or your computer remains inactive for a period of time during a session, our systems automatically log you off.

7. Having automatic lockouts. After a number of incorrect attempts to log in, we disable online access to your HSBC MiVision user profile. To re-activate your account, you should contact your company administrator.

You are reminded to:

- promptly check any notifications, statements, advices that we may send to you
- frequently check your account information, balance and transactions
- log off after each online session
- clear your browser cache after each online session
- take note of the MiVision last login date and time

If you notice any irregularity or unusual transactions, please contact us as soon as reasonably practicable at our Customer Service hotline 1800 227 6227 (Singapore) or (65) 6227 6227 (overseas).

Don't share private information online
Double-check privacy settings on social networking sites.

What's your mother's maiden name? What's the name of the first school you went to? What was your favourite subject at school? What's your address? Birthday? Phone number?

All this information is useful to people who want to steal your identity or break into your personal internet banking. You wouldn't give this information away to a stranger in the street but if you use social networking sites, such as Facebook, Twitter or MySpace, you could be over-sharing personal data.

You may want to think carefully about the information you put into your profiles on sites like this. It is also a good idea that you check the privacy settings on each site that you use, to make sure you only share personal information with people you trust.

Please also remember that you must take all reasonable precautions to keep your details safe and prevent any unauthorised use of any cards and security details. If any information forms part of your security details, you should make sure that you do not disclose it to anyone else – see the terms and conditions that apply to your account(s) for more detail.

Avoid online fraud and scams
If it's too good to be true, it probably is.

When it comes to protecting yourself and your money on the internet be wary of ridiculous deals.

Criminals may contact you by e-mail, through websites you use, via SMS or even by phone. It pays to be on your guard because they can be quite convincing.

Here are some warning signs:

- Big promises. "You have won the lottery"
- Big threats. "Your account has been hacked"
- A false sense of urgency. "Act now or it'll be too late"
- Unnecessary secrecy. "Don't tell anyone"
- There is no reason for them to contact you. Did you even buy a lottery ticket?
- ''Business opportunities'' that involve holding or receiving money for strangers

If an attachment looks suspicious, don't open it. Don't install software unless it comes from a website you trust. If it doesn't feel right, take your time.

HSBC may send SMS notifications to you upon completion of certain actions, e.g. user registration on HSBC MiVision platform. Please stay alert for the SMS notifications and approach us immediately if you find any irregularity.

Learn to spot fake e-mails and fake websites
Criminals use fake e-mails and fake websites.

They set them up to con people into giving away passwords and bank details. The technical word for this is 'phishing'.

For example, they might send you an e-mail that looks like it comes from us and it might contain a link to a website that looks like this one. When you try to log on, they can steal your password. They could also ask you to make a phone call or reply by e-mail.

They are good at making their e-mails and websites look realistic. But you can often spot the fake ones:

- Strange looking e-mail or web addresses
- Poor design, typos or bad spelling
- They ask you to do something unusual
- A site doesn't display the padlock symbol in the address bar when you log in

Do not access bank websites through hyperlinks embedded in e-mails, Internet search engines or suspicious pop-up windows. Instead, always connect to a bank website by typing the authentic website address into the browser by bookmarking the genuine website for subsequent access. You may also check the authenticity of the website by comparing the URL and the bank's name in its digital certificate or by observing the indicators provided by an extended validation certificate. You should also check that the website address changes from "http://" to https:// and a security icon that looks like a lock or key appears when authentication and encryption is expected.

If in doubt, stop. Don't click on any links. Don't open any attachments. Just forward the e-mail to phishing@hsbc.com and we will investigate it.

Use trusted devices

Always access MiVision through a trusted computer or device. Do not use any public or internet café computers to access MiVision or perform any financial transaction.

Remove file and printer sharing in computers, especially when they are connected to the internet.

Secure your wireless network

A wireless network allows you to connect your computer to the internet without having to use a cable. It typically contains a wireless router, which uses radio signals to transfer data to computers within the network. Some wireless routers come pre-set to very insecure settings to help users connect to them for the first time – but this also means that other people could access your internet account quite easily. For this reason, you should always consult your manual or online guide to find out how to connect more securely through your wireless network – usually by creating a password.

Customer Service and Dispute Resolution

If you have any queries, problems, disputes or claims relating to or arising out of the use of MiVision, please contact our 24-hours HSBC Commercial Credit Card Hotline 1800 227 6227 (Singapore) or (65) 6227 6227 (overseas).

We will attend to any claim or dispute which you may have in respect of or arising out of MiVision as soon as we can. Without affecting either party's right to take immediate steps to seek urgent relief before a Singapore court or the right to seek legal redress, we will immediately investigate any claim/dispute brought to our attention and will strive to respond to you within fourteen (14) working days from the date of receipt of notification. Thereafter, we will consult you in good faith with a view to reaching a quick and amicable resolution of the matter, satisfactory to both parties.