Andrew McDonnell

Andrew solves tricky problems for a living as Vice President of Security Solutions with AsTech Consulting, and has been a Mac user since before the first time Apple was “doomed”.

MACTECH PRO EVENTS

Managing Security With the Growing Threat of Malware

MACTECH PRO EVENTS

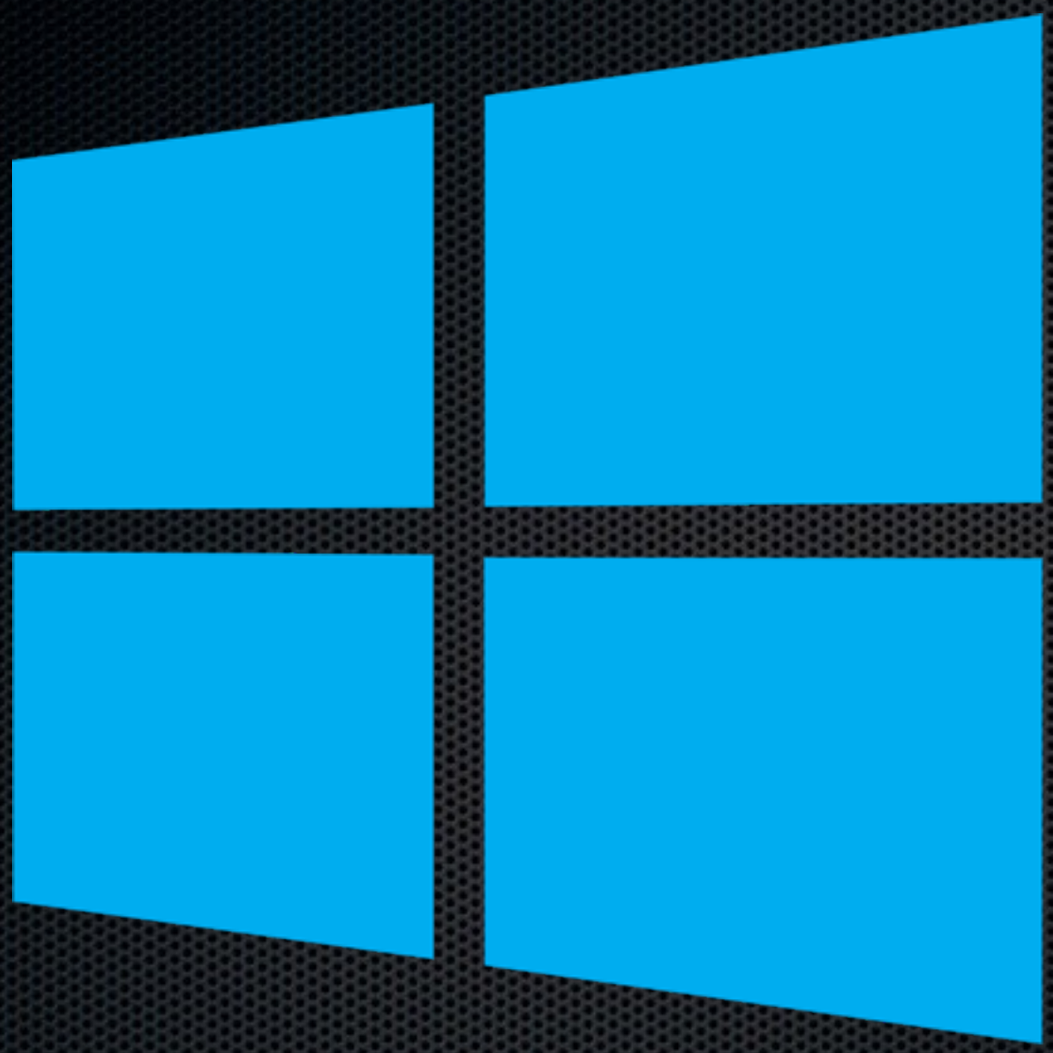
Wrong

Susceptibility

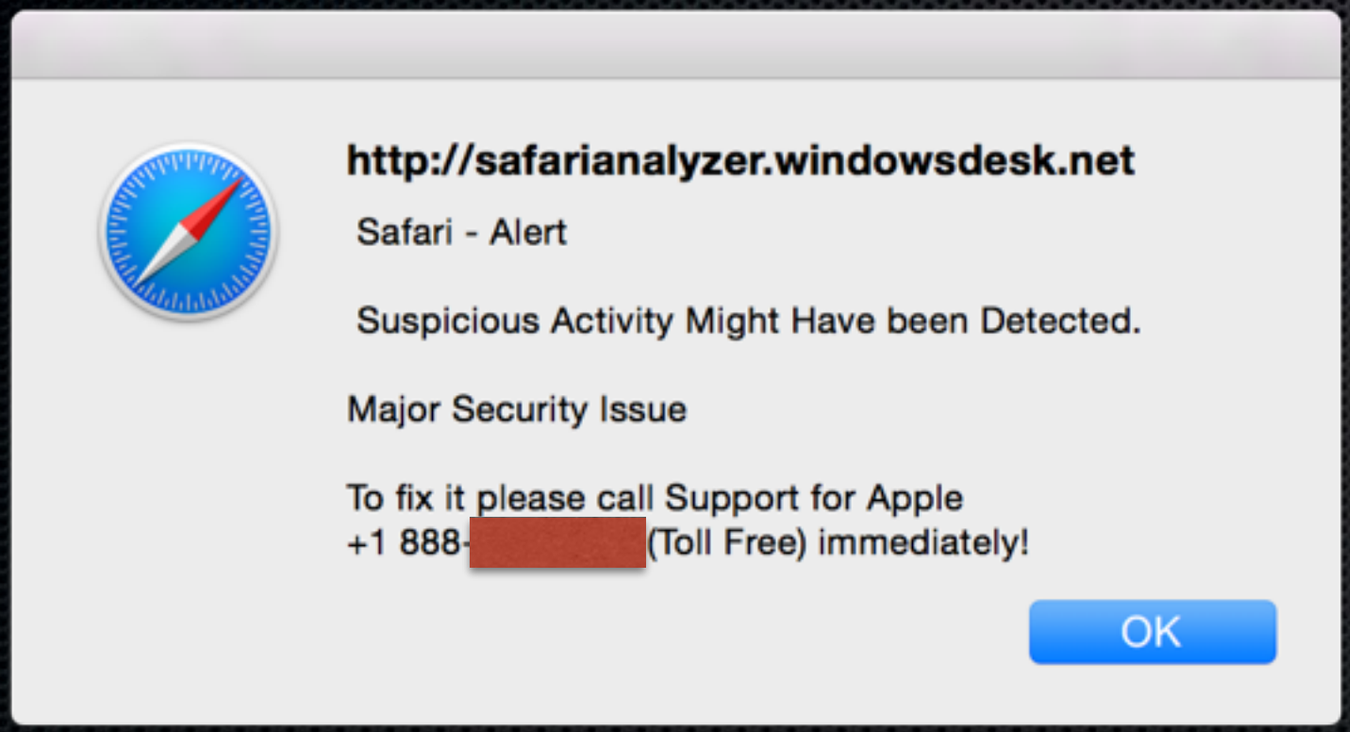
What's the difference?

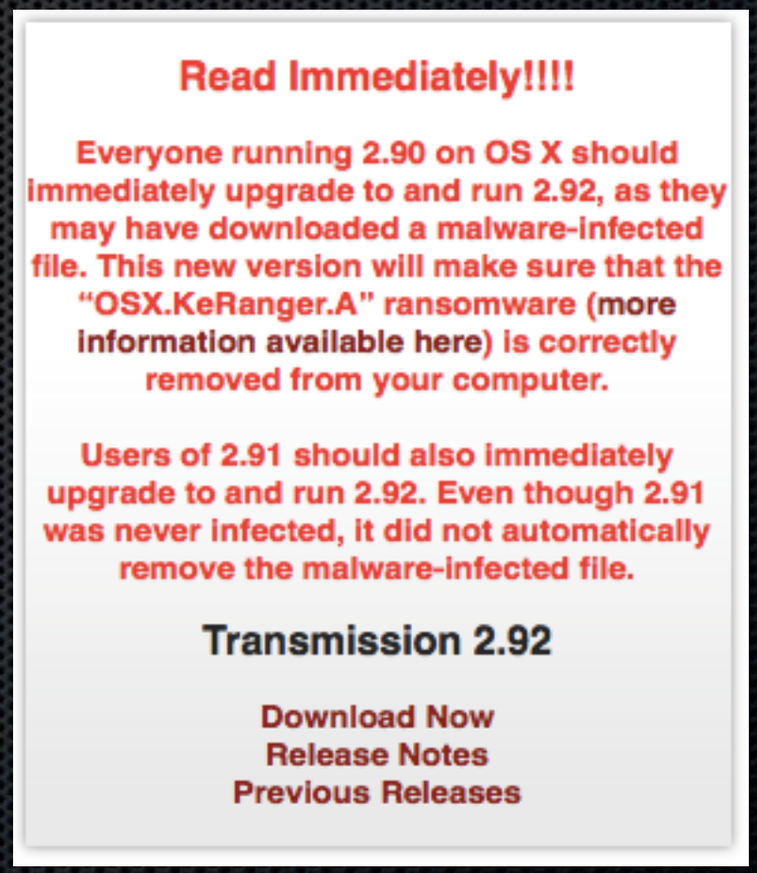
- Virus
- Adware
- Trojan
- Ransomware
- Windows Viruses

Not Immune

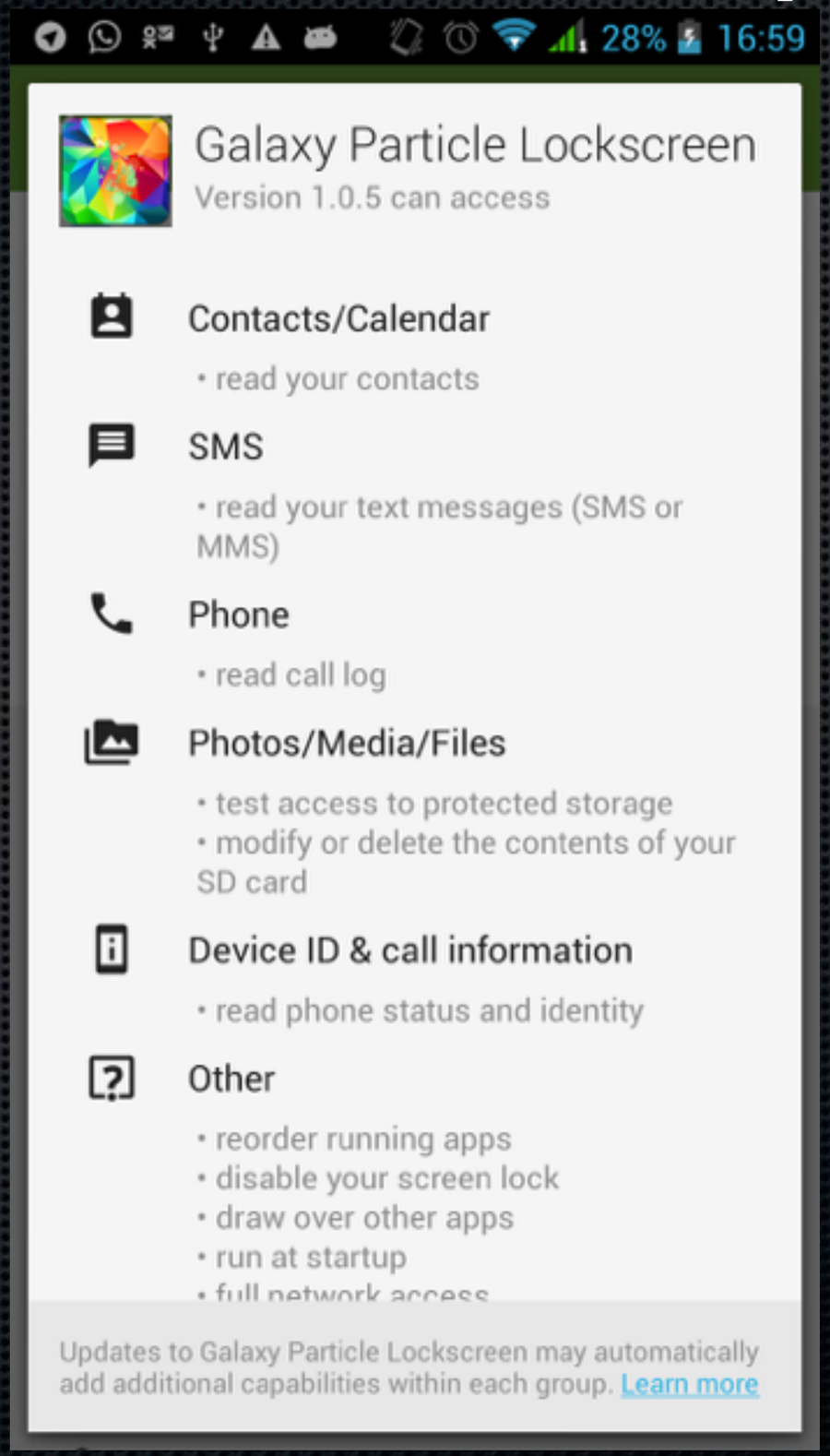


Also Not Immune





2.3% Immunity

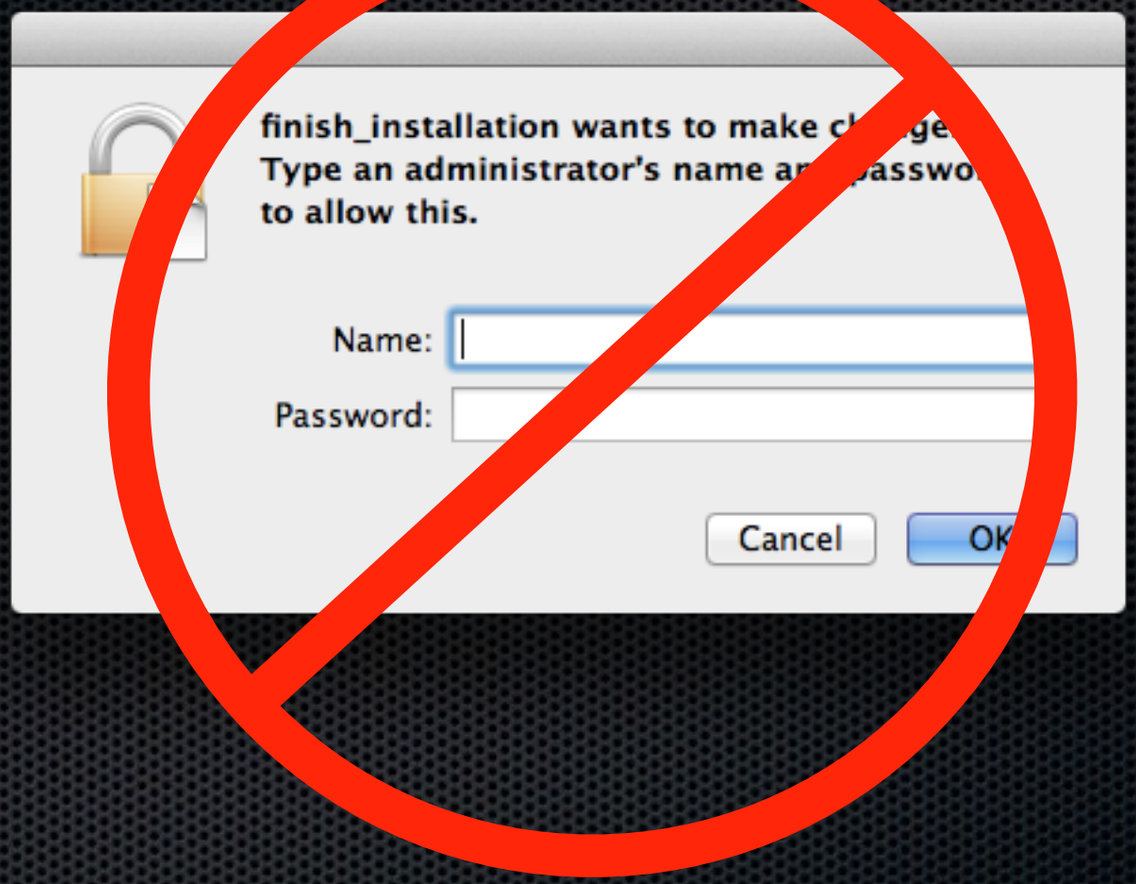


Trouble Brewing


I'm invincible

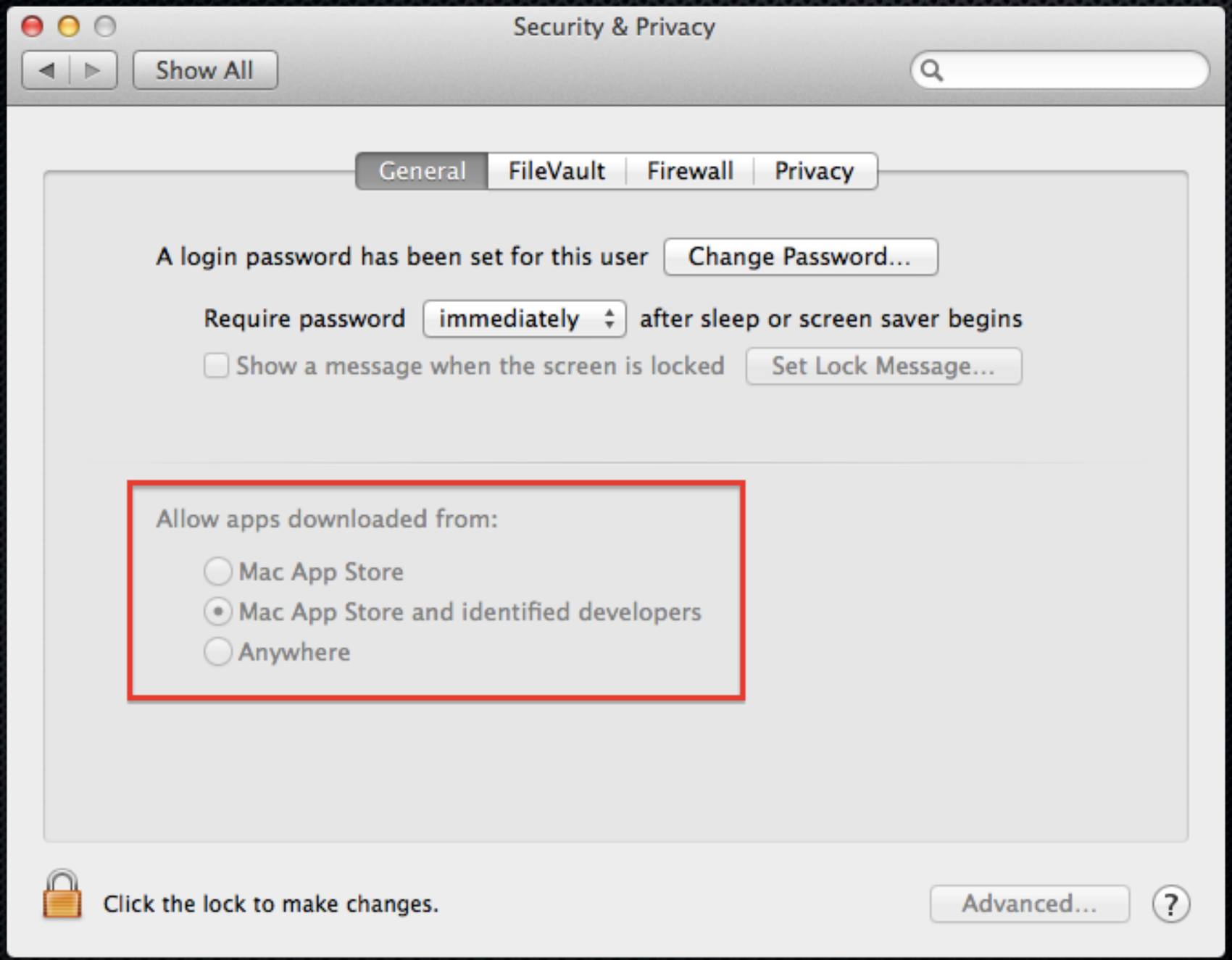
What Can I Do?

- User Education – Security Mindset
- Update Everything
- Protection
- Response
- Backups – Redundant & Offline


finish_installation wants to make ch ge
Type an administrator's name an passwo
to allow this.
Name:
Password:
Cancel
OK

Basic OS X Hardening

Basic OS X Hardening

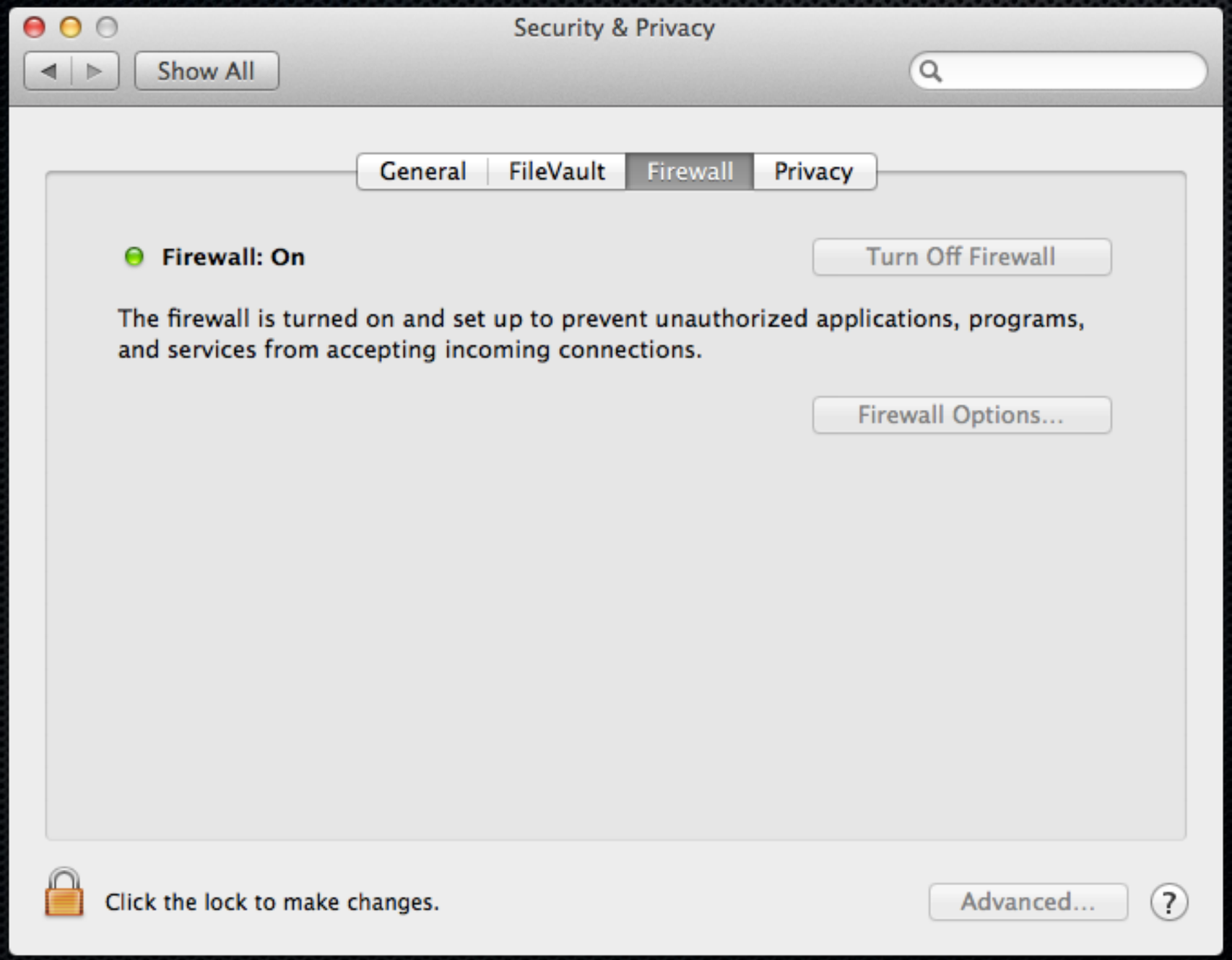


MACTECH

Basic OS X Hardening

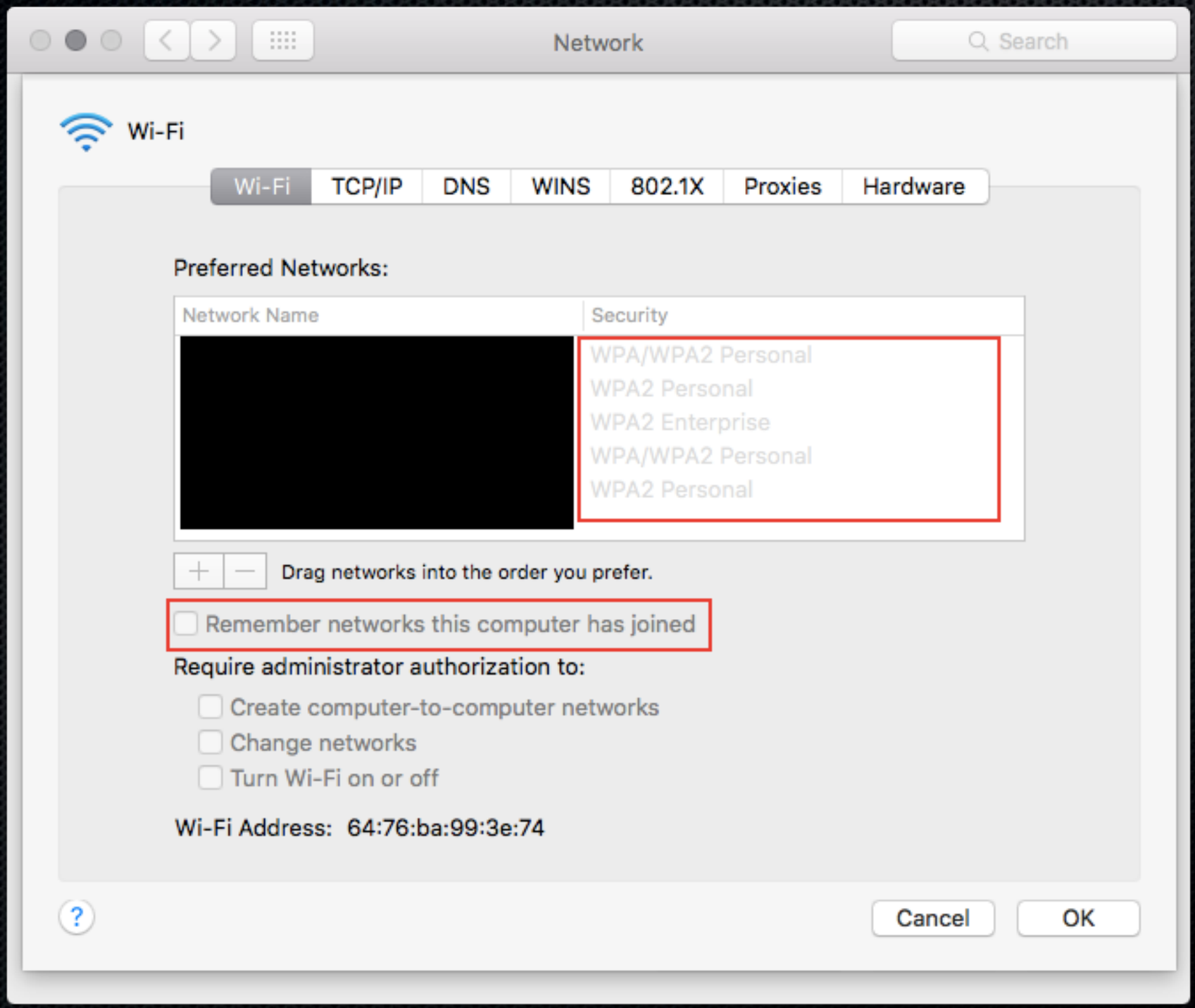
MACTECH

Basic OS X Hardening



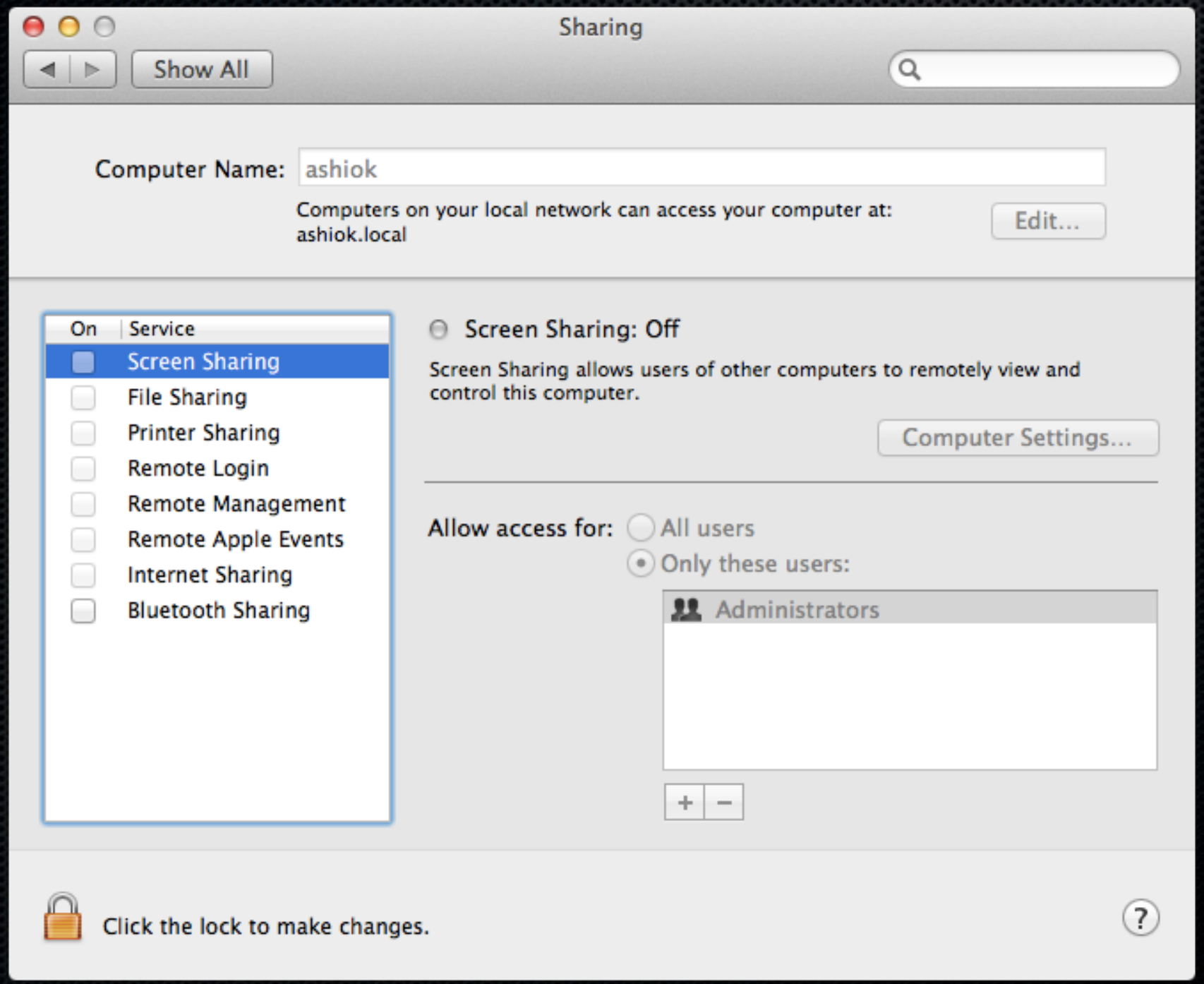
MACTECH

Basic OS X Hardening



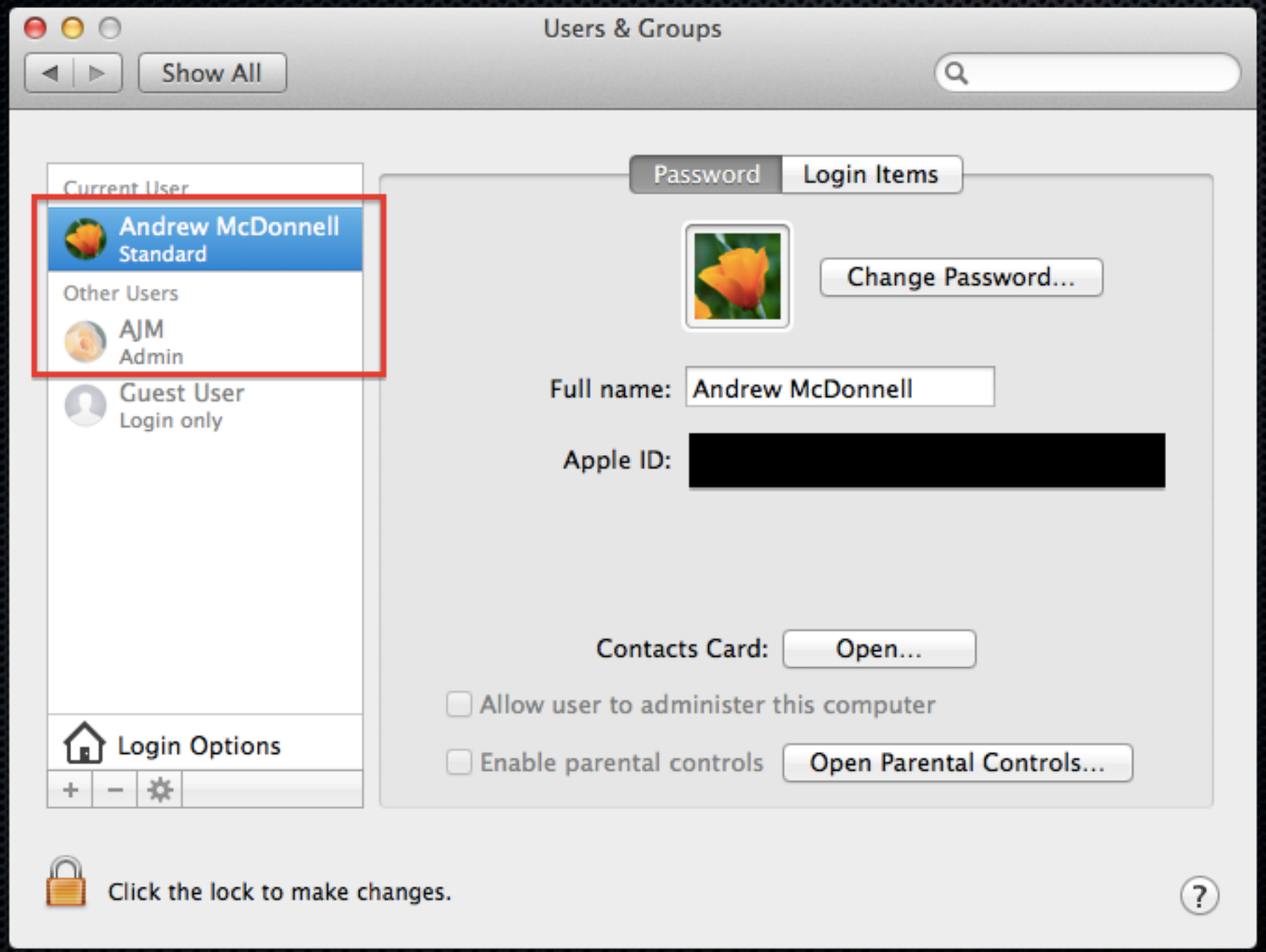
MACTECH

Basic OS X Hardening



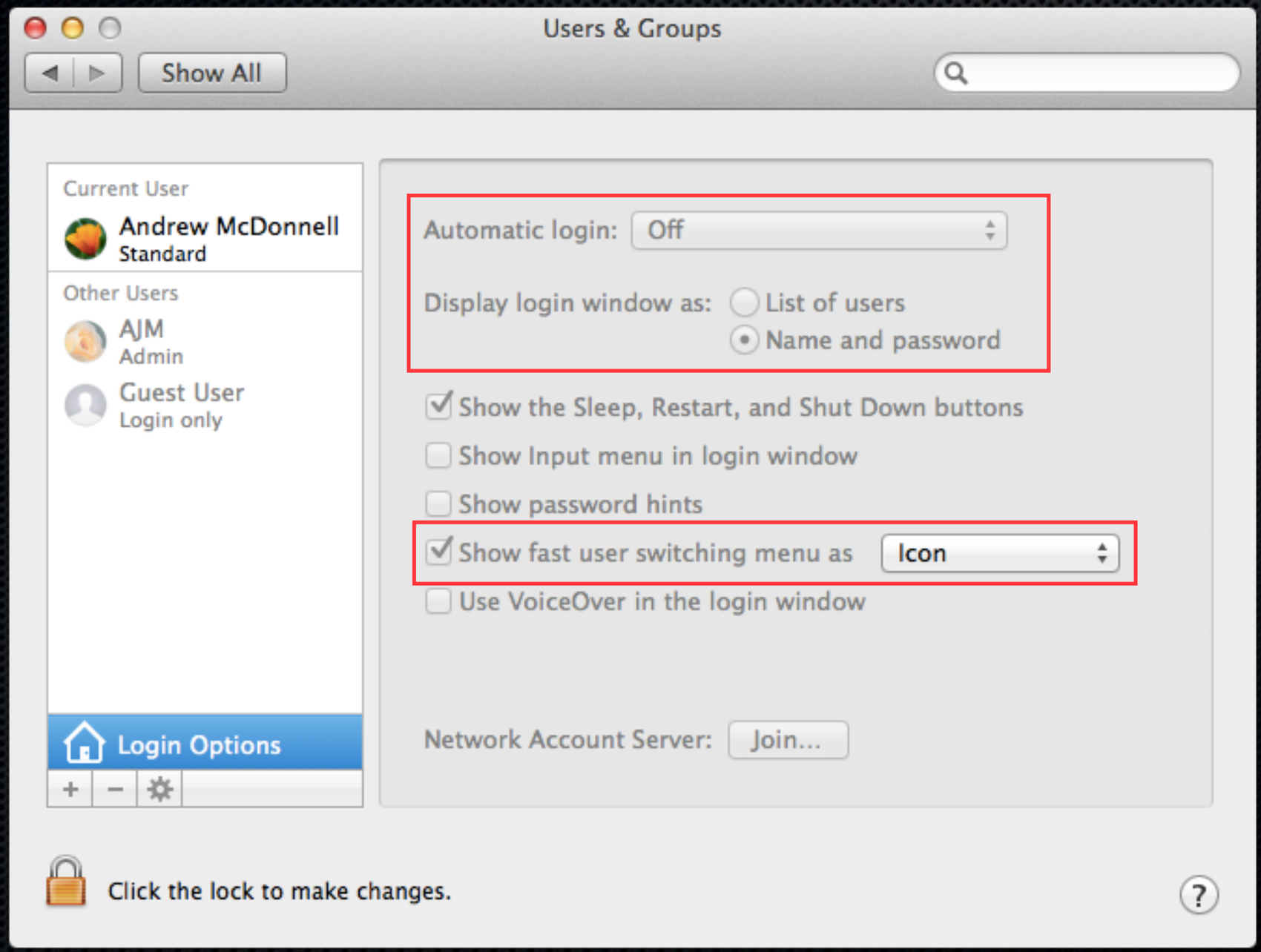
MACTECH

Basic OS X Hardening



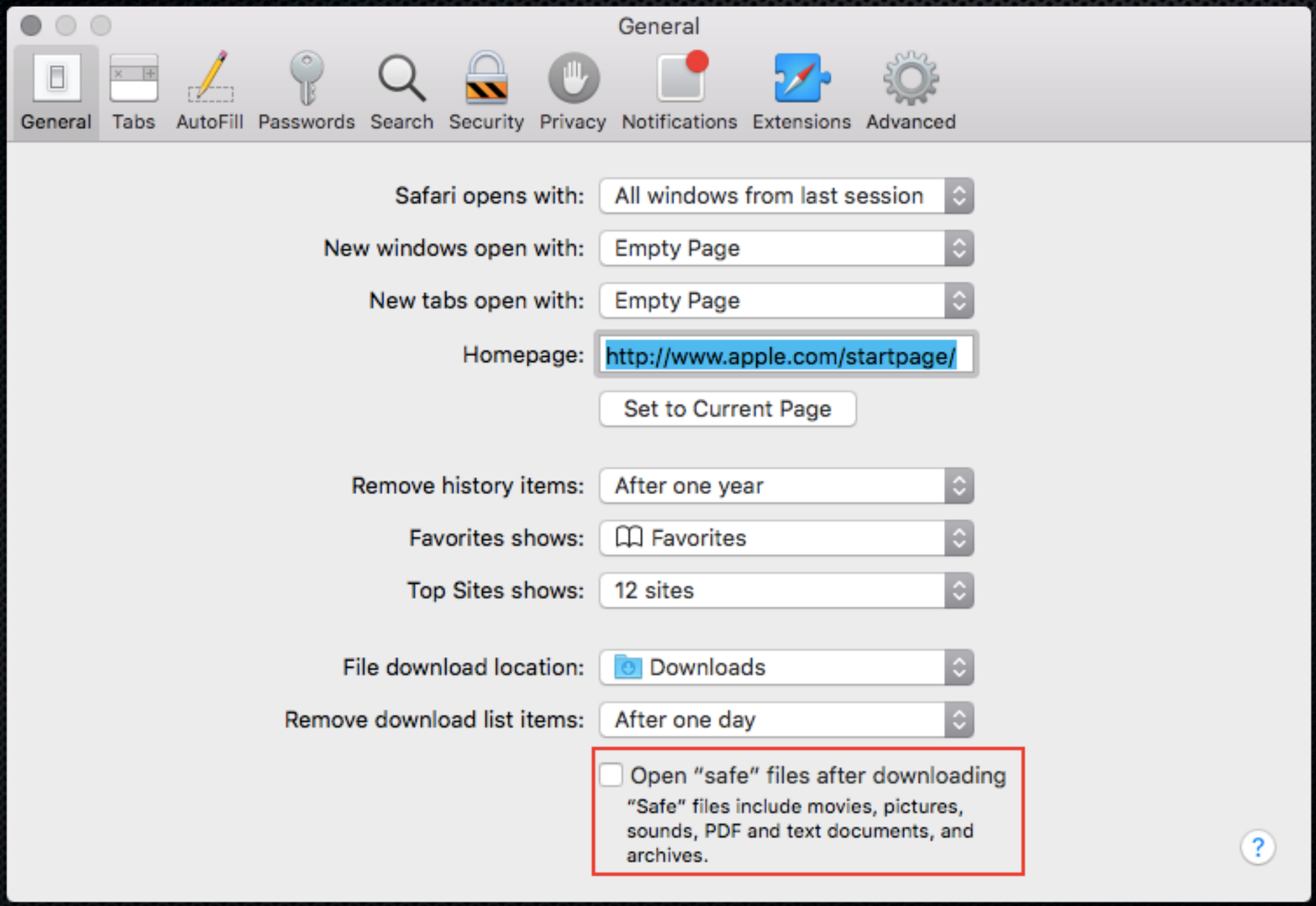
MACTECH

Basic OS X Hardening



MACTECH

Basic OS X Hardening



MACTECH

Get Rid of These

Microsoft® Silverlight™

Managing Endpoints

- Control Spectrum – Users ⟷ Administrators
  - Hands-off
  - Shared
  - Locked Down

- Endpoint Protection
  - Policies
  - NAC
  - Definitions
  - Central Management

Endpoint Protection Tools

- Active vs. Passive – Performance
- Apple
- Kaspersky
- Sophos
- McAfee
- Ghostery
- MalwareBytes

Impostors

- Genieo / InstallMac
- MacProtector
- MacKeeper
- Avoid good software from bad sources

More Resources

- thesafemac.com
- www.us-cert.gov
- cve.mitre.org
- schneier.com
- arstechnica.com/apple
- krebsonsecurity.com
- *astechconsulting.com*

Questions?

Andrew McDonnell
andrew@astechconsulting.com

MACTECH PRO EVENTS