

Virtual Keyboard and Password creation

Fraud Newsletter
#1 - Q3 2010
Virtual Banking & Cards Services

Some people will find it tedious and troublesome while others embrace the technology in order to keep up with the latest trends. Whichever it is, we at the Virtual Banking Unit will brief you on the reason behind the introduction of Virtual keyboard for i-Muamalat.

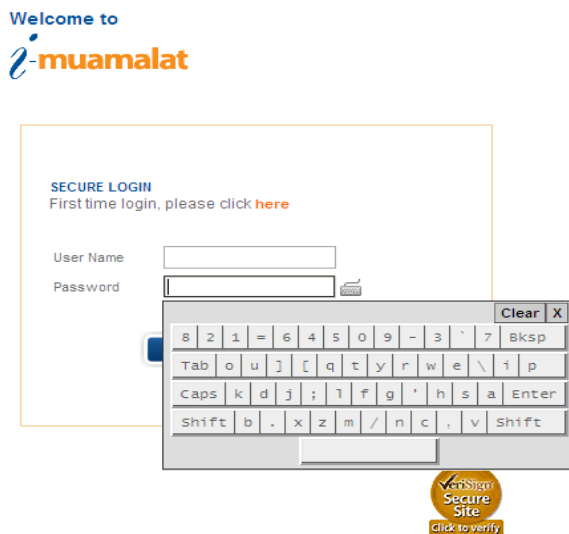


Figure 1 : i-Muamalat Virtual Keyboard

Conventional vs Virtual Keyboard

Most malwares developed for financial gain are often tailored to the targeted bank's internet banking processes. The way the malware operates is normally determined by the bank's system defenses.

Banks normally require their customers to log-in using the conventional keyboard which is attached to the customers' computers. As such, it is rather

vulnerable to spyware in the form of a key-logger malware. A key-logger malware can be secretly deployed as it is capable to record the location and sound of the key that is being pressed. This will enable the crooks to gather valuable information on the username and password.

The introduction of a virtual keyboard which scrambles the location of the keys on the keyboard is one way of covering the vulnerability of a conventional normal keyboard. It secures the customer from threat of theft of username and password as there keys are scrambled and there will be no sound of key tapped to be recorded. This feature further nullifies a mouse-gestures program effect that will record your mouse movement as the location of the key will never be the same on every session.

Too many passwords?¹

How many passwords do you have? Every system, of course, requires you to create a password as identification to access. And if the system is serious about security, it may even set certain rules. For example, it may insist that your password is at least eight characters and/or must contain non-alpha-numeric characters, or must use at least one uppercase letter, etc.

The problem is, with so many accounts, how do you remember a unique password for each one? We all know that it's unwise to use the same password for them all. And it's not much better simply to recycle them - e.g. 'mazlan1', 'mazlan2', 'mazlan3', etc.

There is a solution. Instead of trying to remember individual passwords, start with a fixed component and then apply a simple scrambling formula. Here's an example: start with the name of the online resource, let's say 'muamalat'. Then apply your formula: e.g.

1. **Capitalize the second character.**
2. **Add a chosen number after the second character.**
3. **Add a chosen character to the end.**

This would give you a password of 'mU1amalat#'.

"i-Muamalat requires the usage of, small and big caps, number and character in the password created"

Using this method gives you a unique password for each account, but all you have to remember is the same three steps each time.

Be creative in designing
your scrambling
formula, example shown
here just as guidance

ⁱ *David Emm, Kaspersky Lab Expert, March 03, 14:06 GMT "Too many passwords?"*
http://www.securelist.com/en/blog/208188024/Too_many_passwords
Accessed, 23 September 2010.