Title	Bypassing 2 Factor authentication on DropBox
Author	Zouheir Abdallah, CISA
Date	June 10 th , 2013
Contact details	zabdallah@qcert.org
	zabdallah@ict.gov.qa
Disclaimer	This document is intended only as a demonstration for educational or
	testing purposes. It is not intended for any unauthorized or illicit purpose.

Prerequisite:

• Attacker should already know the username and password of the victim. (Key-logger, easy to guess password, cross-site shared password, etc..)

Steps:

1. Create a new fake account similar to the target's account and append a dot (.) anywhere in the email address. The email address can be a bogus one, because DropBox does not verify the authenticity of the email addresses used.

Sign in zuz.85@hotmail.com Remember me Sign in Forgot your password?	Vour stuff, anywhere test test zuz85@hotmail.com I agree to Dropbox Terms Sign up or Sign in
Genuine Account	Creation of Attacker Account

2. Enable 2-factor authentication for the fake account, and save the emergency code generated at the end of the process. This will be the attack vector.

Enable two-step verification Your security codes will be generated by your authenticator app	×
As a last resort, you can also use this emergency backup code to disable two-step verification and access your account. veh4 gbtk 75av nhsm Write this down and keep it safe	
Back Enable two-step verification	

3. Logout of the fake account, and login using the genuine account using the real credentials.

	\times
Sign in	
zuz.85@hotmail.com	
•••••	
Remember me	
Sign in	
Forgot your password?	
gning in using the genuine account zuz.85@hotmail.com	

4. When instructed to enter the OTP code, choose "I Lost My Phone". You will be prompted to use the "Emergency Code".

Enter securit	y code
Ve sent a security code to y nding in 3473.	our phone number
6-digit code	Submit code
Trust this computer 🕕	
idn't receive one?	
ost my phone	

5. Use the emergency code generated for the fake account to disable 2-Factor authentication on the genuine account.

disable two-step verification by entering you	
emergency backup code.	ur
veh4gbtk75avnhsm	
Submit code	
I need more help	

6. Success, 2-factor authentication for the genuine account is disabled using the emergency code of the fake account.

