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

Security, Viruses, and Malware.
It's real. It's now.
You need to take it seriously

MACTECH PRO EVENTS

My First Mac Virus

My First Mac Virus

Viruses, the history of viruses coming to our platform

- 1980's forward, Being an uninfected carrier
- 1990's forward, Word Macro Viruses
- AdWare: First appeared in 2012
- Malware: From the early 1980s.
- Trojan horses appeared on Mac in 2012 (Flashback Trojan)

What's the difference?

- Viruses
- MalWare
- AdWare
- Trojans
- Windows Viruses

Moving from complacent to vigilant one decade at a time

- Virus scanning software an Enterprise requirement
- Virus scanning software a best practice
- Virus scanning software, it may be necessary to protect productivity
- It finally really matters on a personal level

Statistics

- Estimated over 5% of iPhone users (globally) have jailbroken their devices
- Even non-jailbroken phones could be susceptible
- Millions of Macs are likely infected and people don't know (e.g., emails with Windows viruses).
- Likely a large portion of those Macs are infected and causing trouble
- Many Mac consultants think they know how to deal with viruses on a Mac but often don't

Developing a strategy

- Identify the problems
- Identify the best players in the field for Virus and Malware detection and removal
- Take a product you know personally and demo the product for the group
- Instill the Security Mindset

Password management

- Myth or Fact?
  - Requiring password changes every xxx days is a mistake, and causes other problems
  - You shouldn't use real words
  - Never write passwords down
- Reality and Best Practices

Complexity is everything.

- Go as long as you can 12, 15 and even 20+ characters
- Use a password manager -- choose what matches you best
  - 1Password
  - LastPass
  - iCloud Keychain
- Ok to keep notes in any SSL/encryption protected app: Notes, OneNote, etc…
  - Some people even use secure notes in Keychain
  - Beware of "replacing" the keychain, however

Avoiding Adware Scanner Utilities

- How bad is Genieo?
  - Genieo virus
  - Hard to remove. Proceed with caution
  - Utilities for removal
- MacProtector
- MacKeeper
- Avoid good software from bad sources.

Tools to use

- BitDefender Virus Scanner: Free
- Sophos
- McAfee

- Watchman Monitoring alerts
- Ghostery - https://www.ghostery.com/
- AdwareMedic - http://www.adwaremedic.com/index.php

VPNs: Why you need them

- Basic architecture
- Simplest implementation for a small business
- Using OS X Server to host a VPN
- Using a router to host a VPN

Firewalls

- How they work
- Often a simply way to keep out nasties
- Built-in to OS X
- Third party options

More Resources

- thesafemac.com
- www.schneier.com
- krebsonsecurity.com
- nakedsecurity.sophos.com/2011/10/03/mac-malware-history/
- *astechconsulting.com*

Questions?

Andrew McDonnell
andrew@astechconsulting.com

MACTECH PRO EVENTS