

# Re: [Full-disclosure] Defeating Citi-Bank Virtual Keyboard Protection

**Source:** <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-08/0189.html>

---

**From:** Bart Lansing (*bart.lansing\_at\_hushmail.com*)

**Date:** 08/08/05

Date: Mon, 8 Aug 2005 07:37:57 -0700

To: <adityad2005@users.sourceforge.net>, <lyal.collins@key2it.com.au>

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

On Sat, 06 Aug 2005 13:40:40 -0700 root

<lyal.collins@key2it.com.au> wrote:

>Aditya Deshmukh wrote:

>

>>The only most secure protection is a one time password with a

>challenge /

>>response scheme. Most of the banks in europe already do this.

>>

>>They give out a calculator like device to the customers and when

>u want to

>>login you are presented with a challenge that you punch into you

>device

>>which spits a response that you enter that into the form....

>>

>>Costly for the bank but very effective security for the customer

>and bank in

>>terms of gain in security and decrease in losses due to fraud

>....

>>

>>

>>- Aditya

>>

>>

>>

>>

>>

>\_\_\_\_\_

>>Delivered using the Free Personal Edition of Mailtraq

>(www.mailtraq.com)

>>

>>\_\_\_\_\_

>>Full-Disclosure - We believe in it.

Full-Disclosure: Re: [Full-disclosure] Defeating Citi-Bank Virtual Keyboard Protection

>>Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>  
>>Hosted and sponsored by Secunia – <http://secunia.com/>  
>>  
>>  
>>  
>>  
>Respectfully, I disagree.  
>Although I never attended, this year's IT Underground conference  
>in  
>poland promised a hand on session breaking OTP tokens. As  
>Schneier  
>says, OT token device merely force a tactical shift by the  
>attacker, not  
>a permanent fix.  
>The credit card industry's 'fixes' have only been effective for  
>weeks to  
>months over the past decade, so I don't consider OTPs will make  
>much  
>difference relative to the cost in the mid-long term.  
>  
>Lyal  
>  
\_\_\_\_\_  
>Full-Disclosure – We believe in it.  
>Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>  
>Hosted and sponsored by Secunia – <http://secunia.com/>

There is no permanent security fix...for anything. Every system that exists today will be vulnerable tomorrow, and every measure to secure them that exists today will be thought to be old-school and simplistic in a decade (probably much sooner, I'm allowing wiggle room).

Starting from that point, with all due respect to Mr. Schneier as paraphrased by Lyal, OTP tokens/two factor in general, while not perfect, are light years beyond "Hey, type your password into this webform for us, and we'll pull up your bank account." in terms of doing what matters...securing the customer. Today. Not some nebulous tomorrow where we all rest our finger on the passive DNA scanner built into whatever user interface device we are using at the time (and that will no doubt be vulnerable to man in the middle attacks using DNA Dictionaries).

The Game is not "Can you make it permanently secure?"...you can't. The Game is "Given the resources we have today (technical, fiscal, human, physical, etc), how secure can we make systems that are at risk and are appropriate to take such measures for?". Planning for tomorrow while offering critiques of today's solutions is great...and it will make tomorrow a better/safer place for our data. But right now we have to make do with what's both available and realistically achievable. OTPs are both.

Full-Disclosure: Re: [Full-disclosure] Defeating Citi-Bank Virtual Keyboard Protection

-----BEGIN PGP SIGNATURE-----

Note: This signature can be verified at <https://www.hushtools.com/verify>

Version: Hush 2.4

wkYEARECAAYFAkL3bkQACgkQfw4CJpLBxONDMwCdFkkukBzPPoGzY2RFv5TXjYNYFGEA  
oIPFeDwa/Eu/gqyEHh+DF+SUdUU5  
=rOmT

-----END PGP SIGNATURE-----

Concerned about your privacy? Follow this link to get  
secure FREE email: <http://www.hushmail.com/?l=2>

Free, ultra-private instant messaging with Hush Messenger  
<http://www.hushmail.com/services-messenger?l=434>

Promote security and make money with the Hushmail Affiliate Program:  
<http://www.hushmail.com/about-affiliate?l=427>

---

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>