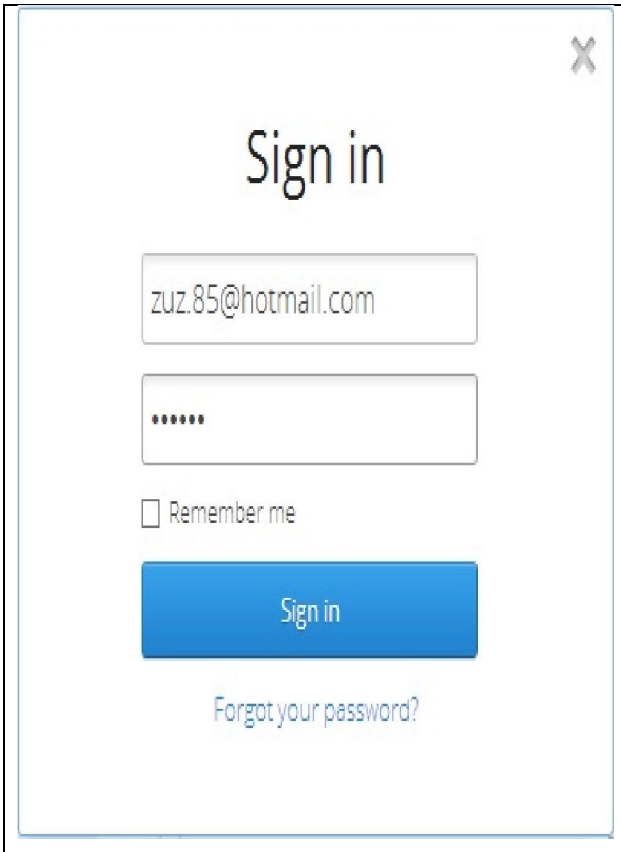
Title	Bypassing 2 Factor authentication on DropBox
Author	Zouheir Abdallah, CISA
Date	June 10th, 2013
Contact details	zabdallah@qcert.org zabdallah@ict.gov.qa
Disclaimer	This document is intended only as a demonstration for educational or testing purposes. It is not intended for any unauthorized or illicit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

Prerequisite:

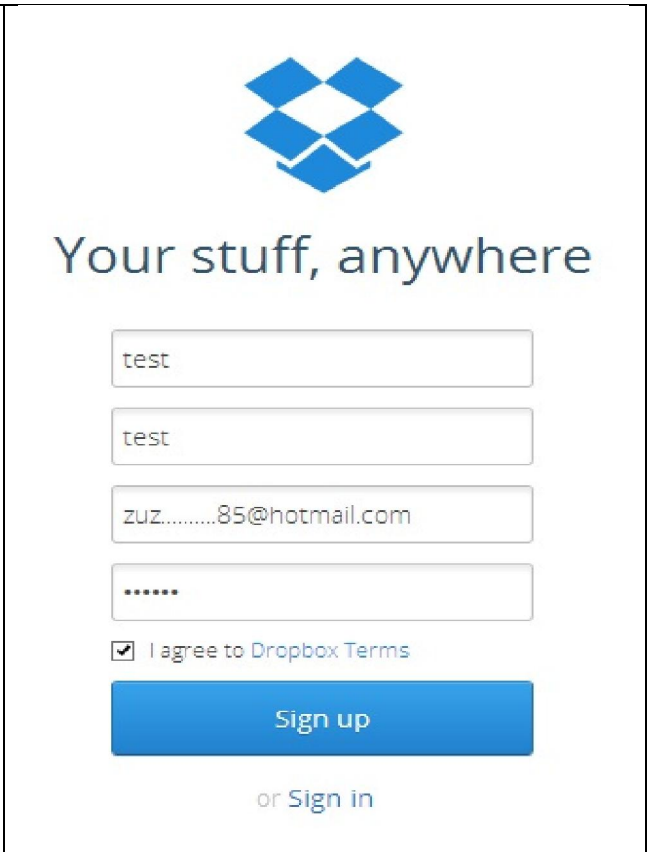
- Attacker should already know the username and password of the victim. (Key-logger, easy to guess password, cross-site shared password, etc..)

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.

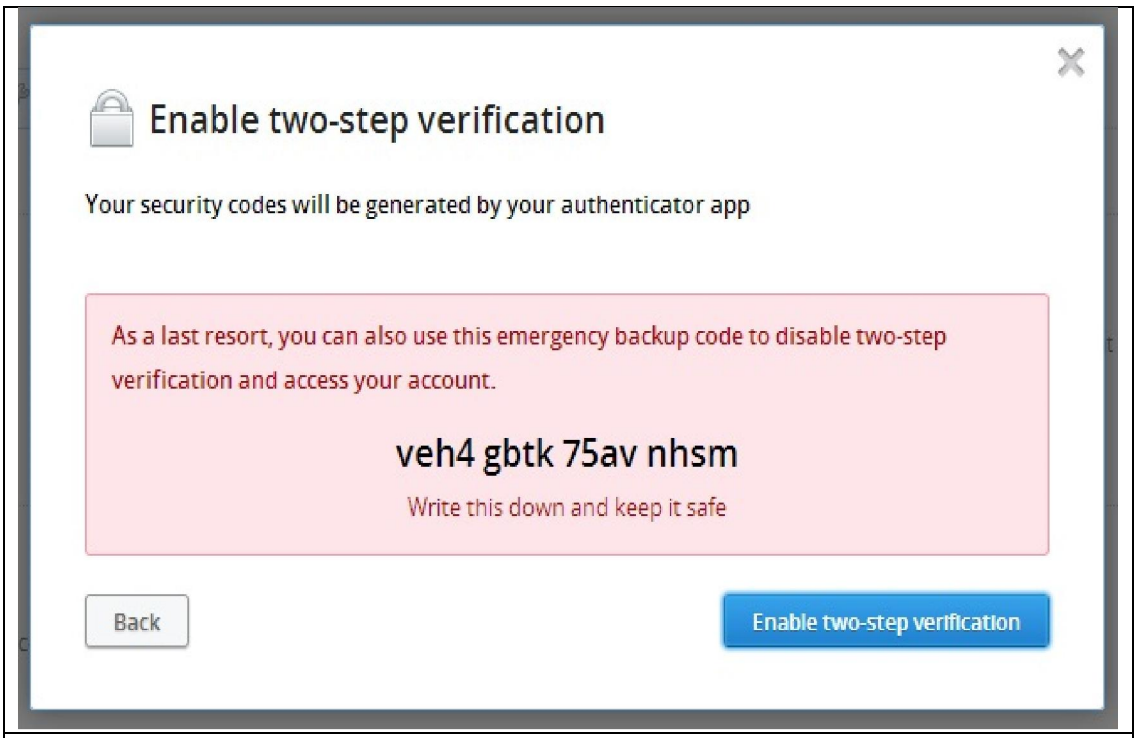


Genuine Account



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.



Emergency Code for zuz…….85@hotmail.com

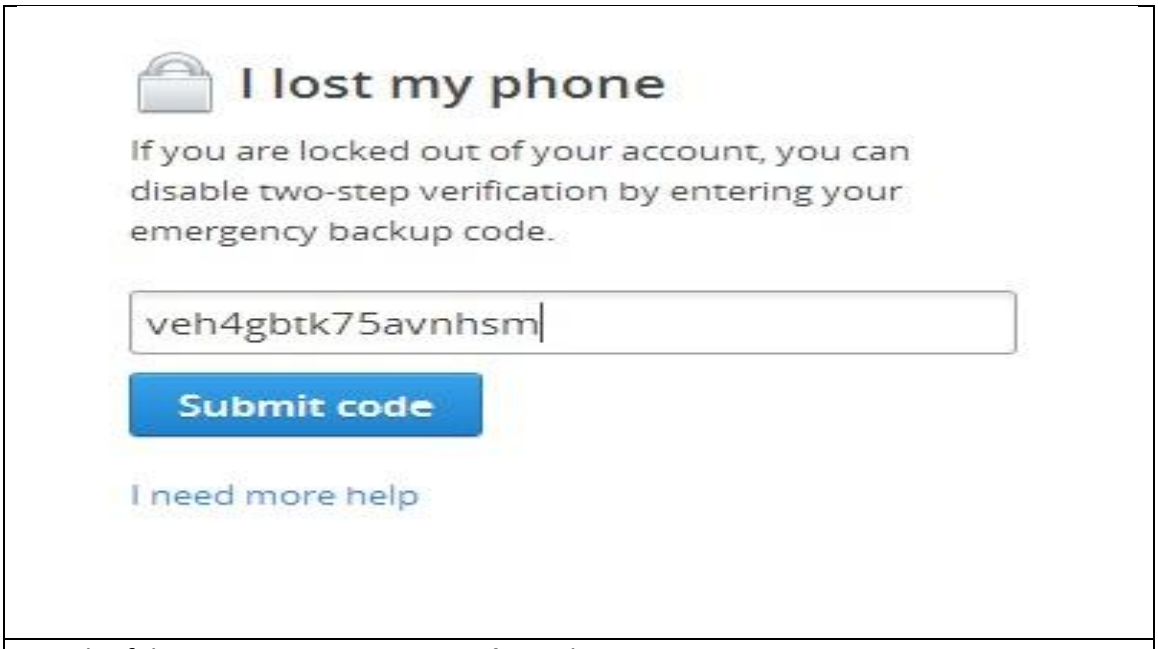
3. Logout of the fake account, and login using the genuine account using the real credentials.

Signing 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”.

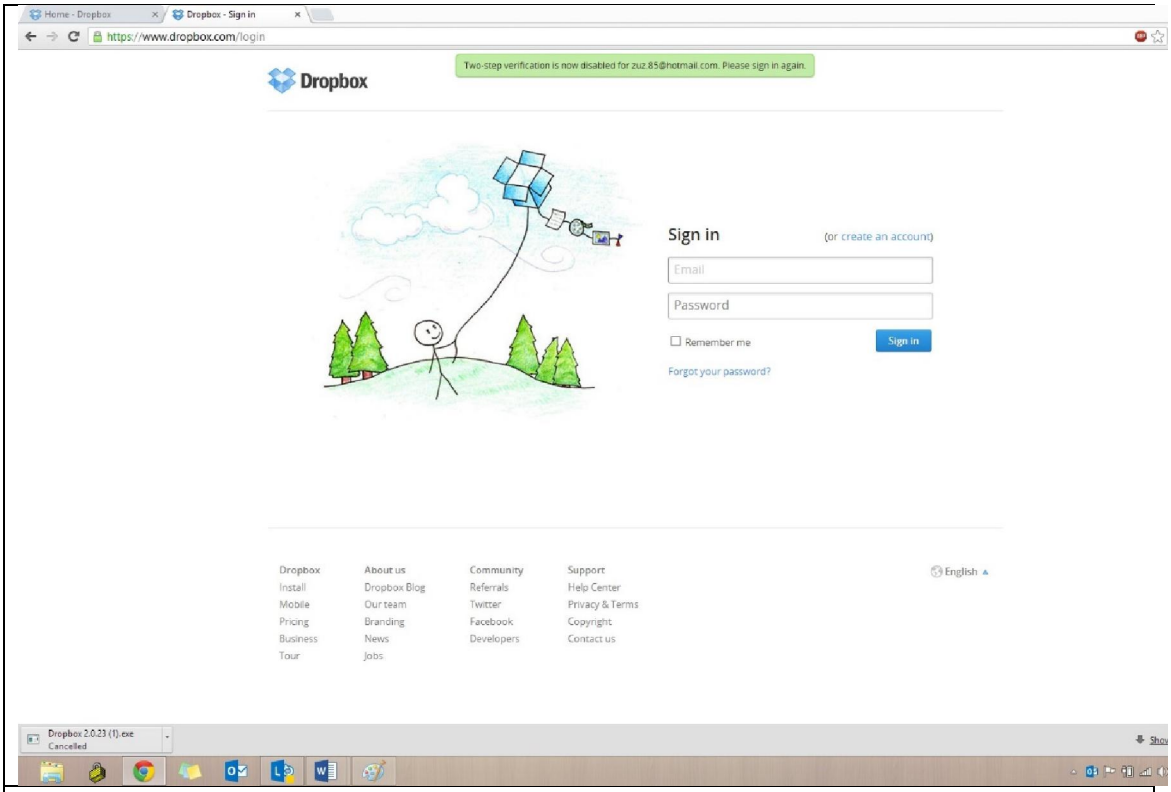
After logging in using the genuine account, click on **“I lost my phone”**

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



Use the fake account **emergency code** as the genuine account.

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



Exploited, notice the green overlay at the top “Two step verification is now disabled for zuz.85@hotmail.com. Please sign in again.