

Improving Password Management

Information Security Office

Laura Raderman, Policy and Compliance Coordinator, ISO

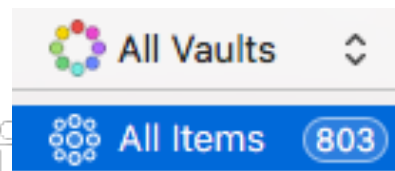
Ole Villadsen, Research Liaison, Cybersecurity, UL

Password Management

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office

- How many passwords do you have?



- Are they all different?
 - How different?
 - Summer2016 vs Autumn2016?

- Picking a password can be difficult
 - Multiple sites have different rules – what may be acceptable on one site is unacceptable on another
 - Biggest culprit: sites that don't accept special characters
 - Very strong passwords generally aren't very memorable
 - `buz%vG9X#paC3s`

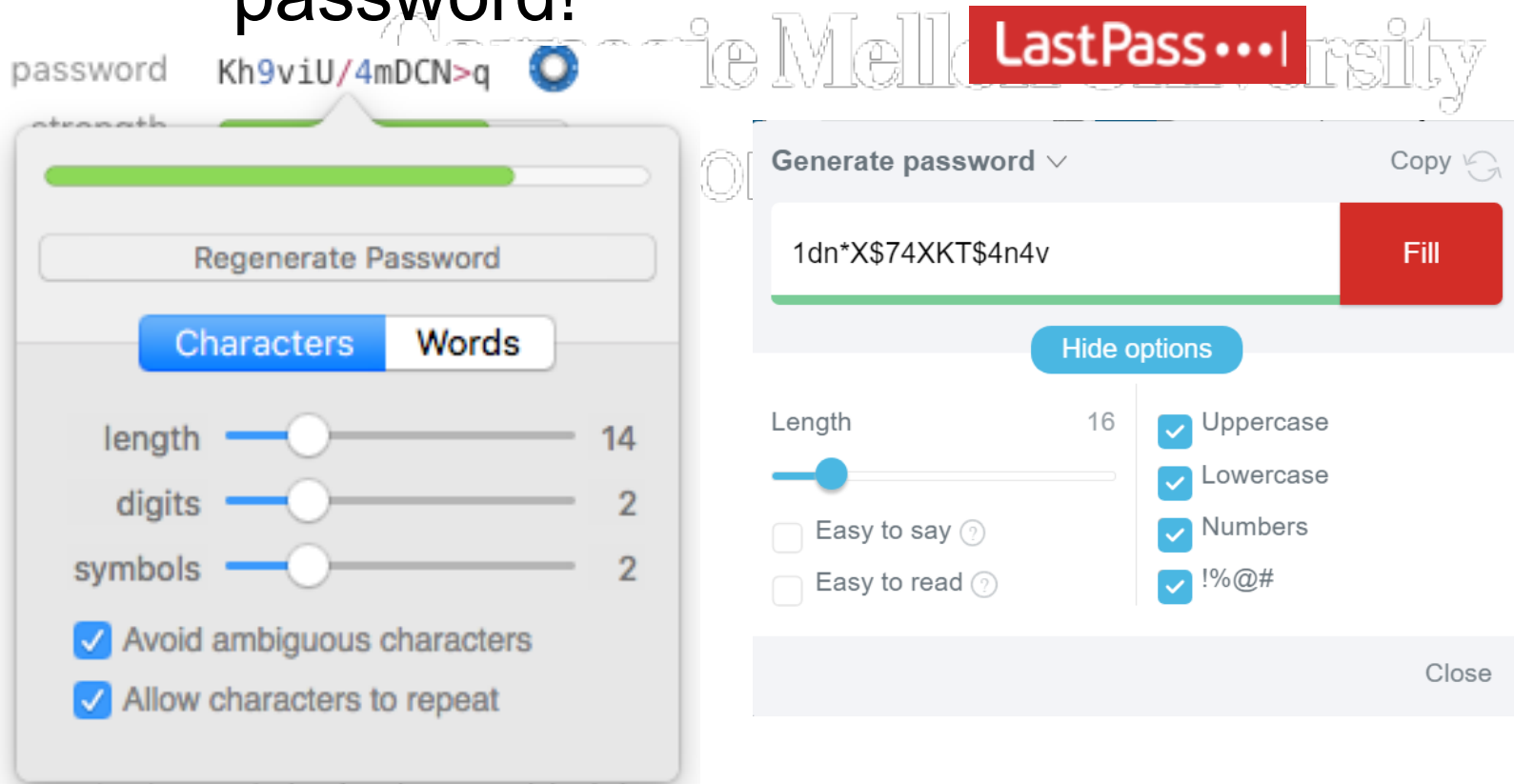


Password Managers!

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office

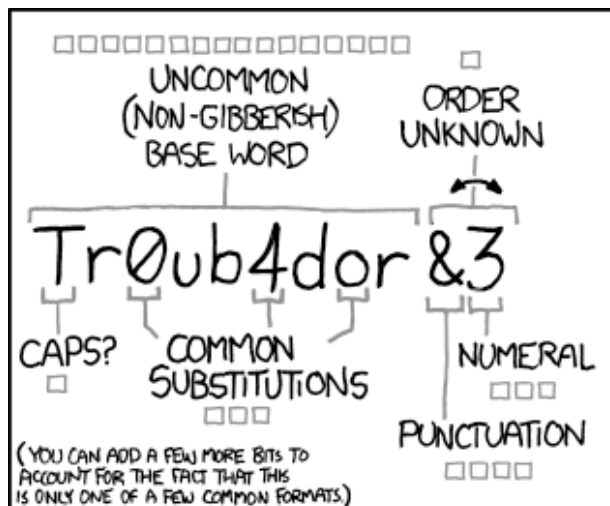
- Generate and store your passwords
 - You don't even have to think up a new password!



- Passwords are protected by a “master” password.
 - This is the password you will have to remember (you can still have the manager generate it for you if you want)
- The master password is used to encrypt all of your other passwords
 - Most are using AES256 with PBKDF2 (Password Based Key Derivation Function 2)

Master Passwords

- Select a very strong master password
 - All managers support changing it should you want/need to
- New NIST Recommendations
 - At least 8 characters
 - Not in a dictionary
 - Not in previously compromised account databases
- ISO's Recommendation
 - Long (16+ character) phrase



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

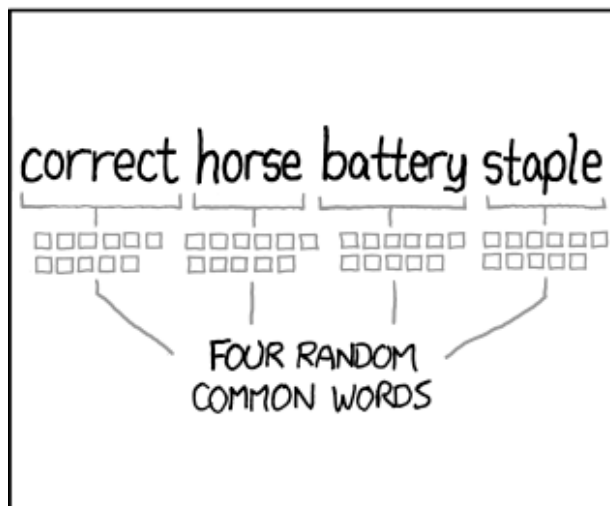
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS:
EASY

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER:
HARD



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS:
HARD

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

**DO NOT FORGET
YOUR MASTER
PASSWORD!**

Storage Options

- Offline storage
- Online storage
- Both are secure with ISO recommendations, but your risk tolerance may differ!
 - If you don't sync/store online – BACKUP your file(s)!

Specific ISO Recommendations

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office

- 1Password
- KeePass
- LastPass
- ISO evaluated design at a high level for security of passwords
 - It's OK to store your Andrew password in these!
- CMU **DOES NOT** support these

1Password

- <https://1password.com>
- Both an online and a desktop/mobile application
 - Both are secure!
- Not free
 - \$64.99 for the “standalone” version (upgrades have been less in the past – usually ~\$35 every 3-4 years)
 - \$2.99/mth billed annually (\$35.88/yr) for online

1Password (cont)

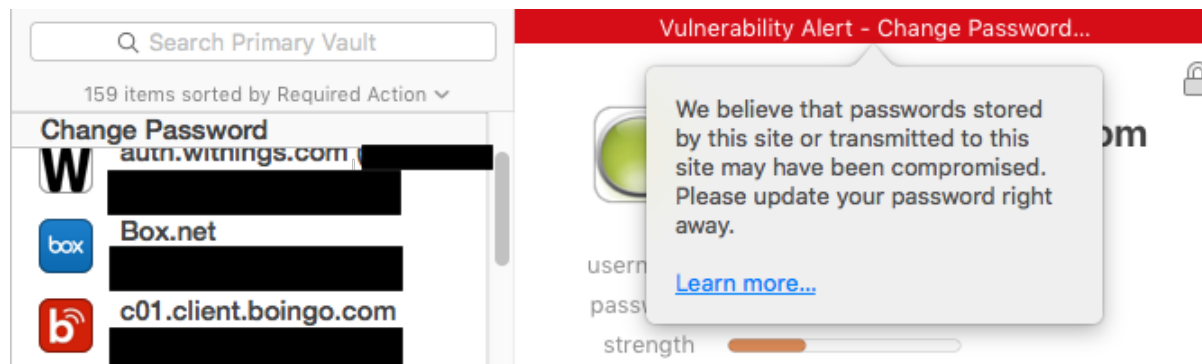
- Standalone version offers syncing through Dropbox, iCloud, file folder (including file shares)
 - Syncing is not required!
- Standalone version is not compatible with Linux
- Online version supports offline caching (via applications), but is primarily online
- Browser integration with all major browsers

1Password (cont)

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office

- Watchtower/ Security Audit
 - Lets you know about password breaches – like Yahoo's or compromised private server keys
 - Points out weak or duplicate passwords



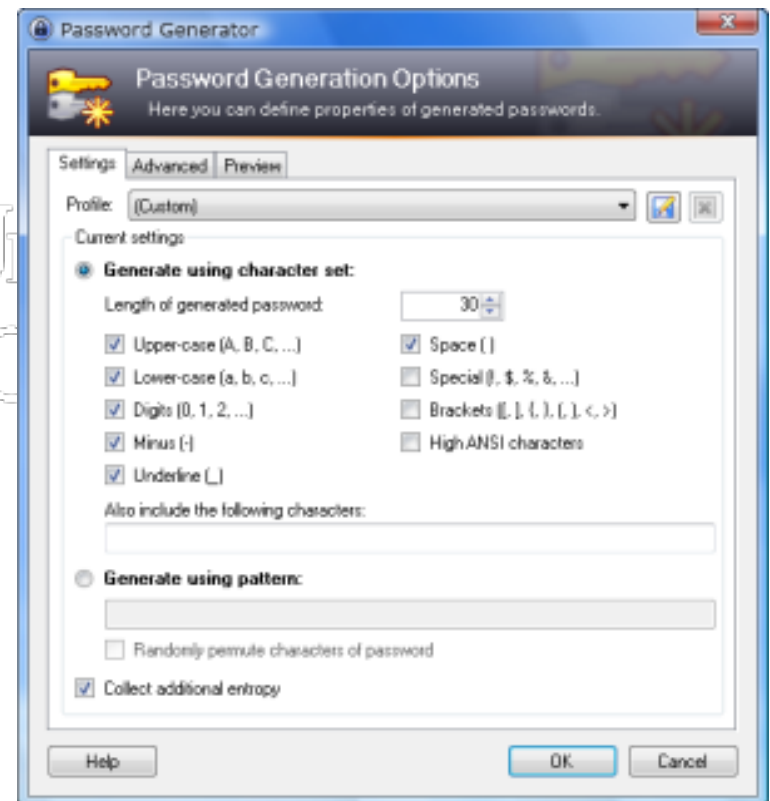
- Offline storage only
 - Plugins (not evaluated) for syncing capabilities: (Dropbox, Google Drive, OneDrive, SCP, SFTP, S3)
 - Don't forget to BACKUP!
- Open Source
- Linux, OSX support via Mono, Windows support via .NET.
- Ports (not evaluated) for mobile devices

KeePass (cont)

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office

- Generates passwords
- Free!
- Browser integration only via plugins (not evaluated)



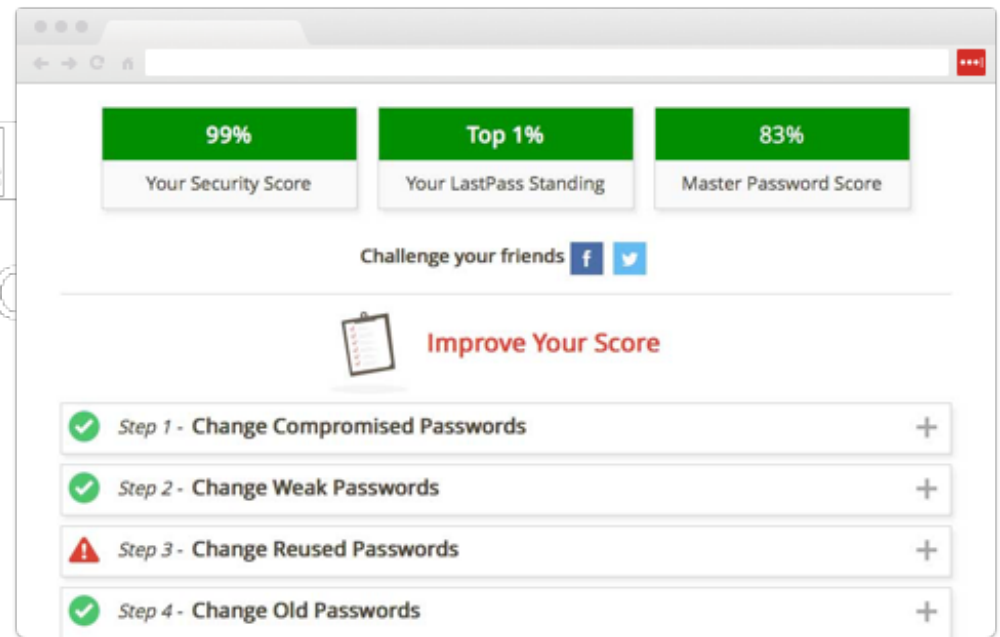
- Online “only”
 - Local password cache
- Supports 2-factor soft token authentication (including Duo!) for free
 - 2-factor hard token authentication available with Premium subscription
- Free for most features. Premium features \$12/year.

LastPass (cont)

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office

- Native Browser integration for all major browsers
- Linux support
- Password Auditing
- Mobile applications



LastPass Features

Carnegie Mellon University
Libraries

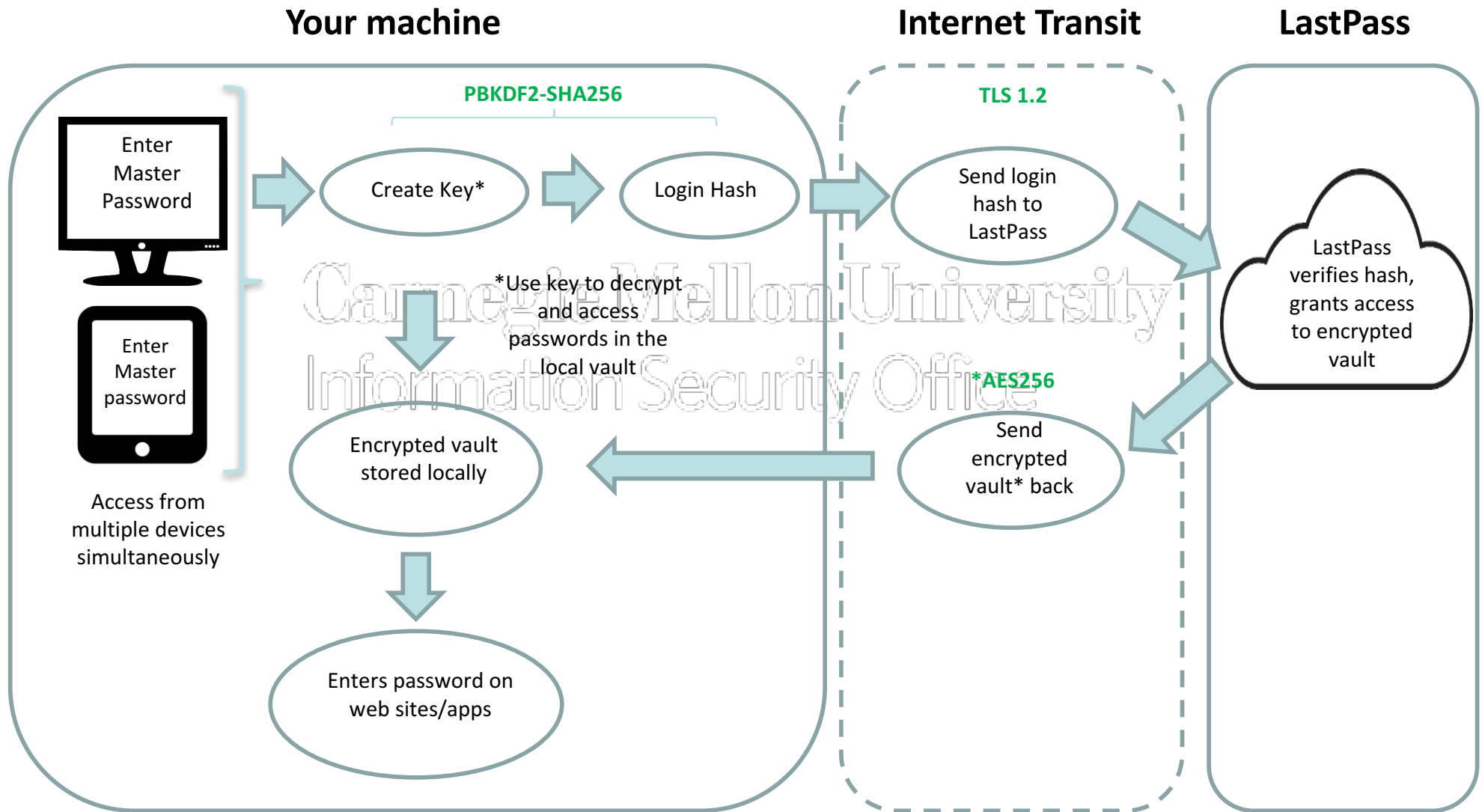
Carnegie Mellon University
Information Security Office

- Create new, unique, strong passwords
- Access passwords to log in to web sites
- Store information in secure notes
- LastPass Security Challenge
 - Identify compromised passwords 
 - Identify weak or duplicate passwords
 - Automatically change some passwords

How LastPass Works

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office



Is LastPass Secure?

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office

**Password Managers are the worst
way to store your passwords... except
for all the others.**

LastPass Security

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office

- Vulnerabilities (bugs) have been discovered
- All software has bugs
- No exploits found “in the wild”
- Would have been defeated by sound security practices (e.g. avoiding phishing attacks)
- Recognized for quick & effective responses

LastPass Security

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office



Tavis Ormandy @taviso

1d

Very impressed with how fast @LastPass responds to vulnerability reports. If only all vendors were this responsive 👍

← 14

↻ 223

♥ 560



Carnegie Mellon University



Project Member [Comment 14](#) by taviso@google.com, Mar 30 (3 days ago)

LastPass sent me a pre-release build to test, their fix looks comprehensive.

They did decide to implement Jann's Proxy() solution, which I think is quite elegant.

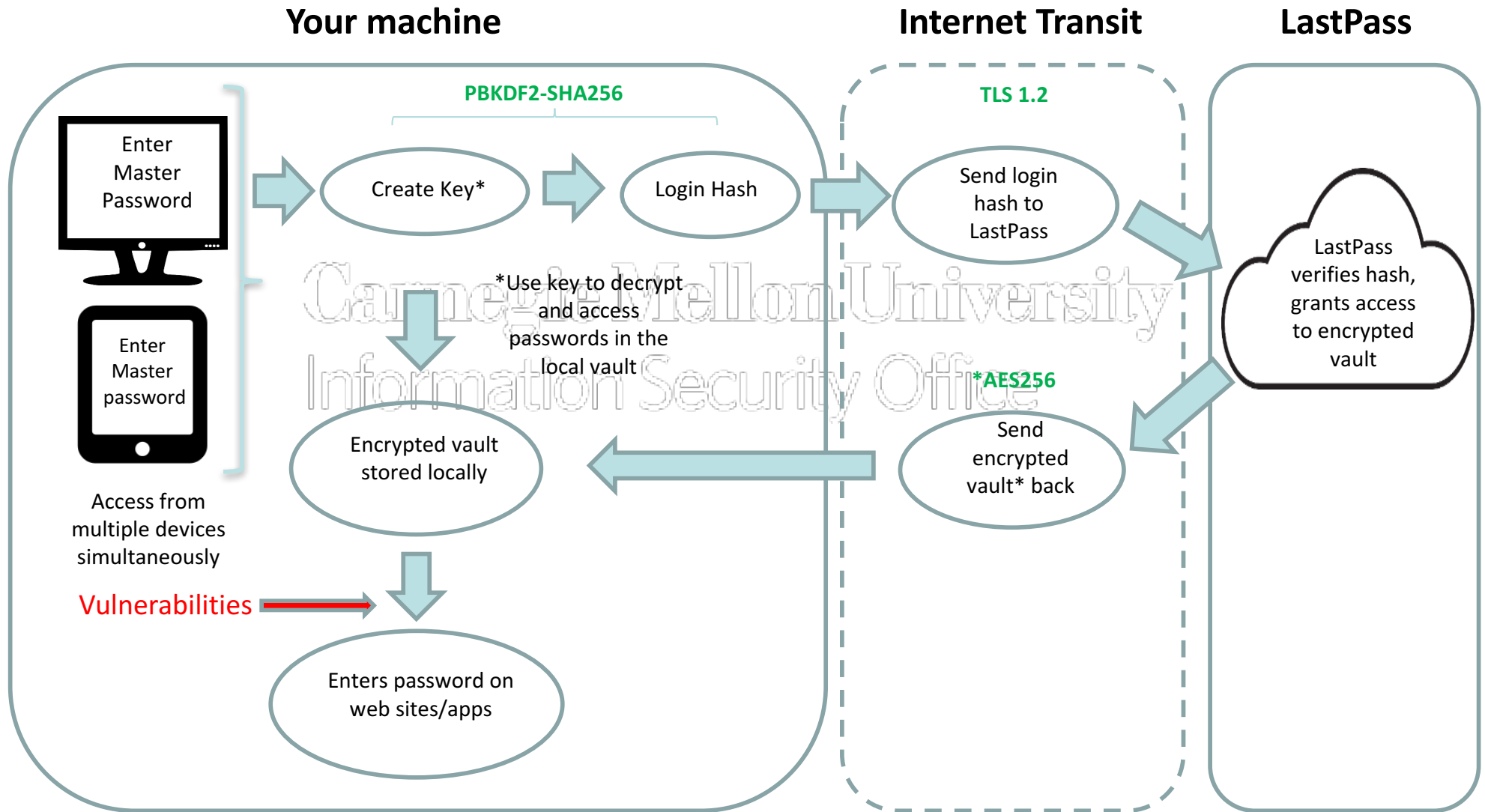
They've also implemented some additional mitigations, and have a plan ready for updates (still on schedule for this week).

Really impressed with their response to this complex issue.

How LastPass Works

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office



Making LastPass more secure

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office

- Enable MFA
 - Disable “offline” access
- Restrict mobile access
- Disable access from TOR
- One IP at a time
- Disable auto fill
- Auto log-off when idle
- Access websites from your vault or bookmarks (and definitely not from a link you clicked)
- Manage your risk; consider keeping separate, strong passwords for:
 - Primary Email
 - Banking & Finance
 - Work vs Personal?

LastPass Settings

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office

The screenshot displays the LastPass web application interface. On the left is a dark sidebar with navigation options: Collapse, Sites, Secure Notes, Form Fills, Sharing Center, Security Challenge (0%), Emergency Access, Account Settings (circled in red), and More options. The top header is red, featuring the LastPass logo, a search bar labeled 'search my vault', and a user profile for 'villadso@yahoo.com' (Free User). The main content area is light blue and contains a large icon of an open box with a shield and a browser window inside. Below this icon, the text reads: **Remember every password** and 'Save and fill passwords for any website or app. Search them all from your vault.' In the bottom right corner, there is an 'Add Site' button and a red circular button with a white icon.

LastPass MFA

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office

Account Settings

General

Multifactor Options

Trusted Devices

Mobile Devices

Never URLs

Equivalent Domains

URL Rules

Add another layer of protection by requiring a second login step. Keep the bad guys out, even if they steal your password through malicious software.

Multifactor Authentication - Free

Multifactor Option	Name	Description	State	Action
	LastPass Authenticator	Generates one time verification codes or sends push notifications to your smart phone.	Disabled	 
	Google Authenticator	Generates one time verification codes on your smart phone. Can also be used with Microsoft Authenticator.	Disabled	 
	Toopher	Sends push notifications to your smart phone to verify your login.	Disabled	 
	Duo Security	Generates one time verification codes or sends push notifications to your smart phone.	Disabled	 
	Transakt	Sends an Accept/Reject notification to your smart phone.	Disabled	 
	Grid	Printable spreadsheet of numbers and letters used to enter different values when logging in.	Disabled	 

LastPass Security Settings

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office

Google Authenticator

To get started:

- Download and install the application on your mobile device.
- View your barcode and scan it using the Google Authenticator application.

Option	Value
Enabled	Yes
Permit Offline Access	Disallow
Barcode	View
Private Key	View
Regenerate Key	Regenerate
More Information	Mobile application Help manual

Update

Trusted Devices

requiring a second

on - Free

Name

LastPass Authenticator

Google Authenticator

Toopher

Duo Security

Transakt

Grid

Printable spreadsheet of numbers and letters used to enter different values when logging in.

LastPass Security Settings

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office

Account Settings

General

Multifactor Options

Trusted Devices

Mobile Devices

Never URLs

Equivalent Domains

URL Rules

Control what smartphones and tablets may access your LastPass account. By default, a unique identifier (UUID) is created to track each device, but you can edit the device label at any time.

You currently have no mobile devices defined.

To restrict access to all mobile devices except those allowed above, click 'Enable'

Enable

Click Enable

LastPass Security Settings

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office

Account Settings

General

Multifactor Options

Trusted Devices

Mobile Devices

Never URLs

Equivalent Domains

URL Rules

Manage your LastPass account information, privacy, email subscriptions, and security settings.

Security

Security Email

Send Test Email

☒ Only allow login from selected countries:

Country Restriction

☒ United States

☐ Afghanistan

☐ Aland Islands

☐ Albania

Tor Networks

☒ Disallow logins from Tor networks.

Master Password Reverting

☒ Allow reverting LastPass master password changes

Disable Email Verification

☐ Skip email verification of unknown devices and locations.

Disable

Hide Advanced Settings

Update

LastPass Security Settings

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office

Account Settings

General

Multifactor Options

Trusted Devices

Mobile Devices

Never URLs

Equivalent Domains

URL Rules

Manage your LastPass account information, privacy, email subscriptions, and security settings.

Disable Email Verification	☐ Skip email verification of unknown devices and locations.	
Disable multifactor trust expiration	☐ Skip 30 day expiration for trusted clients.	
Auto-Logoff Other Devices	☒ Automatically logoff other devices when logging in from a different device. ☒ Do not logoff other devices originating from the same IP.	
Password Iterations	5000	
Website Auto-Logoff	2 Weeks	
Bookmarklet Auto-Logoff	2 Weeks	

Privacy

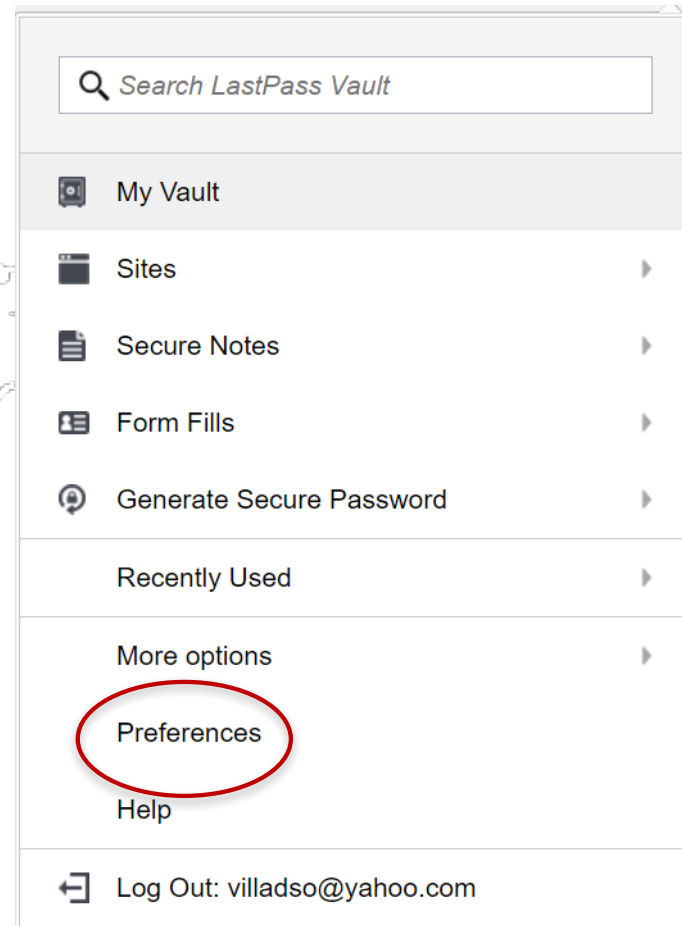
Hide Advanced Settings

Update

LastPass Security Settings

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office



LastPass Security Settings

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office

Preferences LastPass ...

General

Notifications

Hotkeys

Advanced

Icons

Security

☒ Automatically Log out when all browsers are closed and Chrome has been closed for (mins)

☒ Automatically Log out after idle (mins)

General

Open New Pages in

☐ Open extension pages in dialogs

☒ Highlight input boxes

☐ Automatically Fill Login Information

☐ Show My LastPass Vault After Login

Appearance

☒ Show Sites in Folders

☐ Hide Context Menu Options

Restore 'General' Defaults

Cancel Save

LastPass Features

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office

Sites

Sort By: Folder (a-z) ▼

(none) (1) ▼



duosecurity.com
Ole Villadsen

Add New folder

+

Share Item

Add Secure Note

Add Site

LastPass Features

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office

Add Site LastPass... |  

URL:

Name: **Folder:**

Username: **Password:**

Notes:

Advanced Settings:
☒ Require Password Reprompt ☐ Autologin ☒ Disable AutoFill



LastPass Features

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office

Secure | <https://www.gobi3.com/Pages/Login.aspx>

UL CMUAccts CMUSearch CMU Cyber Current Projects CyberCerts CybrImpStdy Ole Google MOOC Utils Tools Help Misc Daily

GOBI®

Login

Email:

Password:

YBP-PRD-WB-0001 Version: 3

System Requirements

If you have trouble logging in, contact gobi3@ybp.com.

Library News

Hard-to-Find Titles Are Available in BookZone

BookZone, formerly MarketPlace, is your source in GOBI for the out-of-stock titles. Its real-time feature stock and condition information for select the copy that meets your and convenient way to order the titles all within your existing GOBI

changed, the new GOBI Library and will provide the same choice of regators as it did under the YBP id the FAQ and check out our new site <https://gobi.ebsco.com/>.

Reports and 2015/2016 Annual Book

in GOBI.

Show and Conference Calendar

Innovative Users Group (IUG) Conference

National Harbor, MD, USA
April 2-5

Customers of SirsiDynix Users Group, Inc. (COSUGI) Conference

Salt Lake City, UT, USA
April 11-13

Publisher Corner



This vibrant and compelling book uses 240 artworks as case studies to tell the story of ten individual colours or colour groups. [more...]



This codebook contains the official CPT guidelines, only offered by the AMA. Rely on it for code, guideline and text changes for 2017. [more...]



AMA
AMERICAN MEDICAL ASSOCIATION



How important has the sea been in the development of human history? Very important indeed is the conclusion of this groundbreaking [more...]



BOYDELL & BREWER



Presenting the state-of-the-art for the theory and practice of qualitative inquiry, this landmark Handbook has been a publishing phenomenon in the human sciences since [more...]



SAGE



The first volume of the *International Yearbook of Soil Law and Policy* includes an important discussion on the implementation of the Sustainable Development Goals [more...]



SPRINGER NATURE

LastPass Features

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office

Add Note

LastPass...|

Name:

Folder:

Note Type:

Generic

Advanced Settings:

Add Attachment

Cancel

Save

LastPass Features

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office

LastPass ... |

Security Challenge

90%

Your Security Score

Top 2%

Your LastPass Standing

100%

Master Password Score

Challenge your friends



Improve Your Score



Step 1 - **Change Compromised Passwords**

Auto-Change Password:



You have no compromised sites!

Password Generator: