

You and Your Passwords



Why Passwords?

Millions of LinkedIn passwords reportedly leaked online

A hacker says he's posted 6.5 million passwords -- hot on the heels of security res issues with LinkedIn's iOS app.

Dropbox sends password change notification to some users

Zappos Passwords Hacked: What You Need To Do Right Now

In an email sent out last night, online shoe and clothing store Zappos let customers know that its database of passwords and usernames was hacked. Your credit card information is safe and all Zappos passwords have been reset, but if you use the same password and email elsewhere, a **password audit** is in order.

by Michael Ross

Aug 1st 2012 at 12:30AM

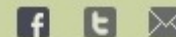
BY THORIN KLOSOWSKI

JAN 16, 2012 8:30 AM

Share

GET OUR TOP STORIES

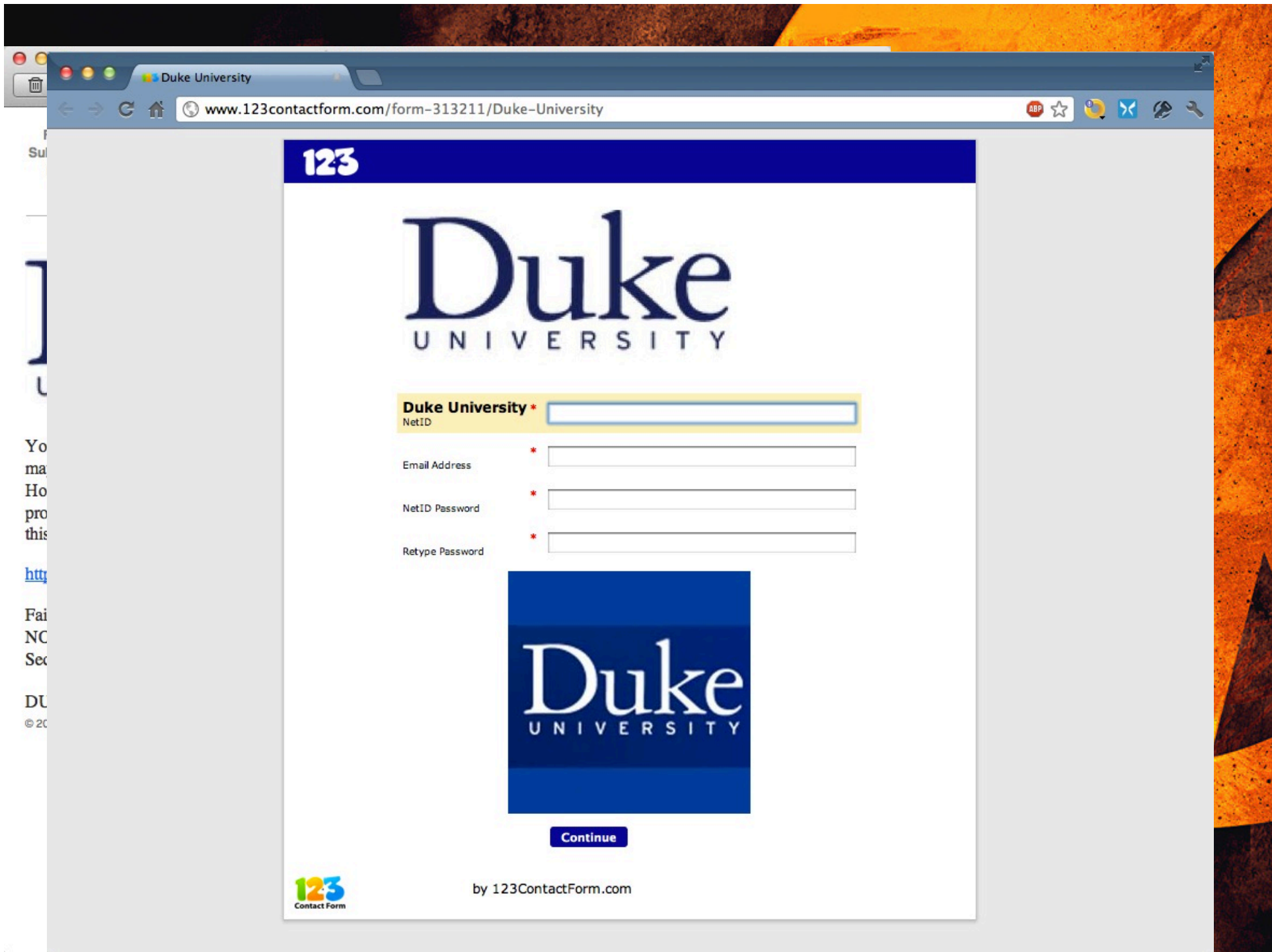
FOLLOW LIFEHACKER



Internet services. This is a word on multiple services, which

you can create a new one [here](#).

We haven't detected any suspicious activity in your Dropbox, but we're [proactively taking steps to keep users safe](#).



Threat - Cracking Passwords



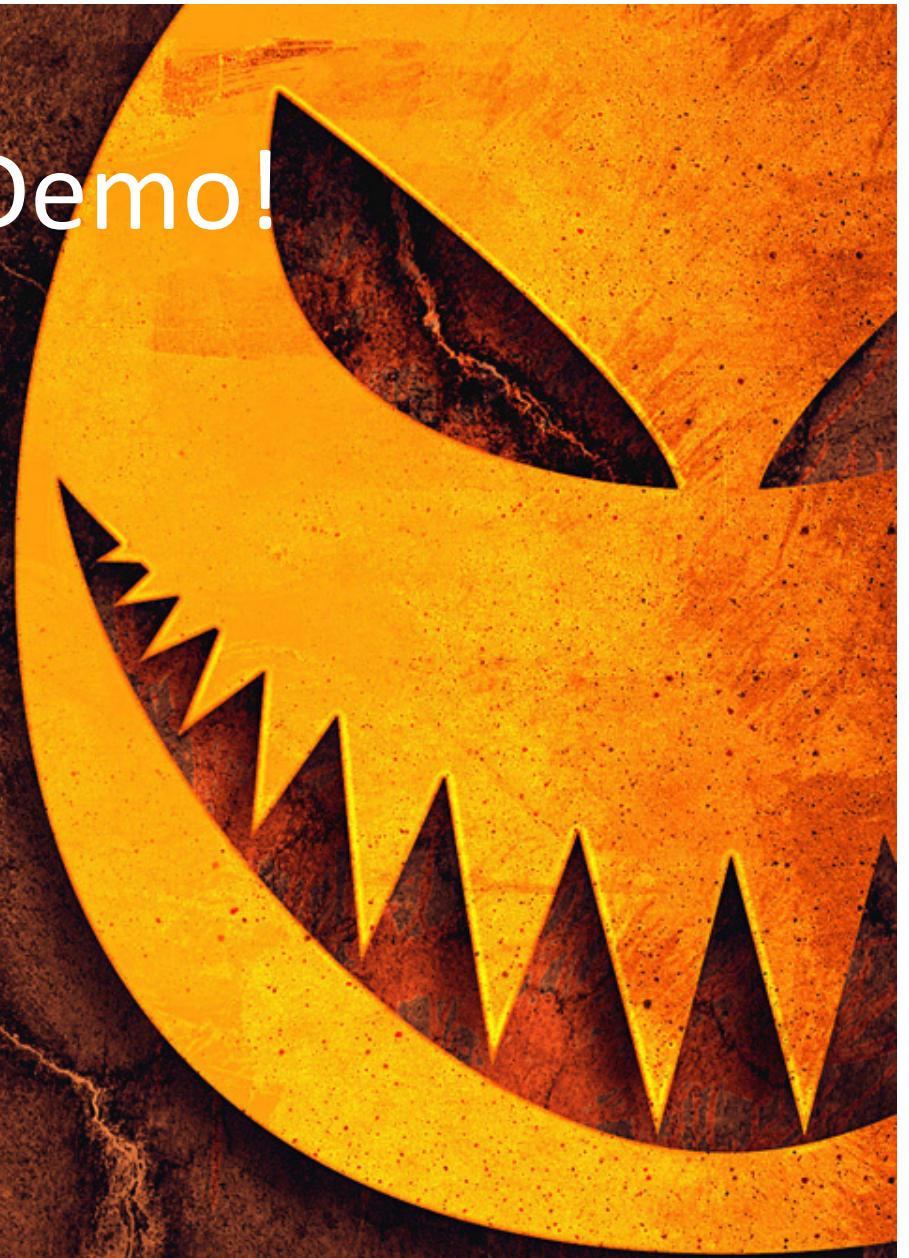
Password Type	Using the CPU	Using the GPU
6 char (no spec chars)	1 hour 30 sec	4 seconds
7 char (no spec chars)	4 days	17 minutes 30 seconds
7 char (spec chars)	75 days	7 hours
9 char (spec chars)	43 years	48 days

Methods to Compromise Accounts/Passwords

Password Attack	Defense						
	Longer passwords (passphrases)	Regular Password changes	Account lockouts	Multi-factor	Education	Network encryption	Host-based security
Password Cracking <ul style="list-style-type: none"> • Dictionary Attack • Brute Force • Rainbow Tables • GPU Cracking 	✓	✓	✓	✓			
Password Sharing				✓	✓		
Phishing/Social Engineering				✓	✓		
Man-in-the-Middle Attack				✓	✓	✓	
Network Sniffing	✓	✓	✓	✓		✓	
Keylogger				✓*			✓

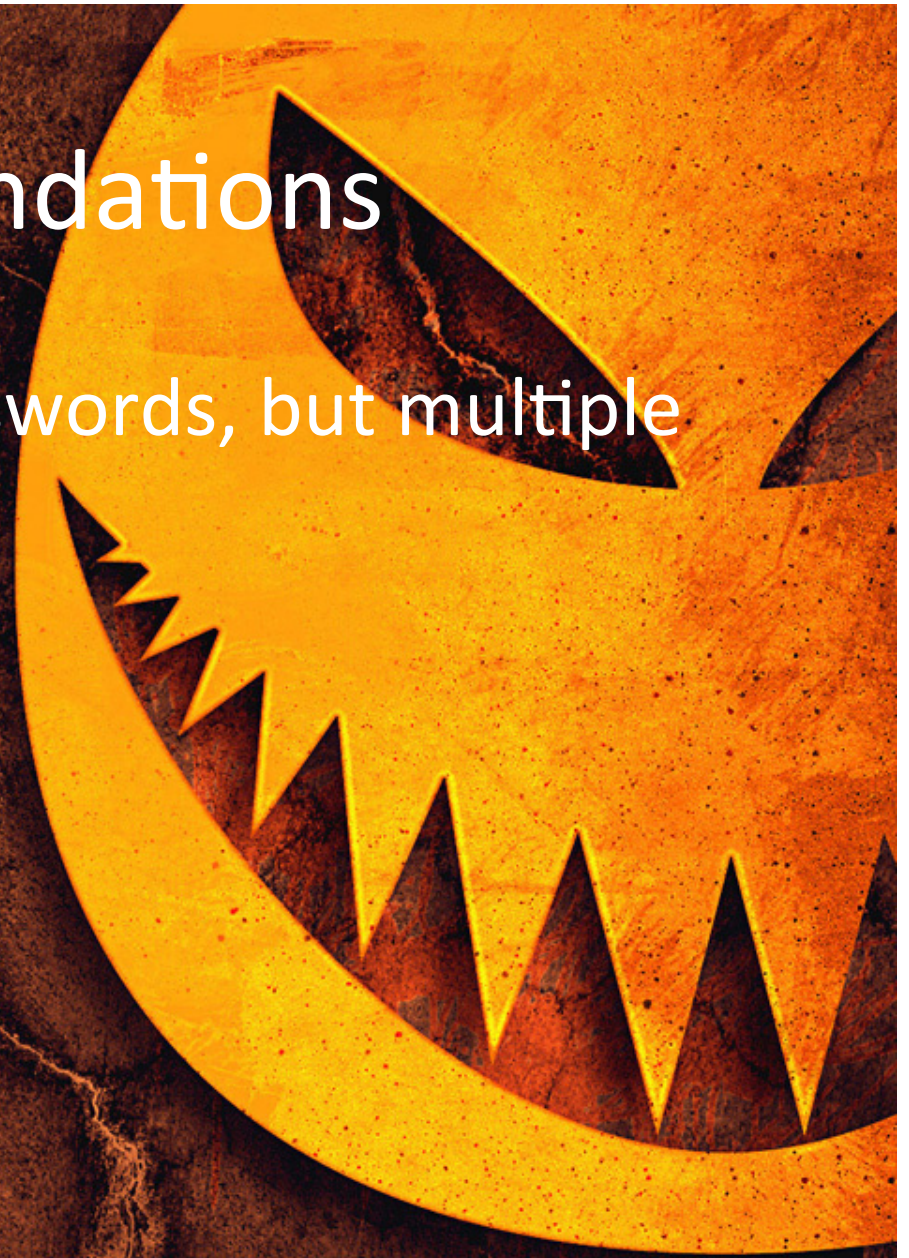
*(unless digital cert)

Look, a Demo!



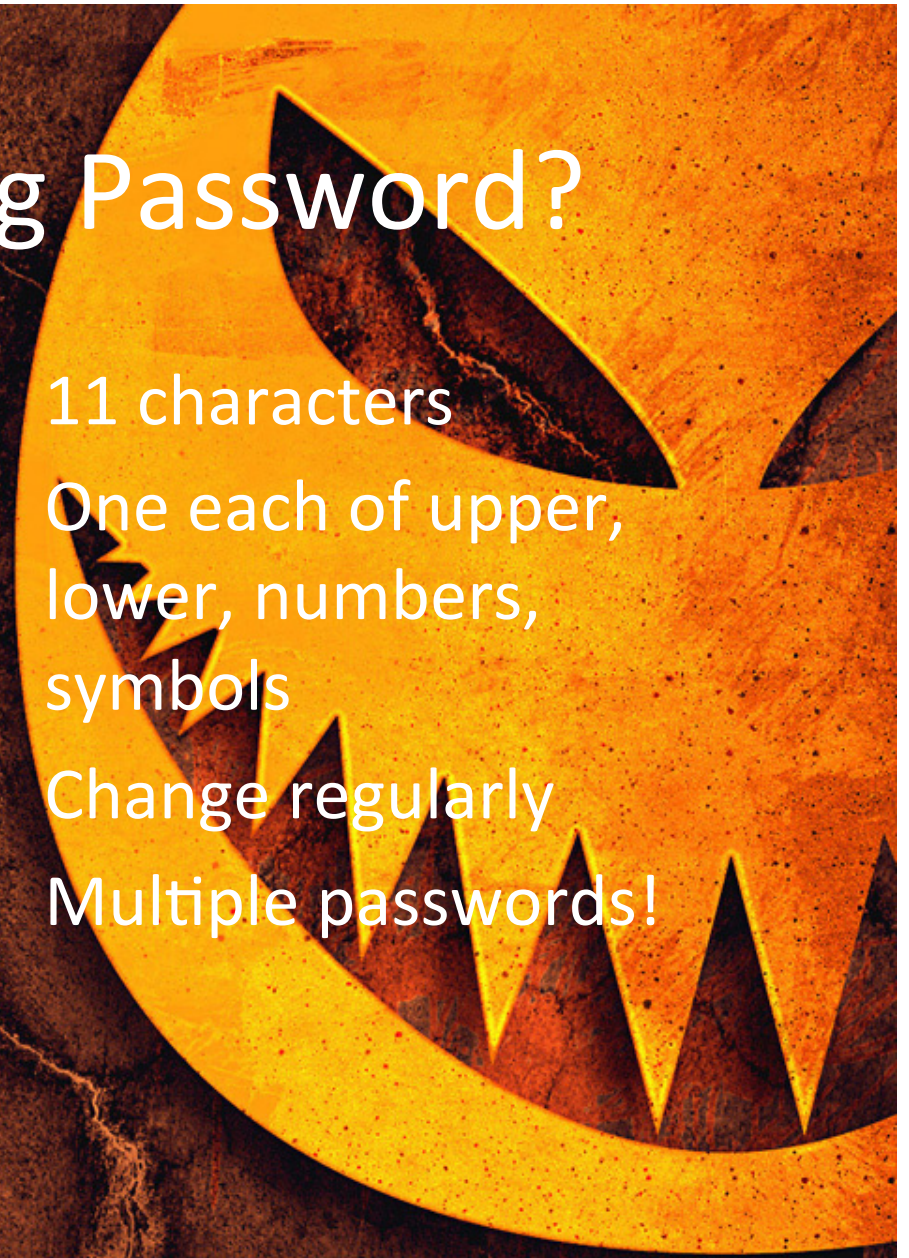
Recommendations

- Not just one strong passwords, but multiple strong passwords
- Password Escrow
- Multifactor



What's a Strong Password?

- 8 characters
- Mix of upper, lower, numbers, symbols
- 11 characters
- One each of upper, lower, numbers, symbols
- Change regularly
- Multiple passwords!



Password Escrow – 1Password

The screenshot displays the 1Password application window. The left sidebar shows the 'VAULT' section with categories like Logins, Accounts, Identities, Secure Notes, Software, and Wallet. Below these are 'FOLDERS' (All, sans), 'TAGS', and 'SYNC' (Generated Passwords, Trash). The main pane shows a search results table for 'duke'.

Title	Location	Modified Date
twitter.com-Duke	twitter.com	Nov 2, 2011 8:46 AM
dukehealth.org	dukehealth.org	Apr 24, 2012 7:37 AM
Mail Gateways	duke.edu	Feb 13, 2012 12:50 PM
google.com	google.com	Aug 16, 2012 11:44 AM
tip.duke.edu	duke.edu	Feb 13, 2012 8:29 AM
Tigris	duke.edu	May 5, 2011 9:54 PM
DSView	duke.edu	Jun 21, 2011 5:26 PM
Sophos Dashboard	duke.edu	Feb 13, 2012 12:53 PM
box.com (Duke)	box.com	Feb 17, 2012 12:37 PM
DNEC	duke.edu	Oct 20, 2011 9:32 AM
Duke	duke.edu	Oct 5, 2012 8:41 AM

Below the table, the details for 'dukeuniversity.webex.com' are shown. The URL is <https://dukeuniversity.webex.com/mw0306ld/mywebex/login/login.do>. The Username is 'rb186' and the Password is masked with dots. A strength indicator shows 'High (Master Password)'. Below this, the 'All Fields' section lists: oldPassword, newPassword, newPassword2, btnLogon (Submit), and Username (rb186). The 'Password History' section shows a single entry: Sep 25, 2012 10:56:36 AM.

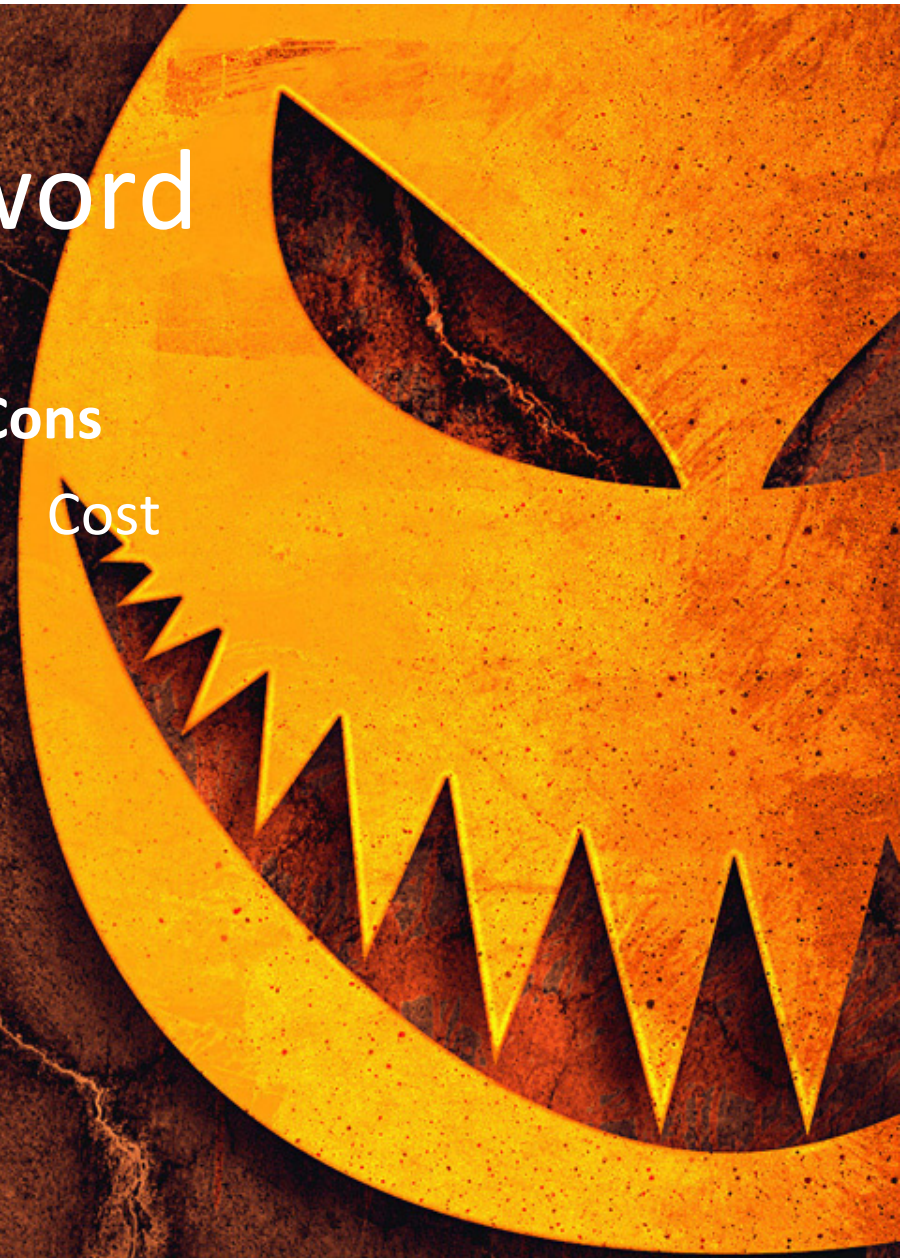
1Password

Pros

- Multiplatform and multibrowser
- Password generator
- Password history
- Sync with mobile devices

Cons

- Cost



Password Escrow – LastPass

LOGOFF: rblever@gmail.com

Generate Password

gFwdT7YE

Password Length

☐ Pronounceable

☒ A-Z ☒ a-z ☒ 0-9 ☐ Special

Minimum Digit Count

☐ Avoid Ambiguous Characters

☒ Require Every Character Type

Sites Groups FormFill Generate Advanced

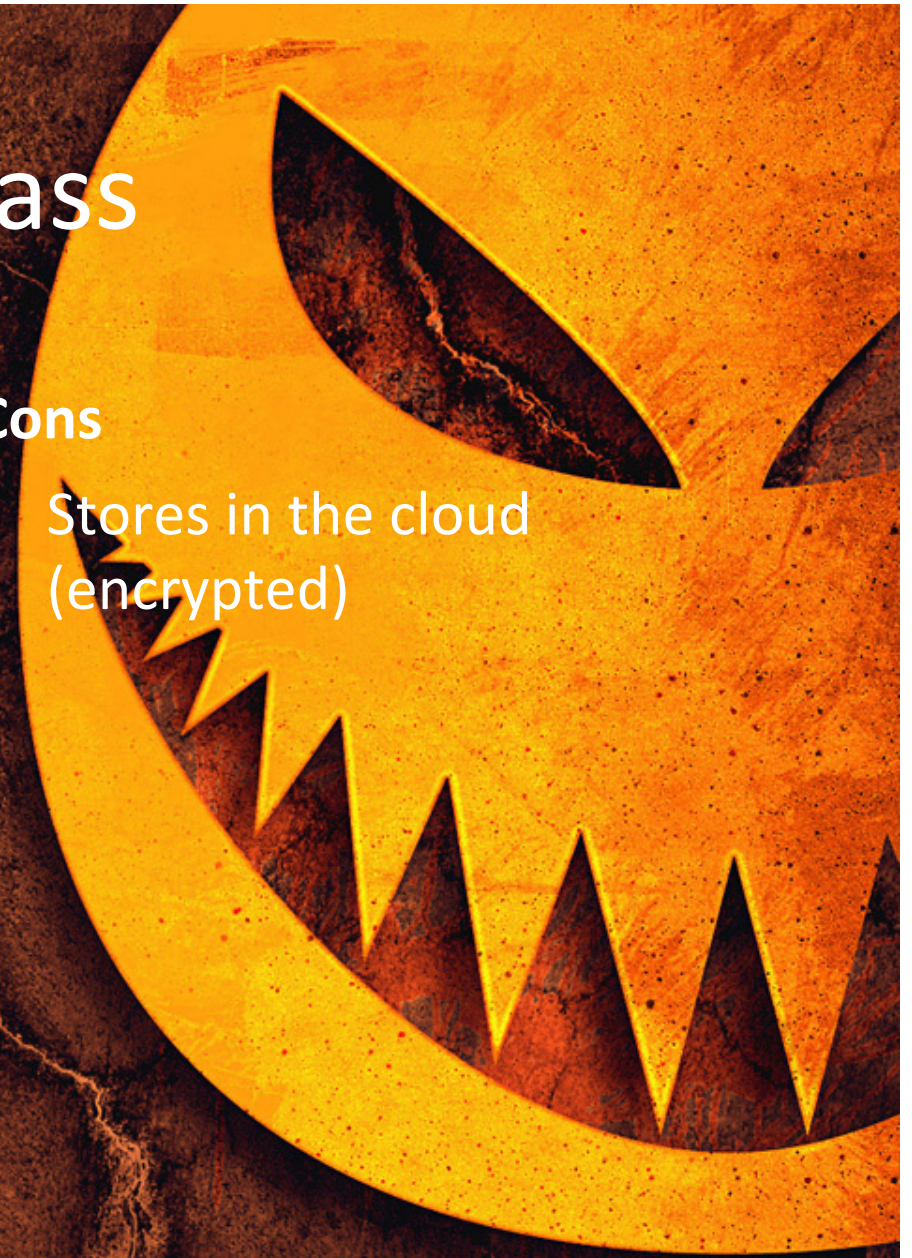
LastPass

Pros

- Free and Pay versions
- Multiplatform and multibrowser
- Password generator
- Sync with mobile devices

Cons

- Stores in the cloud (encrypted)



Password Escrow – Keepass



KeepPass

Pros

- Free
- Multiplatform and multibrowser
- Password generator
- Sync with mobile devices

Cons

- May require different installations for different OS's
- May require some advanced work to sync with mobile devices

Multifactor

The image shows a screenshot of the Duke University sign-in page. The background is a dark, textured brown on the left and a large, stylized orange and yellow sun or moon on the right. The sign-in form is a white rectangular box with a blue header bar. The header bar contains the word "Duke" in white serif font and "SIGN IN" in yellow sans-serif font. Below the header, the form has a "SIGN IN" link, input fields for "NetID:" (containing "rb186") and "Password:" (masked with dots), a "Duo Second Factor" section with a "Please accept the Duo Push request on your phone." message and an "Enter" button, a "Forgot your password?" link, and a note about the URL. At the bottom, there are links for assistance: "http://oit.duke.edu/help" and "http://dhts.duke.edu".

Duke | SIGN IN

► SIGN IN

NetID:

Password:

— **Duo Second Factor**
Please accept the Duo Push request on your phone.

[Forgot your password?](#)

You are on the correct Duke sign-in page if the URL above begins with *https://shib.oit.duke.edu/*.

For assistance, please visit <http://oit.duke.edu/help> or <http://dhts.duke.edu>.