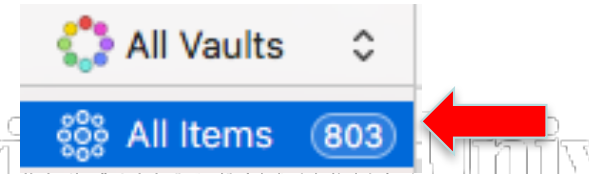
Improving Password Management

Laura Raderman, Policy and Compliance Coordinator, ISO

Ole Villadsen, Research Liaison, Cybersecurity, UL

Password Management

- How many passwords do you have?



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

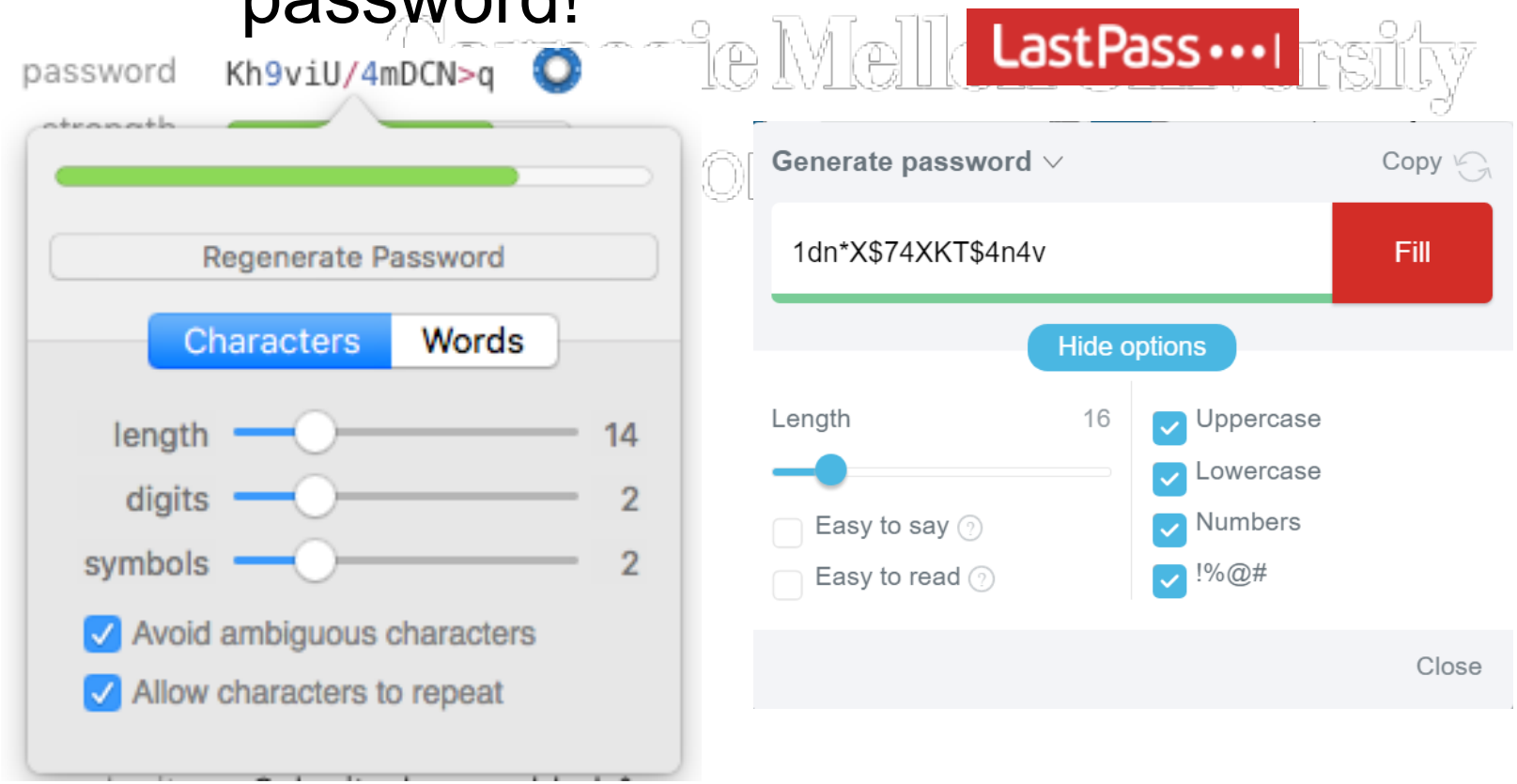
- Picking a password can be difficult
  - Multiple sites have different rules – what may be acceptable on one site is unacceptable on another
    - Biggest culprit: sites that don't accept special characters
  - Very strong passwords generally aren't very memorable
    - buz%vG9X#paC3s

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)

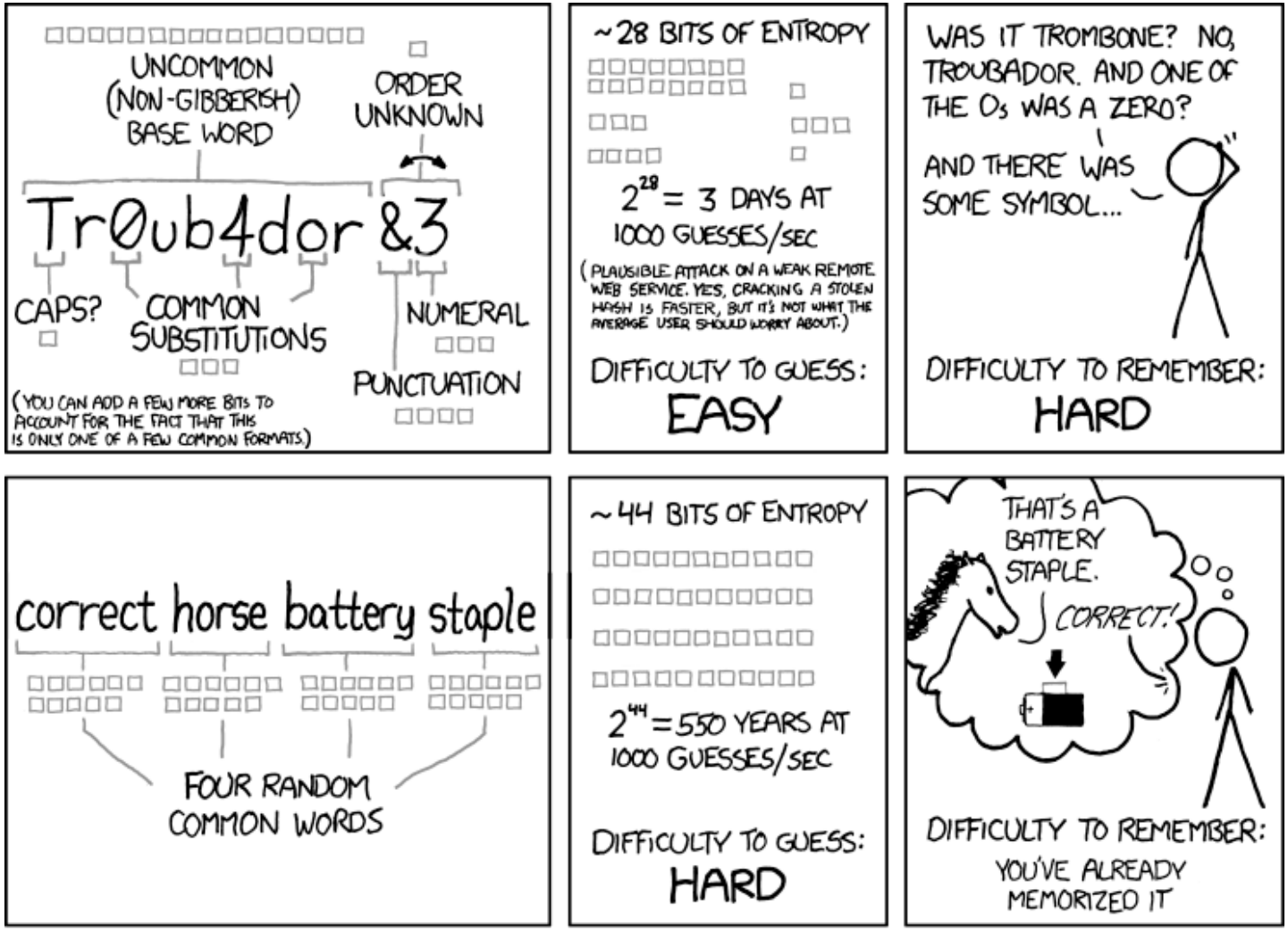
Master Passwords

- 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

http://xkcd.com/936/

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office



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

- 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

Carnegie Mellon University Libraries

Carnegie Mellon University Information Security Office

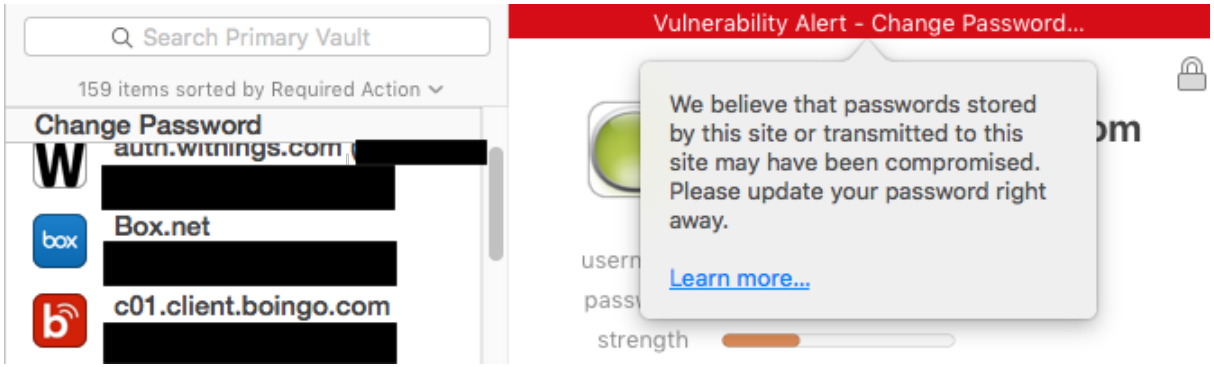
- https://1password.com
- Both an online and a desktop/mobile application
  - Both are secure!
- Not free
  - $64.99 for the “standalone” version (upgrades have been less in the past – usually ~$35 every 3-4 years)
  - $2.99/mth billed annually ($35.88/yr) for online

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)

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

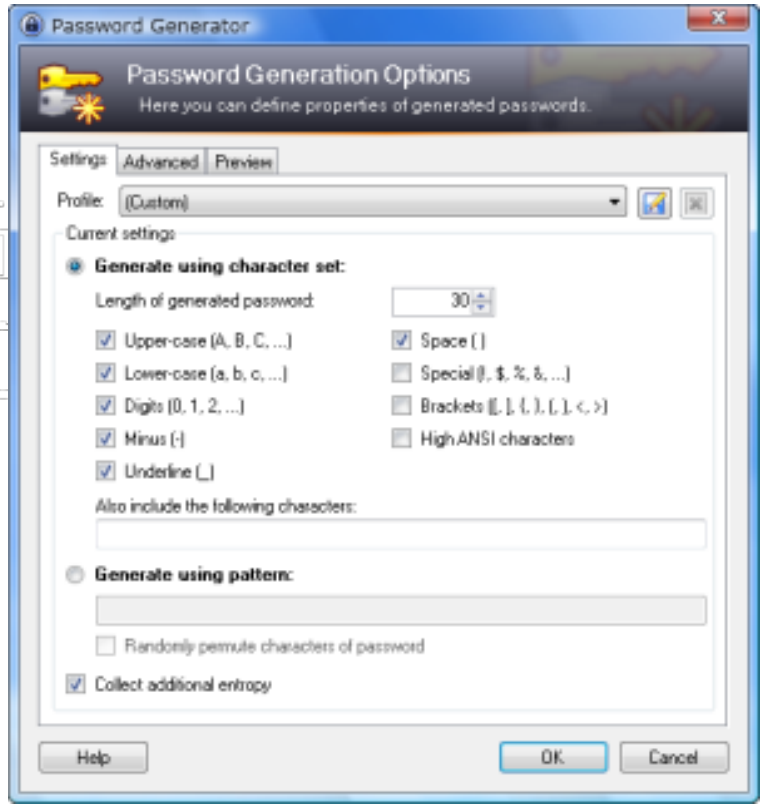


KeePass

- 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)

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



LastPass

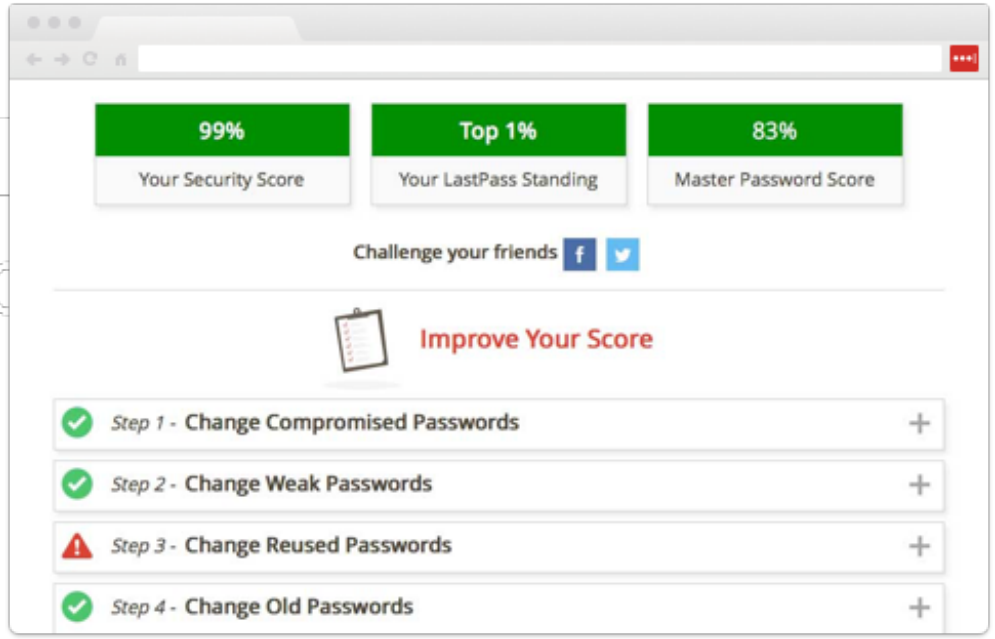
Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office

- 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)

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



LastPass Features

Carnegie Mellon University
Libraries

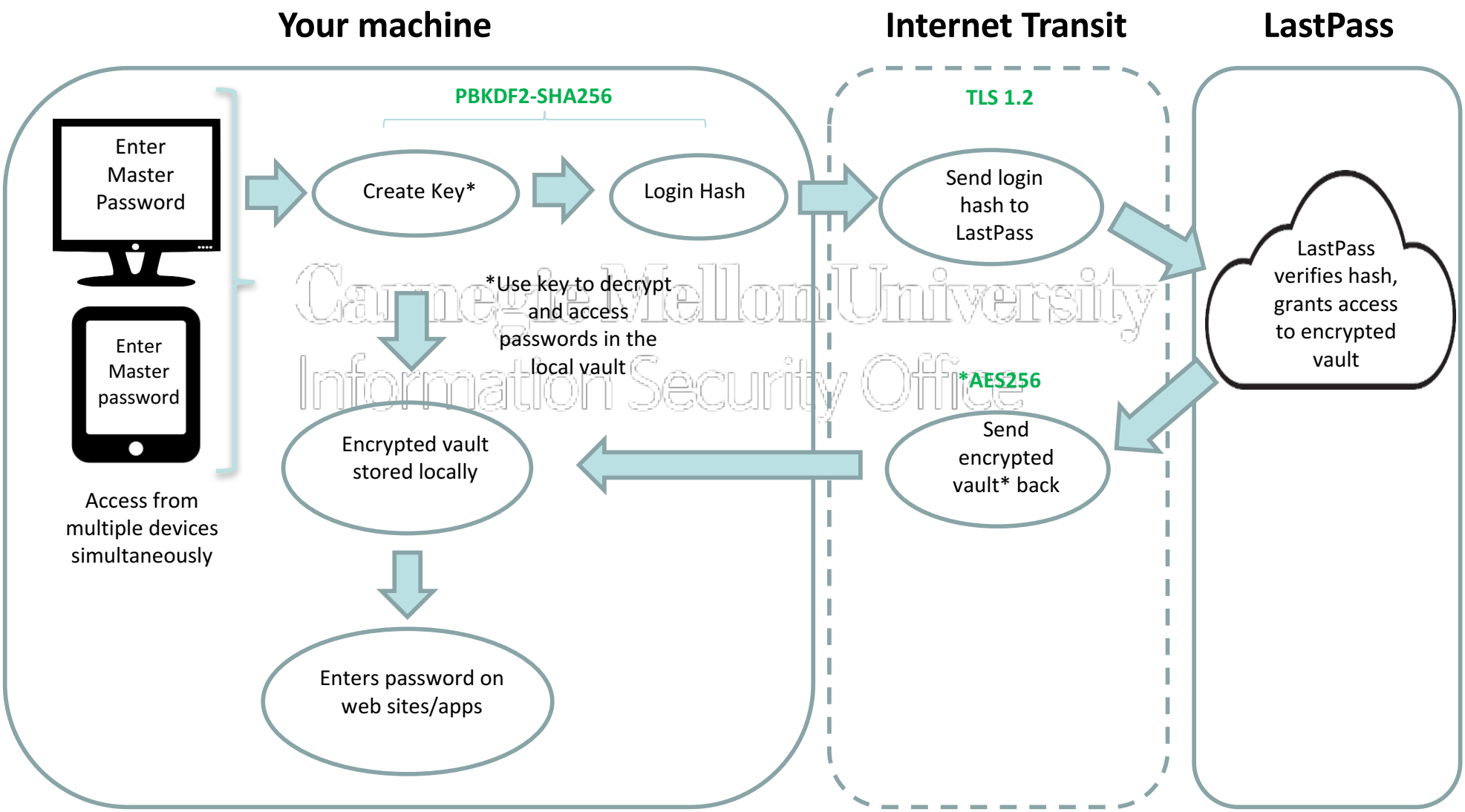
Carnegie Mellon University
Information Security Office

- 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.

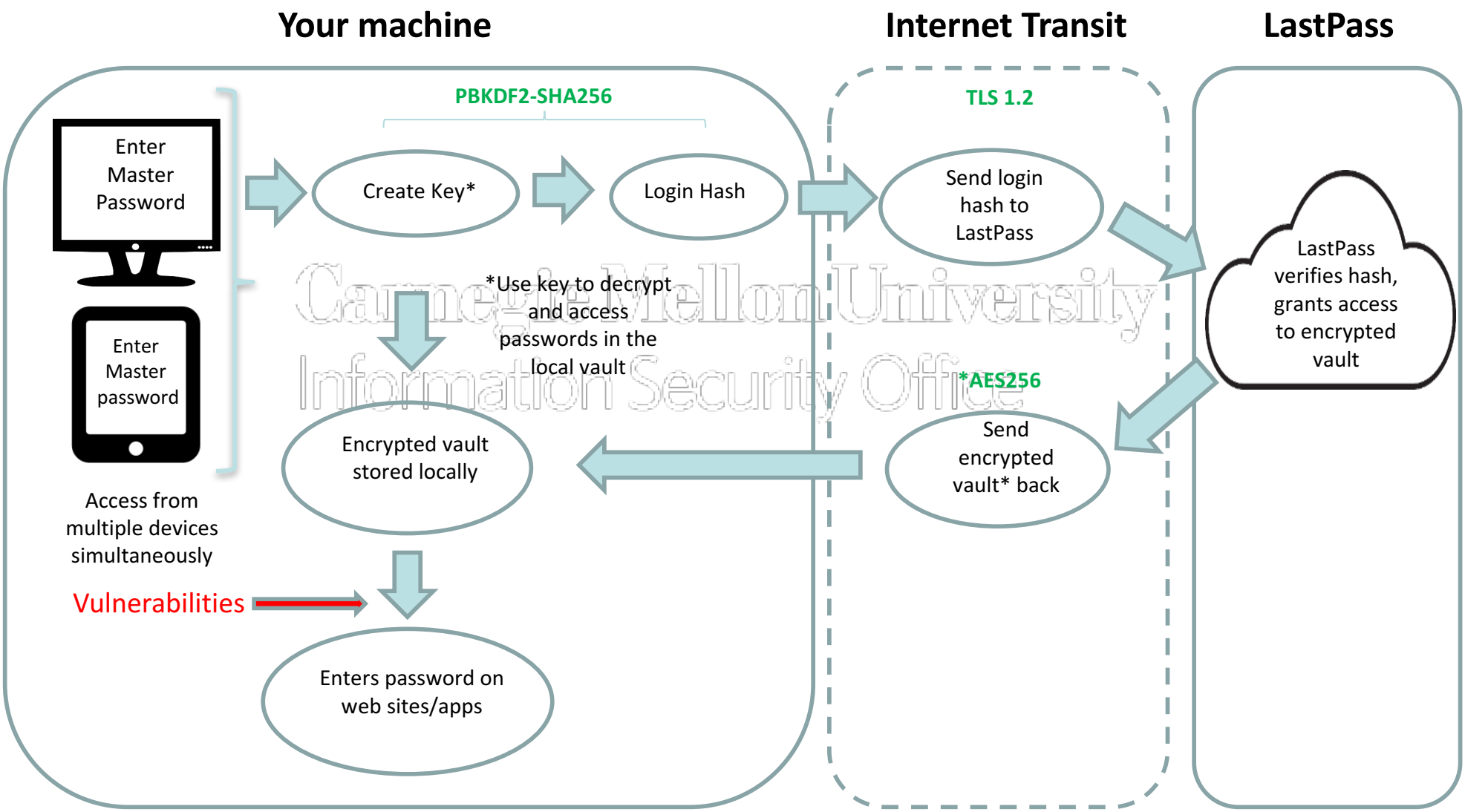
They've also implemented some additional mitigations, and have a plan ready for updates (still on schedule for this week).

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

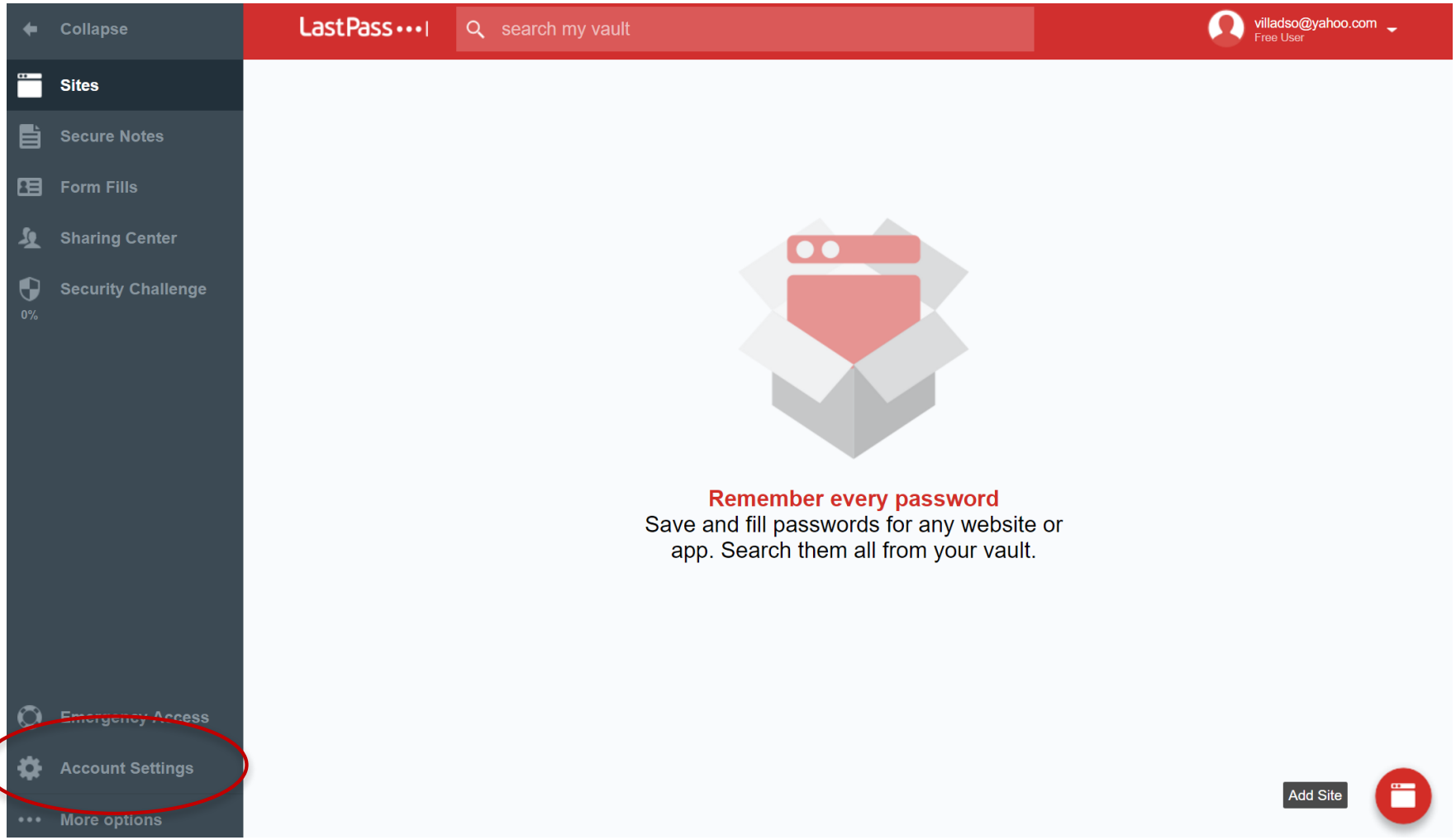
- Enable MFA
  - Disable “offline” access
- Restrict mobile access
- Disable access from TOR
- One IP at a time
- Disable auto fill
- Auto log-off when idle
- Access websites from your vault or bookmarks (and definitely not from a link you clicked)

- Manage your risk; consider keeping separate, strong passwords for:
  - Primary Email
  - Banking & Finance
  - Work vs Personal?

LastPass Settings

Carnegie Mellon University
Libraries

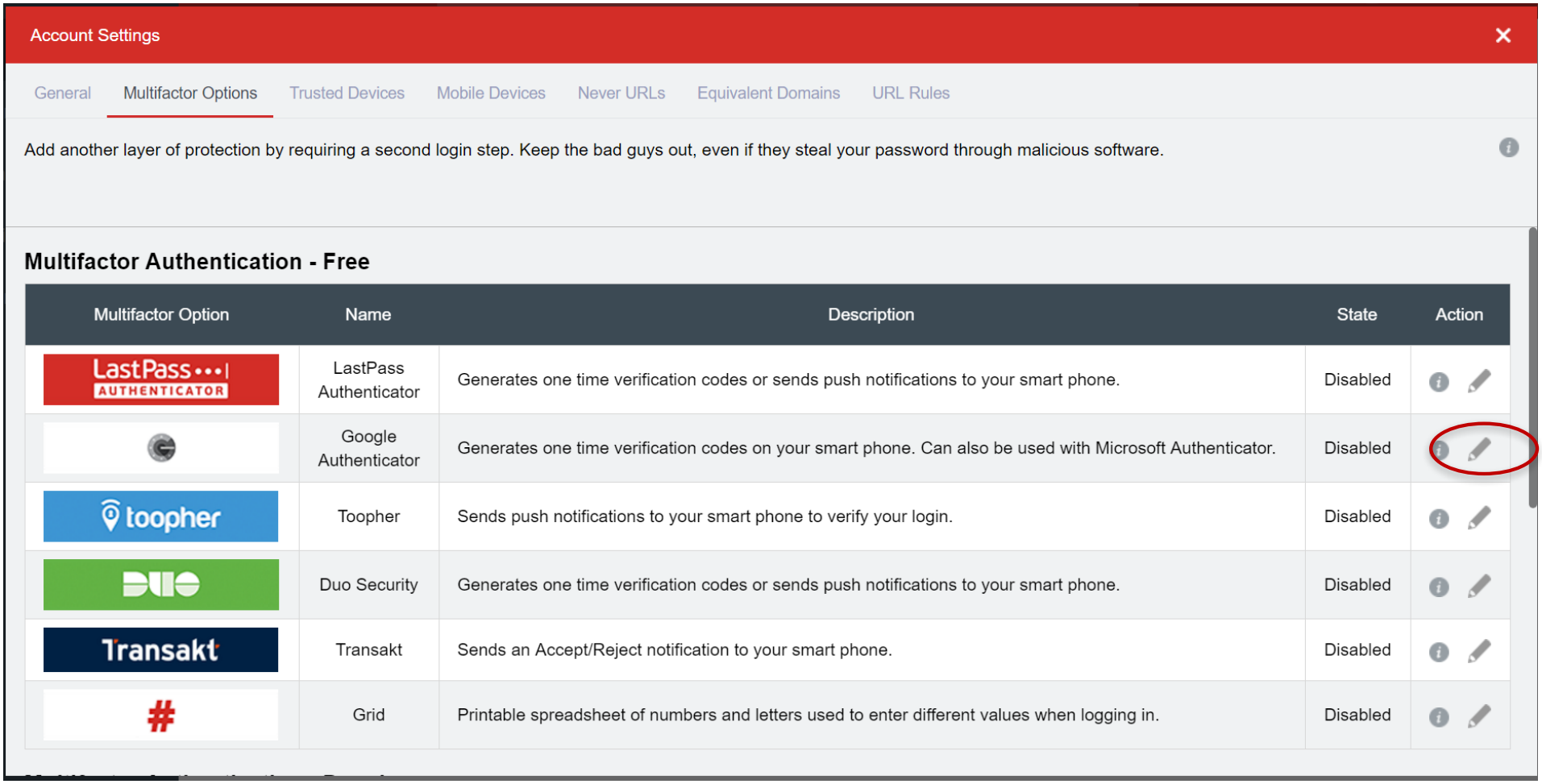
Carnegie Mellon University
Information Security Office



LastPass MFA

Carnegie Mellon University Libraries

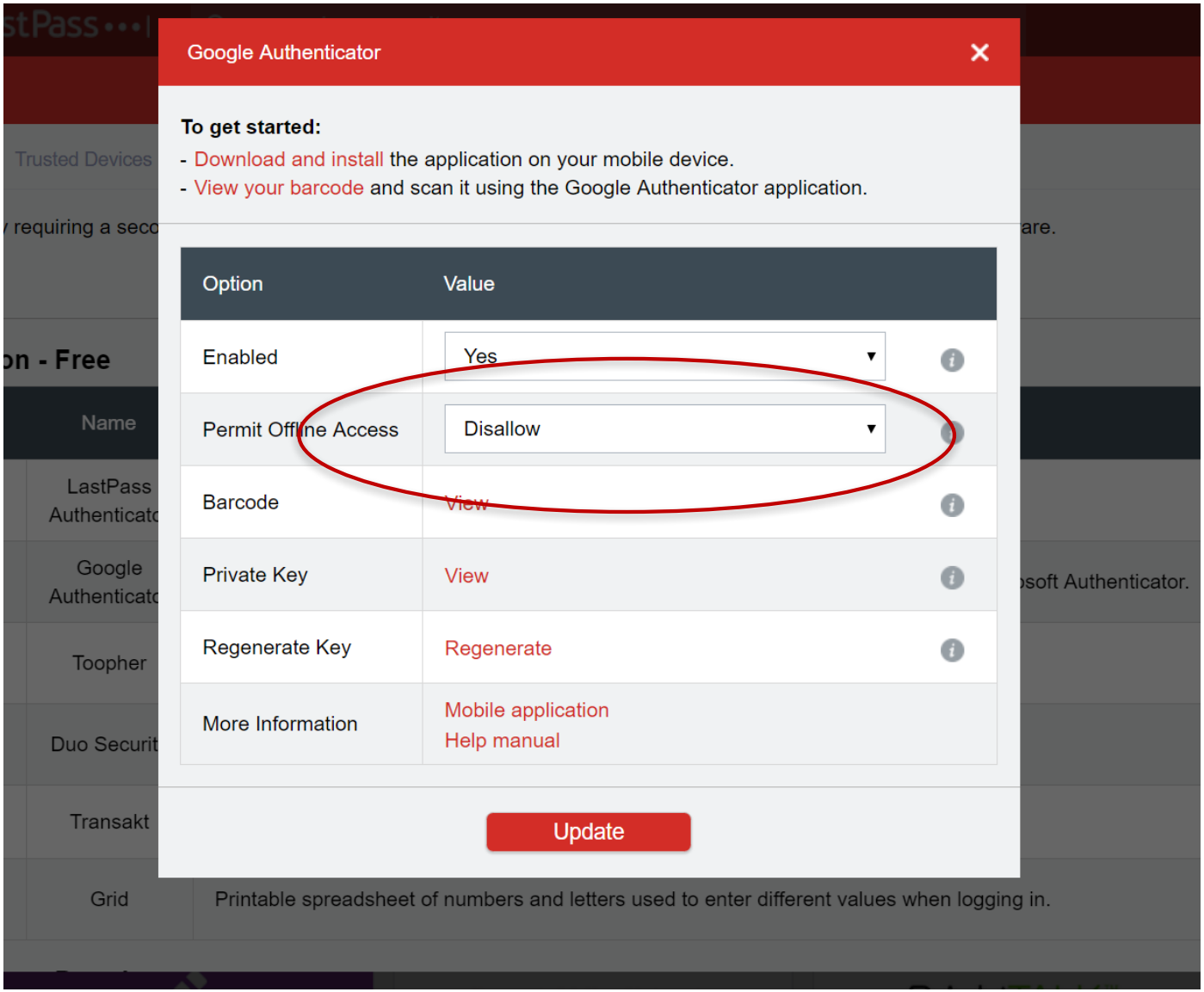
Carnegie Mellon University Information Security Office



LastPass Security Settings

Carnegie Mellon University
Libraries

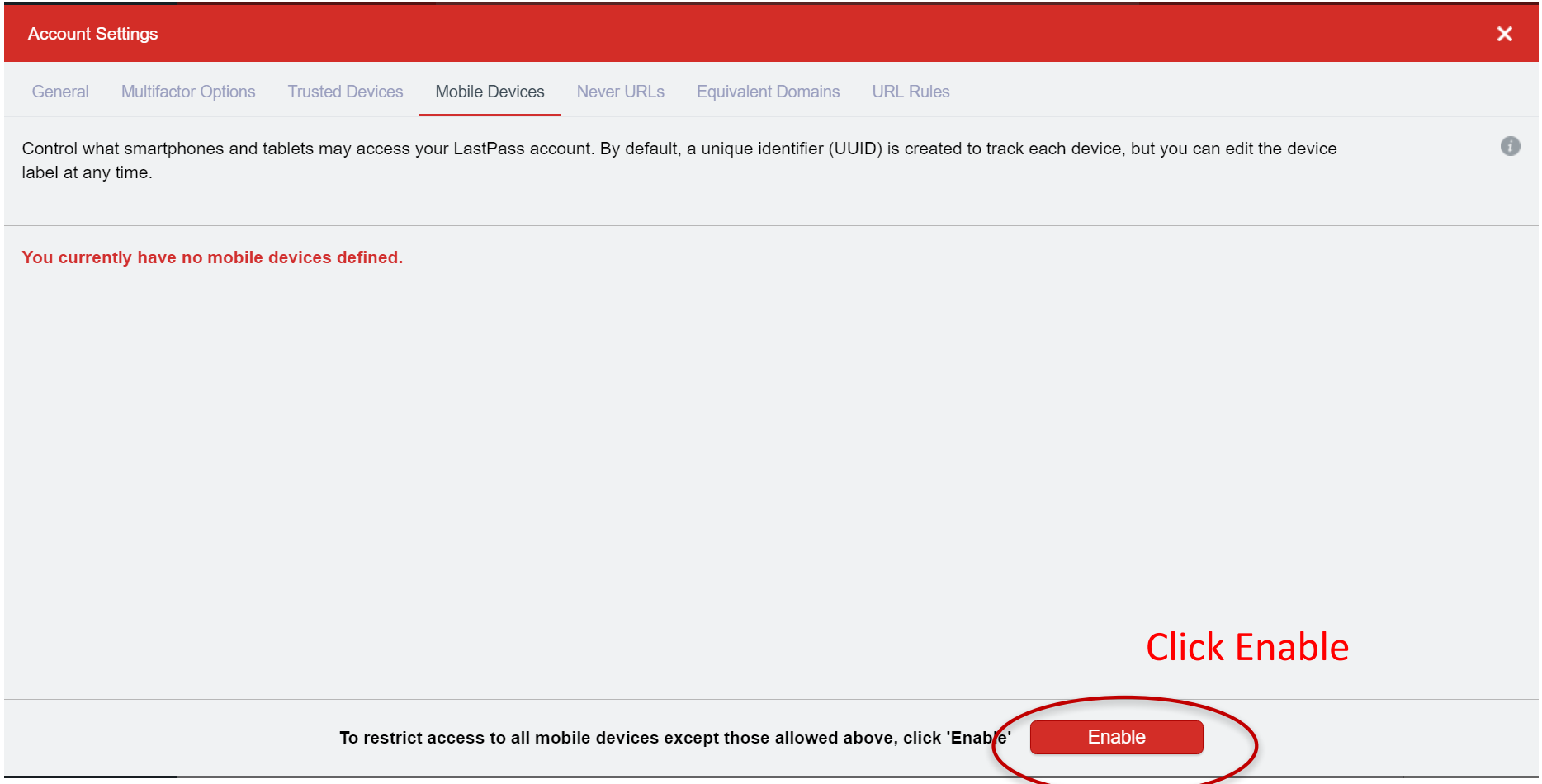
Carnegie Mellon University
Information Security Office



LastPass Security Settings

Carnegie Mellon University Libraries

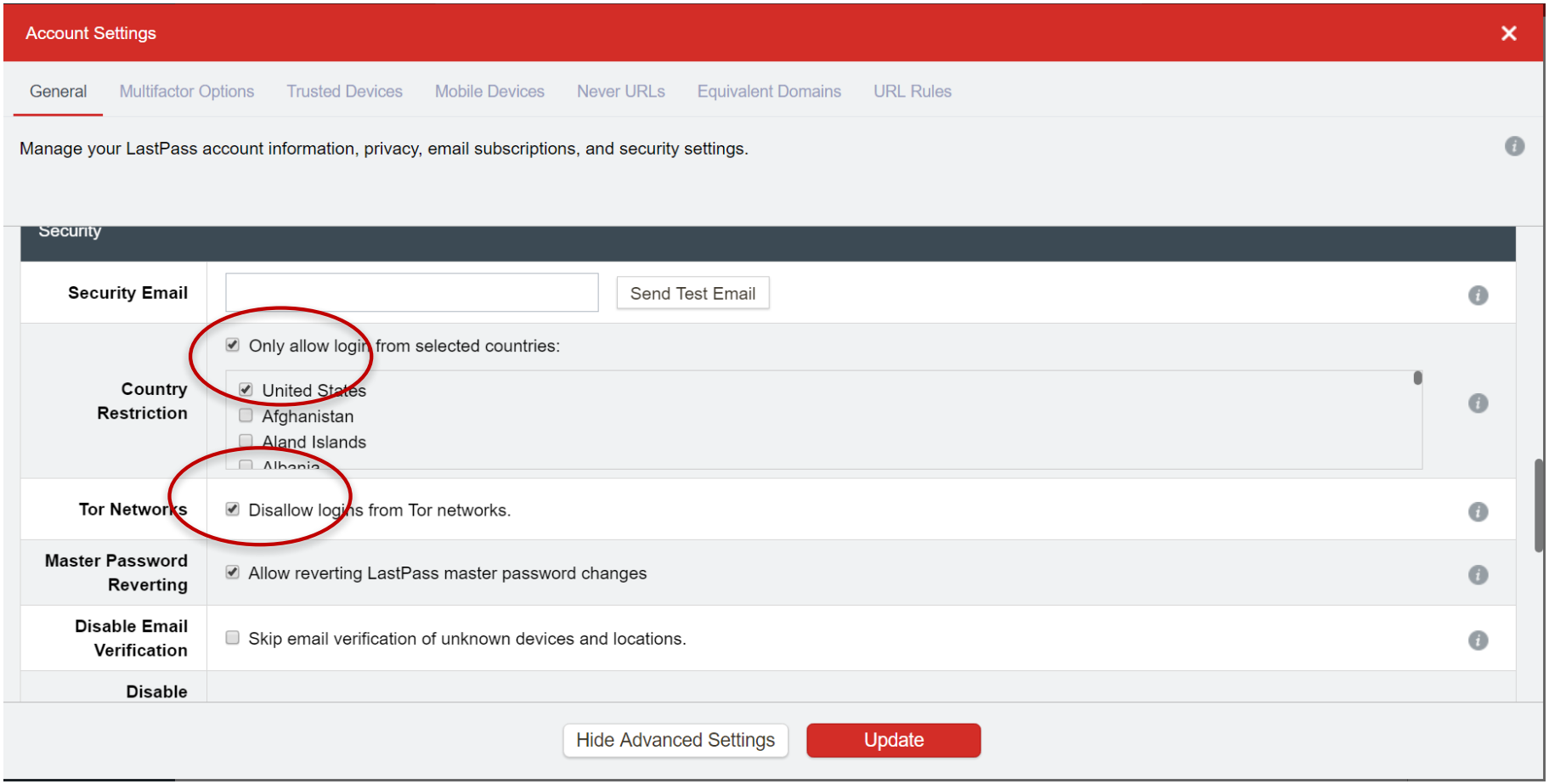
Carnegie Mellon University Information Security Office



LastPass Security Settings

Carnegie Mellon University Libraries

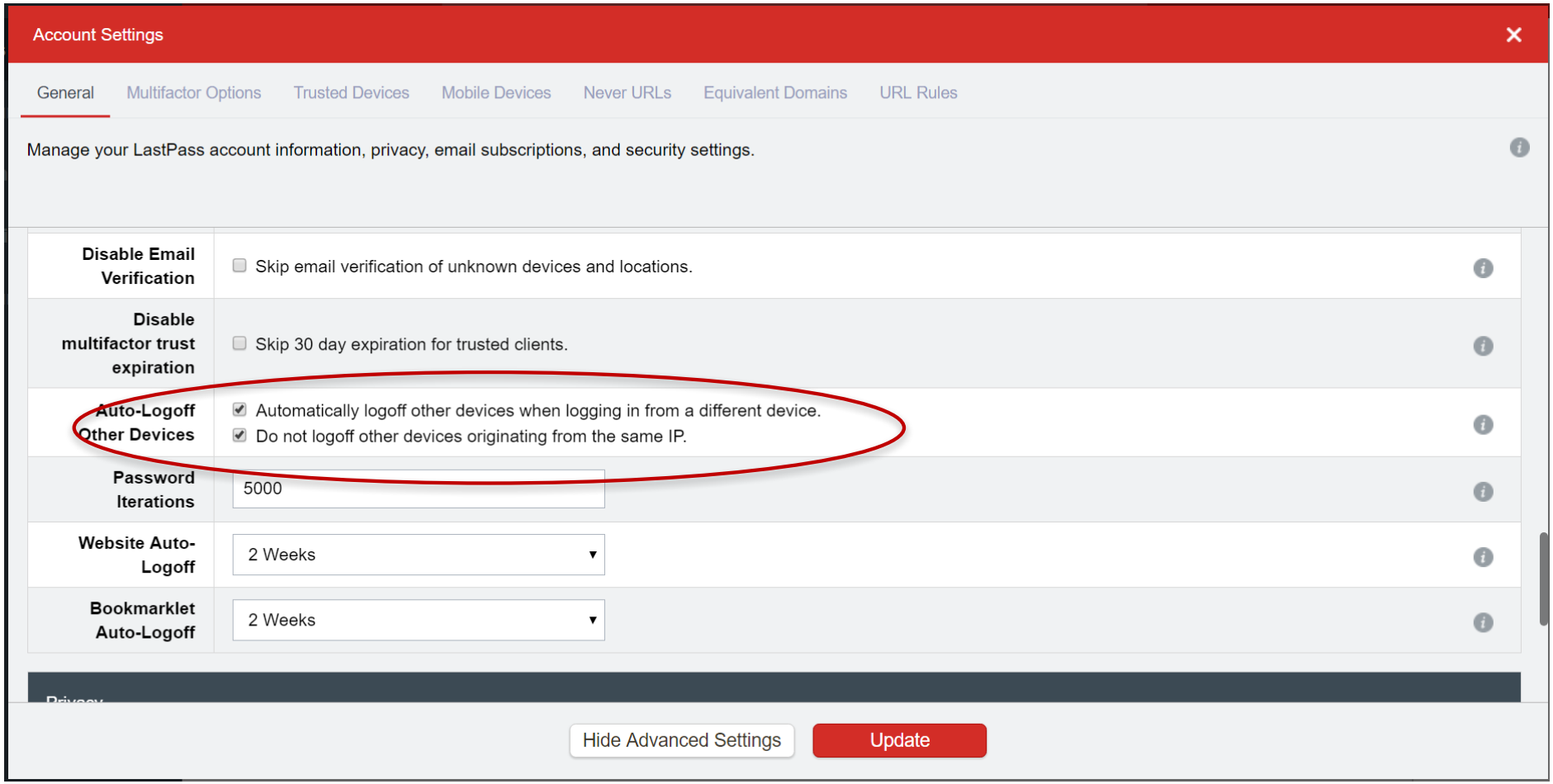
Carnegie Mellon University Information Security Office



LastPass Security Settings

Carnegie Mellon University Libraries

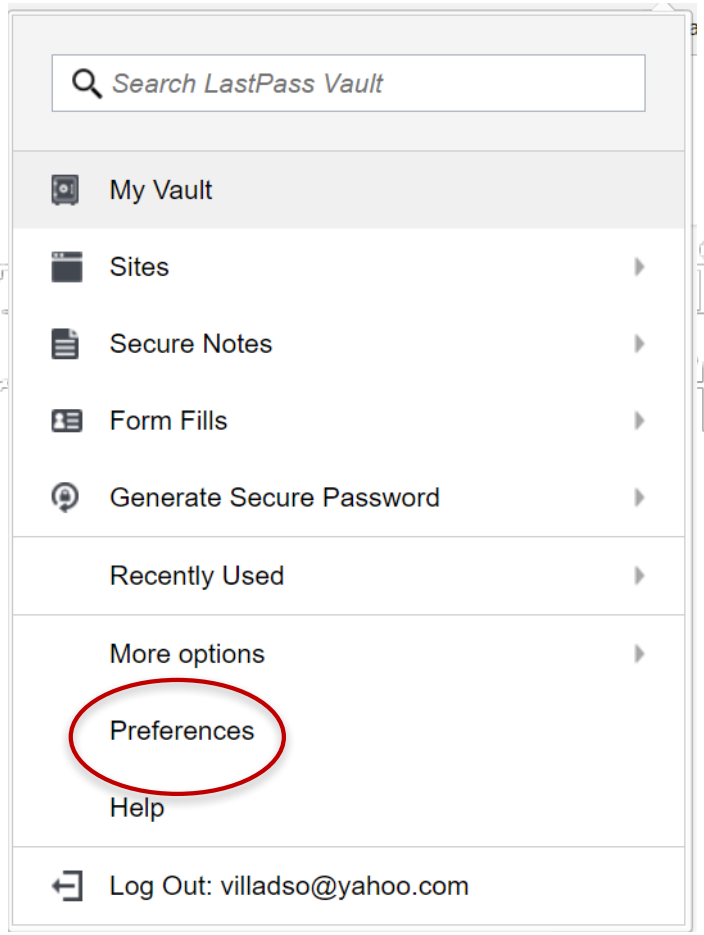
Carnegie Mellon University Information Security Office



LastPass Security Settings

Carnegie Mellon University
Libraries

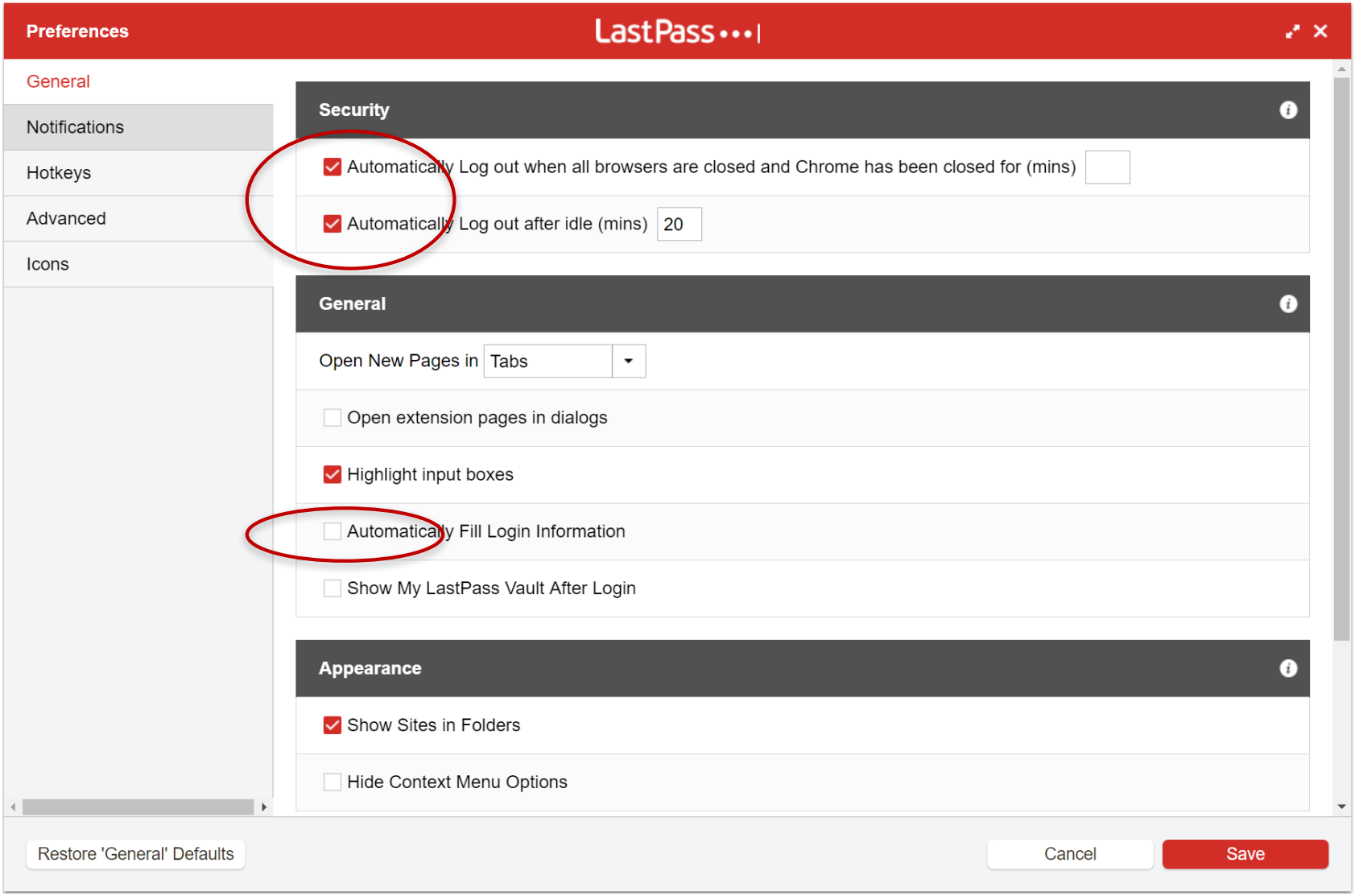
Carnegie Mellon University
Information Security Office



LastPass Security Settings

Carnegie Mellon University Libraries

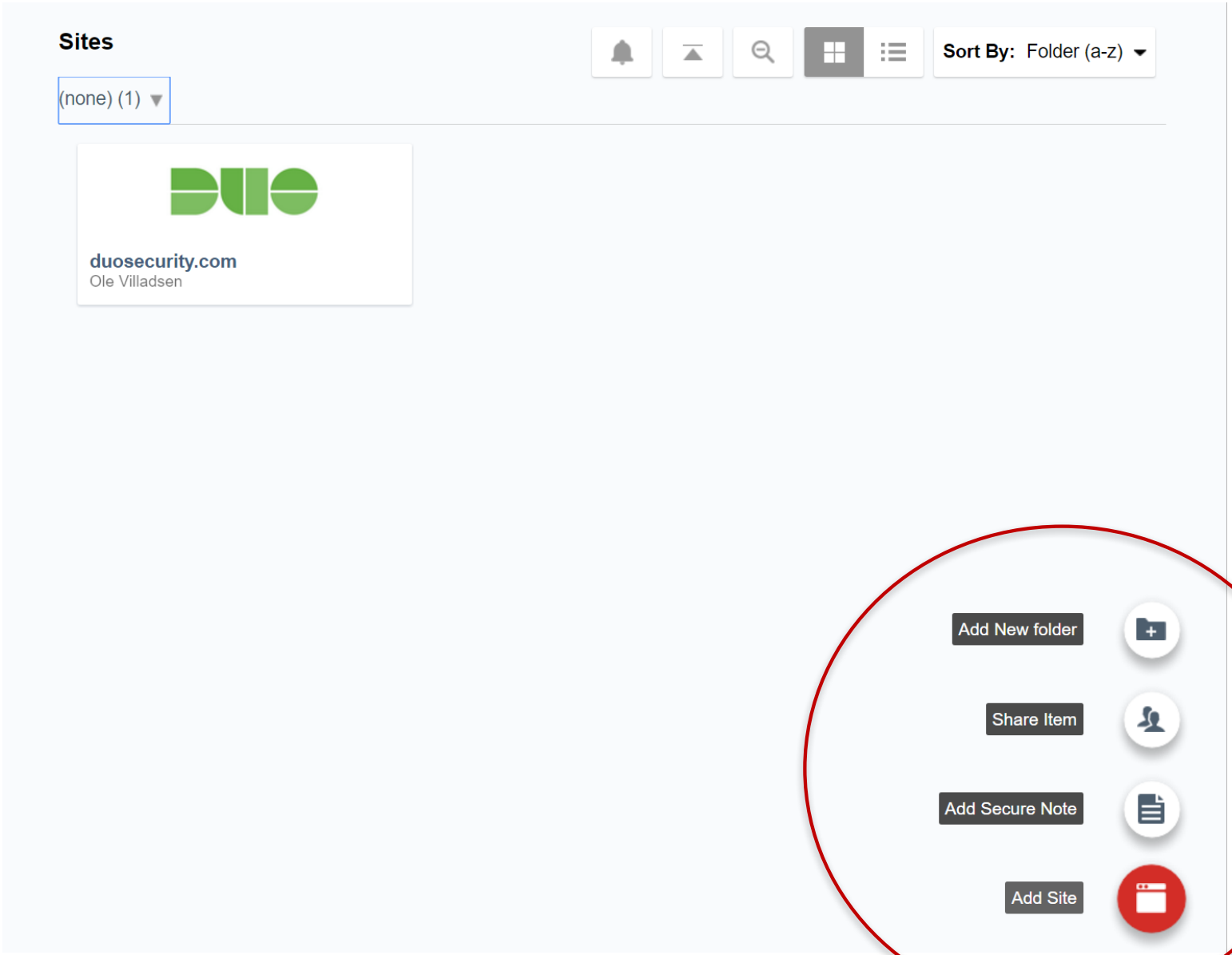
Carnegie Mellon University Information Security Office



LastPass Features

Carnegie Mellon University
Libraries

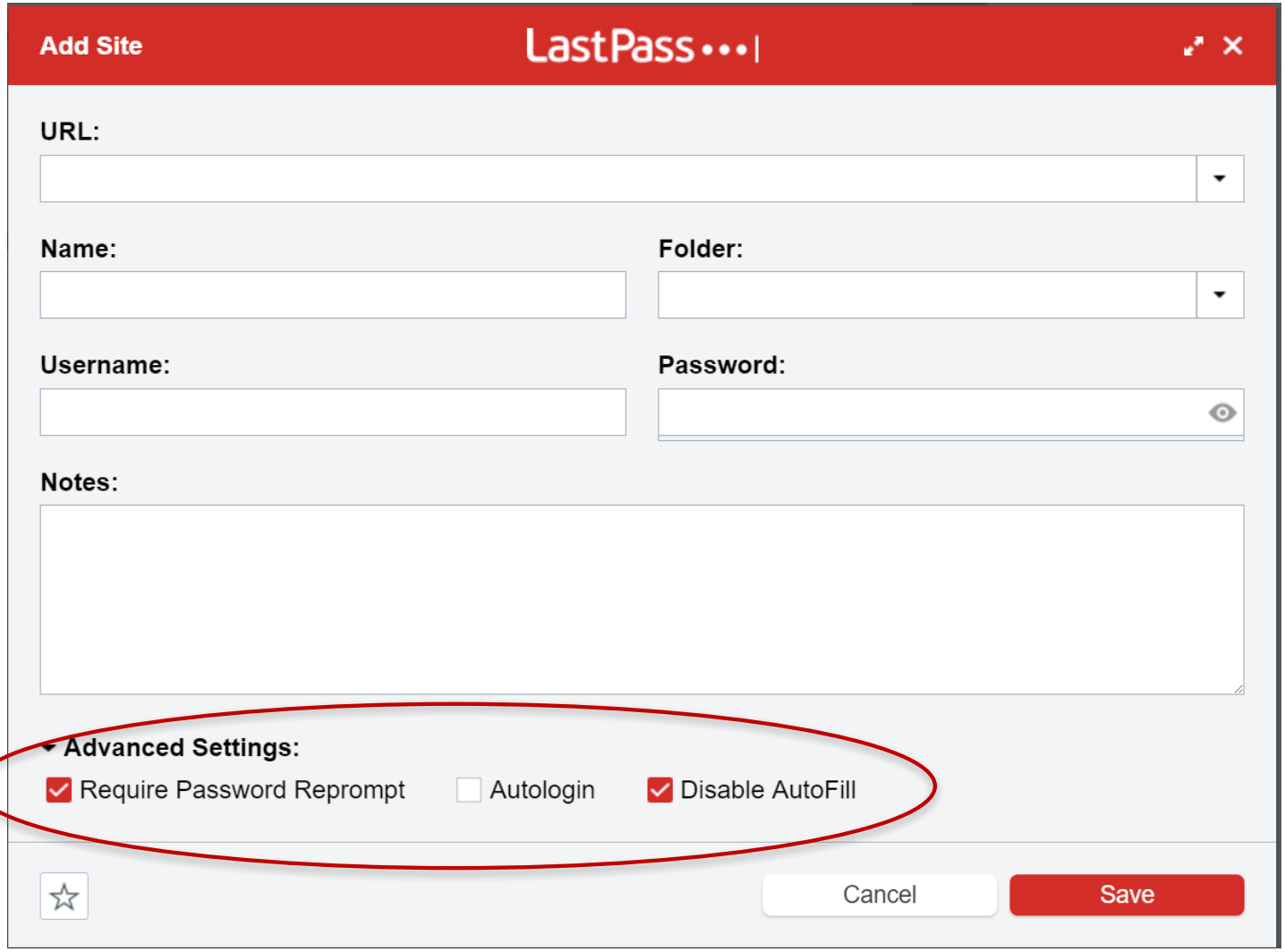
Carnegie Mellon University
Information Security Office



LastPass Features

Carnegie Mellon University
Libraries

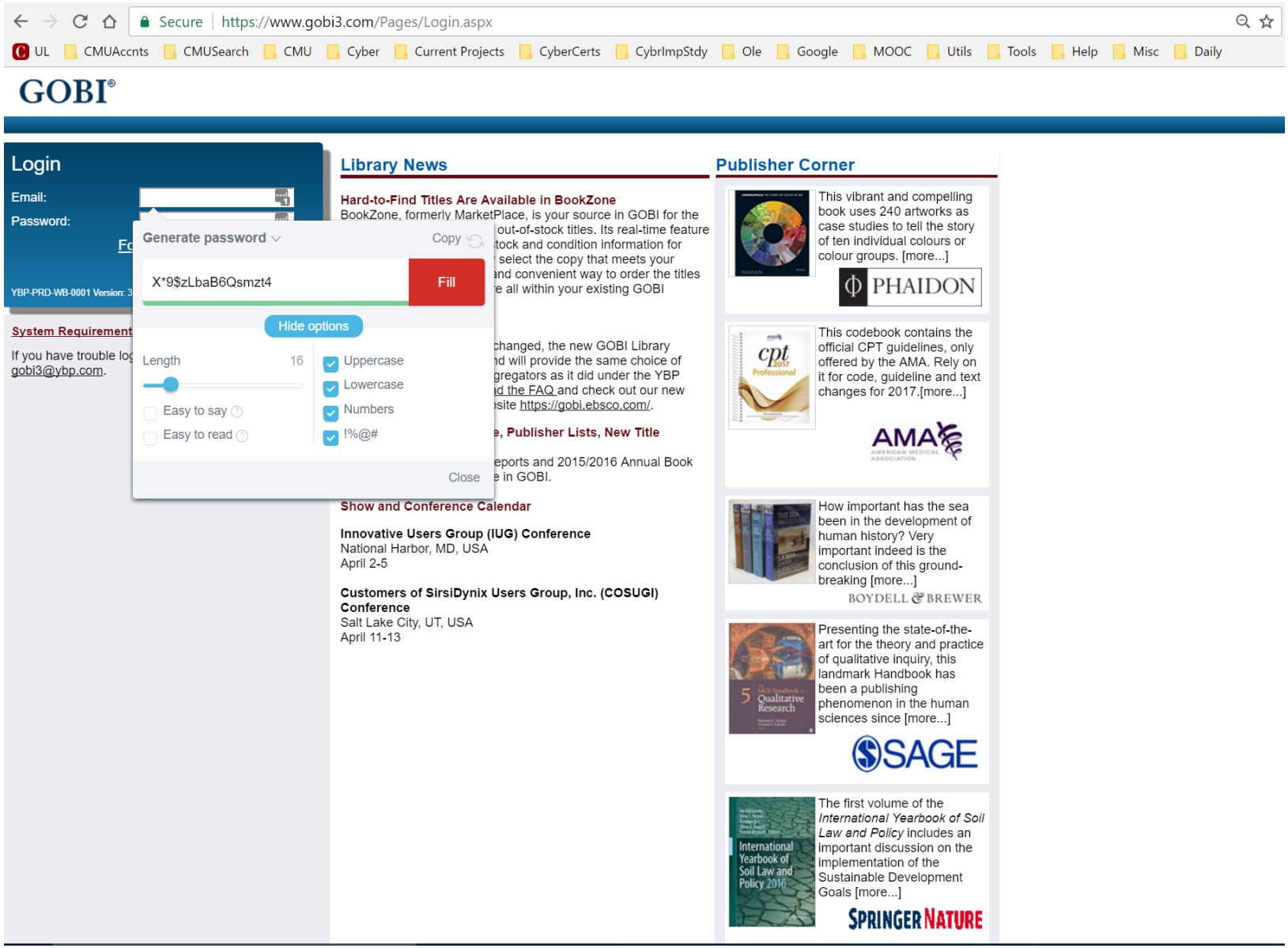
Carnegie Mellon University
Information Security Office



LastPass Features

Carnegie Mellon University Libraries

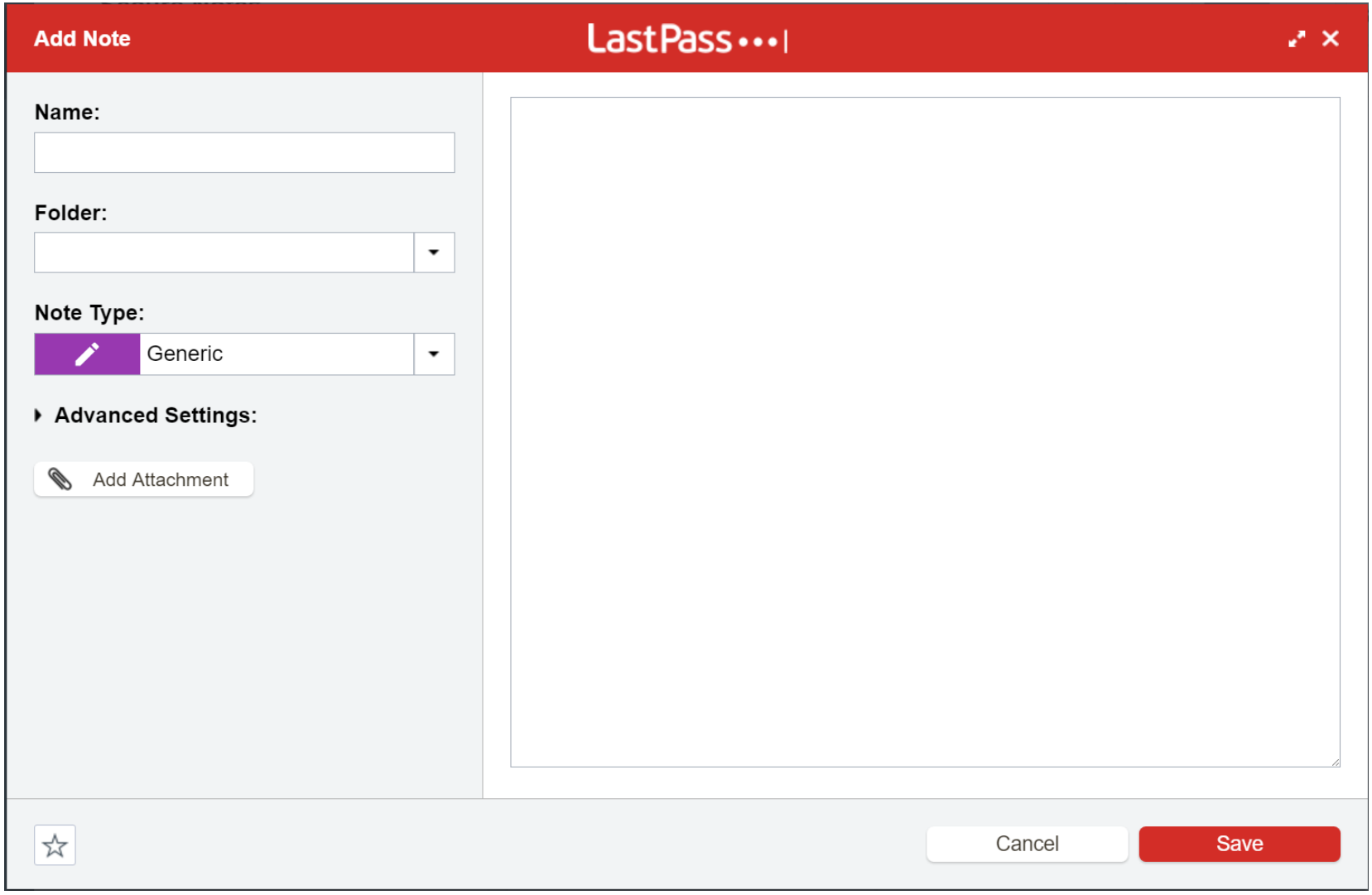
Carnegie Mellon University Information Security Office



LastPass Features

Carnegie Mellon University
Libraries

Carnegie Mellon University
Information Security Office



LastPass Features

Carnegie Mellon University Libraries

Carnegie Mellon University Information Security Office

LastPass •••| *Security Challenge*

90%	Top 2%	100%
Your Security Score	Your LastPass Standing	Master Password Score

Challenge your friends

Improve Your Score

Step 1 - **Change Compromised Passwords**

Auto-Change Password:

You have no compromised sites!

Password Generator: