## Security Tips

Be aware of fraudulent or spoof websites that “look alike” AmAccess Corporate (https://corporate.amaccess.com.my) websites. Scam artists are getting sophisticated and are able to have their web site mirror a legitimate business web site and making forgeries of company's sites that look like the actual web site.

Fraudsters usually poses as the legitimate financial institution asking you to provide personal or account-related information via authentic web sites, or e-mail/phone calls with the intention of carrying out Internet theft and fraud

AmBank Group takes the privacy and confidentiality of customers' information seriously and will never request customers to reveal or verify their AmAccess Corporate Password for whatsoever reasons via email or phone.

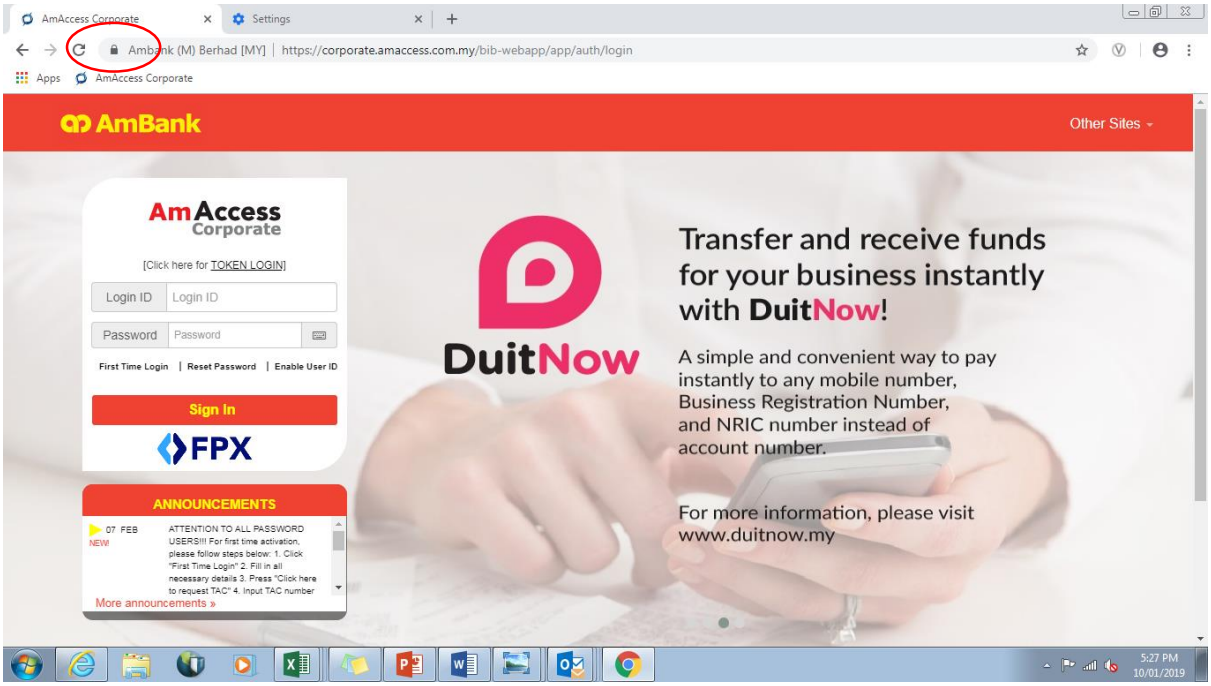
### 1. Steps to Authenticate Website

Here are some ways to protect your ID and Personal Information to minimise risk of ID theft or fraud:

- Always enter a website URL (i.e. https://corporate.amaccess.com.my) at the Browser Address Bar.
- Ensure you are in the correct site by checking the URL (i.e. https://corporate.amaccess.com.my).
- Look for the padlock icon at the left of you browser’s address bar, which indicates that the site is secure. Always “Double-Click” on the padlock to view the Digital Certificate which must show "Issued to: corporate.amaccess.com.my".
- To verify the web page belongs to AmAccess Corporate, follow these steps to view the site certificate and authenticate the validity of the web site:

**Google Chrome Browser**

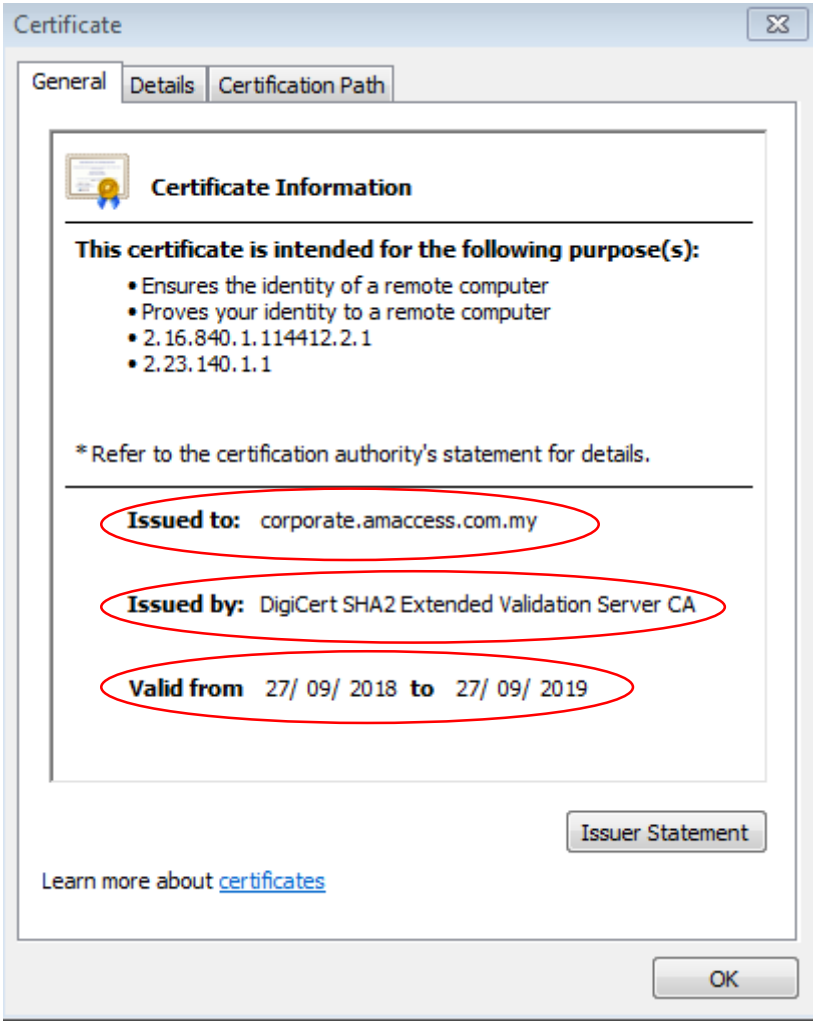
Step 1: Double click the Padlock at the top left of the login page




Step 2a: Verify the digital certificate should state “Issue to: corporate.amaccess.com.my”

Step 2b: Verify the digital certificate should state “Issue By: DigiCert SHA2 Extended Validation Server CA

Step 2c: Verify the digital certificate expiration date is NOT Expired




## 2. Easy Ways Protecting Yourself

- Don't open suspicious e-mail attachments.
- Do not send any information about your account via e-mail.
- Never use the "remember password" function in any website because this information can be easily accessed by hackers.
- If you suspect the website that is not what it purports to be, leave this site. Do not follow any of the instructions it may present to you.
- Do not share your password with friends, relatives or anyone. Your password and PIN are designed to protect the privacy of your banking information. They will only work if you keep them private to yourself.
- Change your password frequently. If you think your AmAccess Corporate password has been compromised, inform your Security Administrator immediately to reset your password. Click here for AmAccess Corporate contact information immediately or email us at amaccesscare@ambankgroup.com for our assistance.
- Do not provide your account details or passwords in response to an e-mail or by phone. Bank will never ask for this information over the phone, email or any electronic means.

- Avoid downloading free programs. These may incorporate ads-ware and hacker-friendly software.

- Always log out of AmAccess Corporate immediately after completing transactions and before visiting other web sites.
- Clear your cache (information stored in your computer memory) each time you log out.
- Install anti-virus software into your PC and update your anti-virus software when new virus information is available.
- Keep your Operating System and browser to latest version or with updated patches.

If you have queries about e-mail from AmBank or are suspicious that someone may be trying to get your PIN or account information under false pretences, Click here for AmAccess Corporate contact information. or email us at amaccesscare@ambankgroup.com

**3. Email Security Tips**

Email has become fast and convenient way to communicate with others, taking a few simple precautions below will help to ensure you are protected.

- Don't trust e-mail headers, which can be forged easily.
- Never fill out a form in an e-mail message. You never know who will get it.
- Be alert for scam email. These may appear to come from a trusted business or friend, but actually are designed to trick you into downloading a virus or jumping to a fraudulent website and disclosing sensitive information.
- Be alert if you receive e-mail or a phone call requesting for information related to your PIN, account number or confidential account details.
- Do not send sensitive personal or financial information via general email. AmBank will never ask you to provide confidential information via general email or phone.
- Be aware of phony "look alike" websites, which are designed to trick consumers and collect their personal information via e-mail.
- Beware the links in an e-mail message. Scam artists are getting sophisticated and are able to have their web site mirror a legitimate business web site and making forgeries of company's sites that look like the real thing.
- Beware when opening attachments sent to you via e-mail. You should know the sender and you should scan using anti-virus utility before opening all attachments.
- Don't trust e-mail messages on the status of your account. Always go directly to a company's web site to access your account information by means of your personal identification and login
- If you receive e-mail asking you to reactivate or update your account for any purpose or to provide personal account information, verify that the web page is secure and that it belongs to AmBank.
- If you have queries about e-mail from AmBank or are suspicious that someone may be trying to get your PIN or account information under false pretences, click here for AmAccess Corporate contact information or email us at amaccesscare@ambankgroup.com

## 4. How do we Safeguard e-AmBiz User

### Authentication

AmAccess Corporate caters for two types of authentication.

- Standard Login ID and Password authentication
- Token Based authentication

The standard Login ID and Password authentication will provide you access to inquiry pages only. To ensure the integrity of your Login ID and Password, the Bank advises you to periodically change your Password and under no circumstances should you reveal your Password to anyone. You should not disclose your Password to the Bank's personnel even if requested to do so. When selecting a Password, do not associate your selected Password with anything personal such as names, birth dates, phone numbers or other familiar words

All transactions can only be performed by Token Based Users.

Token Based Users are authenticated using a Two-Factor Authentication token such as VASCO®, which is activated by a Personal Identification Number (PIN), in addition to your Login ID. Each time you enter your Login ID, a Challenge will be provided. A Response to the Challenge has to be generated from a VASCO® token device that is assigned to your Login ID. The Challenge will be refreshed every 50 seconds to prevent fraudulent use of expired Response.

Attempts to impersonate valid users are locked by the Bank's system after four (4) incorrect sign-on attempts.

### Automatic Log Out

If there is inactivity of eight (8) minutes during your AmAccess Corporate session, the Bank's system will automatically log you out of the system. You are then required to re-login.

To ensure that no unauthorized persons gain access to an active AmAccess Corporate session, the Bank advises you to logout of the system by clicking the Logout button before leaving your workstation.

### Data Security & Confidentiality

The Bank, in its goal to protect the privacy and security of your information, has implemented the following security features:

- Login ID and Password Verification for Static Users
- Two-Factor Authentication for Token Based Users
- Encryption of Passwords and Response
- Firewalls & Intrusion Detection Systems
- Anti-Virus Application
- Internal Policies & Guidelines
- Server side Authentication through Digital Certificates

AmAccess Corporate is designed to give you control over your financial information. The Bank uses the industry standard security measures available through your browser that is known as Transport Layer Security (TLS) encryption. To ensure that your financial information is kept secure, the Bank stores it on a data repository in a secured data centre.

If you believe that someone is attempting to commit fraud on our AmAccess Corporate we appreciate if you contact us immediately. Click here for AmAccess Corporate contact information.