

Fundamentals of Online Security



HSBC 
The world's local bank

Awareness for secure online banking

The growth of the Internet has offered greater flexibility for us all, but it also brings new risks that must be guarded against. At HSBC, we use industry standard security technology and practices, focusing on three key areas – Privacy, Technology and Identification to safeguard your account from any unauthorised access.

Recently e-mail users across the world have been targeted by a global scam - sometimes referred to as "Phishing". Unsolicited e-mails are being sent out to as many email-addresses that the fraudster can obtain. These e-mails typically tempt bank customers to click a link which then takes them to a fairly realistic looking web site that mimics the look of the bank's own website. Customers are then asked to enter information such as their user identification, passwords, credit card numbers and other personal information.

There are steps that YOU can take to protect yourself against fraud. Detailed guidance can be found on our website www.uae.hsbc.com by clicking the security banner on the right-hand navigation bar. In short, the four key areas can be summarized as follows:

1. Protect your information:

HSBC will **never** contact you to request you to provide or confirm your logon details or personal information for Internet Banking, Phone Banking or ATM services. When you receive a suspicious e-mail or phone call claiming to be from HSBC, please inform us immediately on **800 4525** (from within the UAE) or **+971 4 227 4310** (from outside the UAE).

2. Practice safe computing:

Updates and patches

From time to time, vulnerabilities are discovered in software programs. Check your publisher's website for latest patches and fixes.

Anti-virus software

You may already be using anti-virus software, but to be effective, the software should be updated on a regular basis with the latest virus definition files.

Personal firewalls

Install a personal firewall on your computer. A personal firewall is a small program that helps protect your computer and its contents from outsiders on the Internet. When installed, it stops unauthorised traffic to and from your PC.

Shared PCs

Avoid using shared PCs to access Internet Banking.

Emails from Unknown Sources

If you receive an email from an unknown source do not open it. Such mails can contain malicious codes. Simply ignore and delete the mail.

3. Use strong passwords:

Your password is the key to your online account information. Use passwords that are difficult to guess. Do not be tempted to use passwords that can be easily guessed, e.g. children names, pets names, birth dates, telephone numbers. Never write down passwords. Remember to change them regularly.

You should never disclose your Internet Banking login details anywhere, except at your usual Internet banking website which should be accessed through a bookmark or by typing in the URL www.uae.hsbc.com. Never access a link in an email that will take you directly to an Internet Banking logon page.

4. Monitor your accounts regularly:

Check your bank account transaction history often to ensure transactions are legitimate. You should also use the SMS Alert service to be advised of activity on your account. This is now available free of charge for Personal Banking customers.

Our team of specialists is available to serve you and answer any questions on 800 4525 (from within the UAE) or +971 4 227 4310 (from outside the UAE). Enjoy the convenience of safe online banking!