

## IClick Security Tips

### 1. Accessing IClick

- Always access IClick by typing URL [www.imbank.co.rw](http://www.imbank.co.rw) and then going to Online Banking link.
- Never click on a link in an email to take you to a website and enter personal details either in the email or website.
- Whenever possible avoid login to IClick on public computers or cyber cafes. If it is urgent and you find yourself doing it, change your password immediately you get your home computer.
- Note that some Wi-Fi connections are just like cyber cafes. So do not access IClick services from an open unsecure Wi-Fi hotspot. If you do not know the business responsible for maintaining the Wi-Fi hotspot, do not access Internet banking services from it. Access Internet banking services only from a Wi-Fi hotspot maintained by reputable organizations.
- Always use the Virtual Keyboard (onscreen) when log-in to I-click. The system has been designed to enforce this.

### 2. Password Security

- You should always be cautious if you receive unsolicited emails or calls asking you to disclose any personal details or card numbers. This information should be kept secret at all times.
- Never disclose personal information to individuals you do not know.
- I M Bank would never contact you directly to ask you to disclose your PIN or all your password information.
- Never write down or store your passwords in a file on your computer. Don't share your username and password with others. Be cautious of sharing your usernames and passwords with sites, software, or services- especially when your personal information and money is involved.
- Never use online password storage.
- Make your password lengthy. Your password should be 8 characters or more and a combination of alphabets and numbers. Don't use a password that is easy to guess e.g. family name.

### 3. Ensure IClick session is secure

- When undertaking any banking on I-click, check that the session is secure. There are two simple indicators that will tell you if your session is secure.
- The first is the use of <https://> in the URL (address box). Some browsers such as Mozilla Firefox change the colour of the URL window when you are in a secure session.
- The other indicator is the presence of a digital certificate represented by a padlock or key in the bottom right hand corner. If you double click on this icon it should provide you with information about the organization with which you have entered in to a secure session.

### 4. Computer Security

- It is important to use up-to-date Anti-virus software. If your computer uses Microsoft Windows operating system, it is important to keep it updated via the Windows Update feature, equally if you use another PC operating system or have an Apple Mac you should check regularly for updates. You should be vigilant if you use Internet cafes or a computer that is not your own and over which you have no control.

- In addition to being protected by using up-to-date antivirus software you should also regularly use software to remove Spyware from your computer, as these programs record information about your Internet use and transmit it without your permission. In some circumstances this can compromise your PC security.
- Avoid downloading files from unknown sources. Malicious software (also known as 'malware') and computer viruses can be hidden in email attachments and other files downloaded from the Internet. Before you download anything, verify you trust the source. Even when you receive files from friends and family, make sure your anti-virus software scans the files before opening them.