Information Security Forum
Fall 2018

Gary McCrillis & Jon Vazquez
Information Security Analysts,
Cal Poly Information Security Office
Better Passwords, with LastPass and Duo
Ninjio Video
Passwords Are (Still) Hard

• Secure passwords are hard to remember.
• Should be unique per site, but often aren’t.
• Passwords are still used everywhere.
• Everyone has a horror story about passwords.
• Over 1 billion passwords breached by hackers.
Why Use A Password Manager?

• One password to remember.
• One thing to secure well.
• Auto-fills unique, secure passwords.
• Works great on Android and iOS.
• LastPass, purchased by Cal Poly, allows secure password sharing.
• LastPass link: lastpass.com
• Mac/iOS alternative: 1password.com
A Warning!

- Master Password MUST be remembered and kept secure.
- Lose your Master Password and you lose ALL your passwords.
- Reputable vendors cannot access your passwords.
- TIP: Print out your master password and keep it with you for a few days.
- TIP: Use Multifactor Authentication
LastPass & Duo Getting Started Guide

- Set up Duo on the Cal Poly Portal
- Official LastPass Getting Started Guide
LastPass Tips

• Install the iOS/Android apps and browser extensions.
• If you have many passwords in Chrome/Firefox, you can import them into Lastpass.
• Use LastPass to generate and fill in long, secure passwords for sites.
• Enterprise LastPass allows for simple password sharing.
Use Multi-factor/2-Step Verification

• Use Multifactor Authentication (MFA) for password manager and for email.
• Email is a common central point for many accounts (Netflix, bank, news site subscription, retirement account, etc.)
• No Google employee have been successfully phished with MFA in place since 2017.
• Cal Poly DUO provided for free to faculty/staff.
• Google 2-Step instructions link
Cal Poly Information Security Office
infosec@calpoly.edu

Report suspicious emails to abuse@calpoly.edu