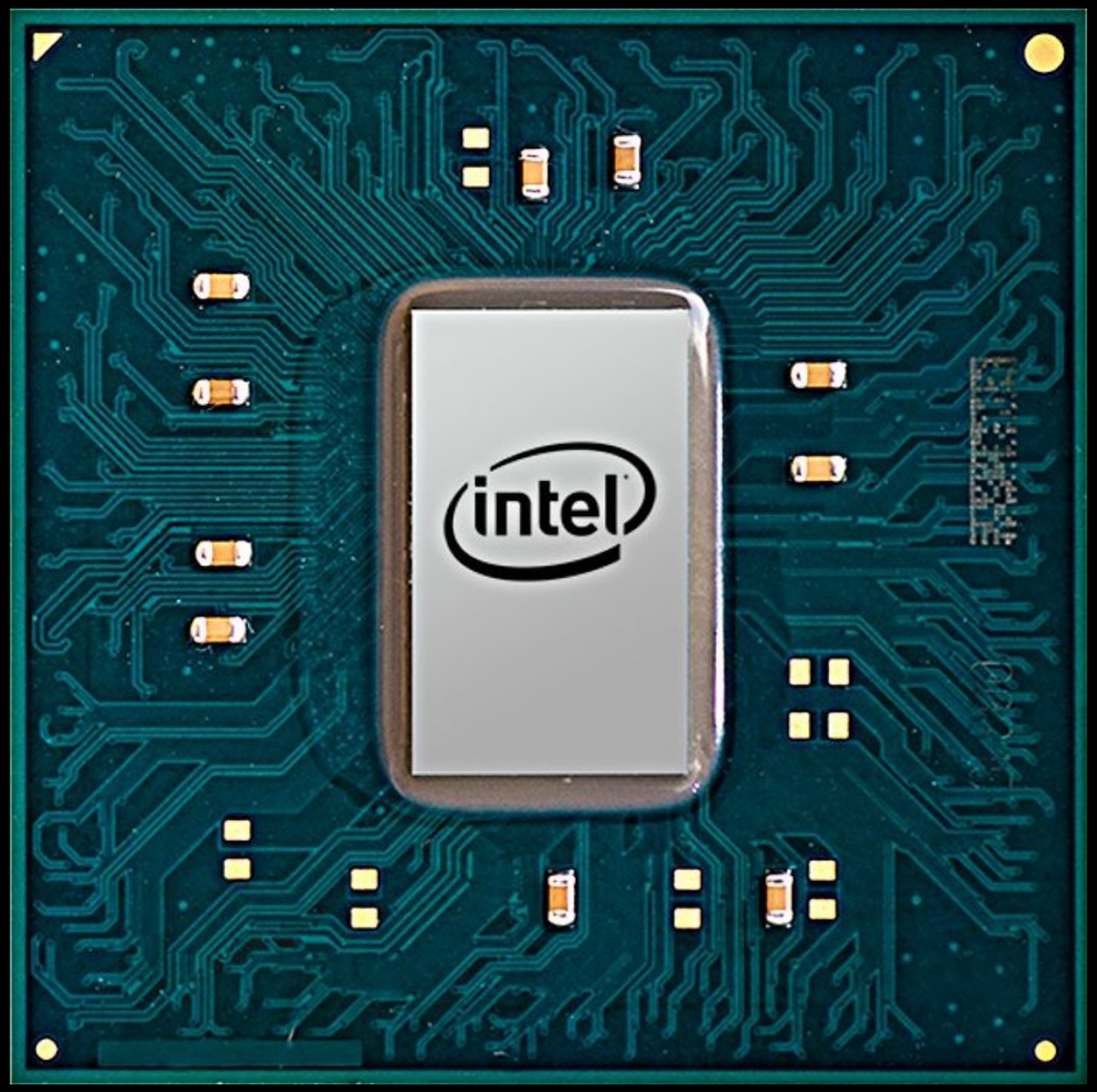
Meltdown & Spectre

Main Line Macintosh User Group
January 2018

Mike Inskeep
Gentle Computer Helpers
www.gentlehelpers.com
mike [at] gentlehelpers [dot] com
610-742-3927

Exploit Hardware Design



“These aren’t normal software vulnerabilities.... These vulnerabilities are in the fundamentals of how the microprocessor operates.”

- Bruce Schneier

Not Your Usual Vulnerability

- Rely on processor to function as designed
- Independent of the operating system
- Don’t depend on poor application security

Break Memory Isolation

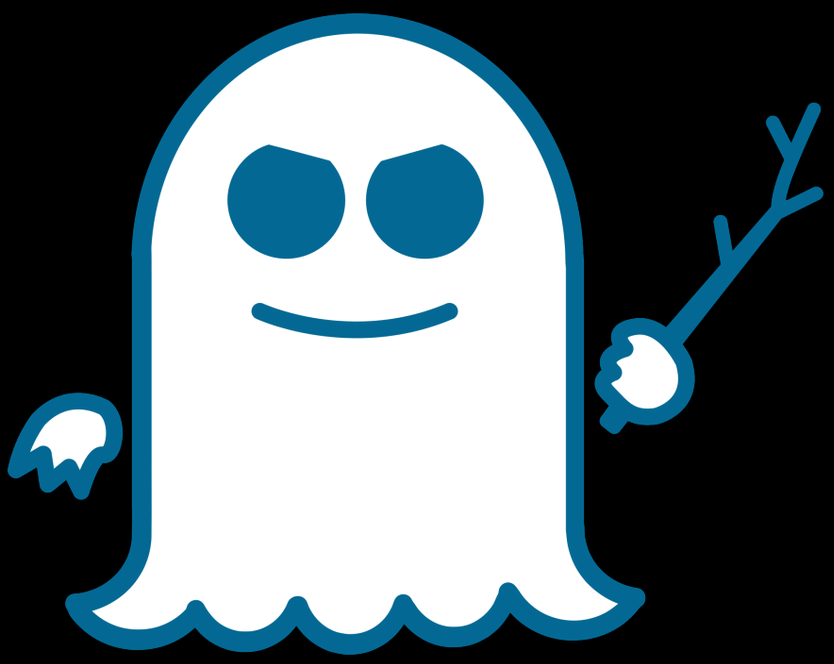
- Access privileged data stored in working memory
- Transmit this data via microarchitectural covert channel to outside recipient

Good News - Only Read Data

- Can’t change the contents of memory
- Don’t gain control of applications or the device

Meltdown

- Breaks isolation between user applications and the operating system
- Allows a program to access the data used by other applications and the operating system



Spectre

- Breaks isolation between user applications
- Best practice programming safety checks actually may make applications more vulnerable
- Harder to exploit; harder to mitigate

Meltdown Demo

https://www.youtube.com/embed/RbHbFkh6eeE

Affects Most Apple Devices

- All Macs
- All iOS devices (iPads, iPhones, iPods
- All Apple TVs

- Apple Watches *not* vulnerable

Detectable?

- Don’t know if there are active exploits
- Can’t tell if you’ve been exploited
- Anti-virus programs won’t detect them

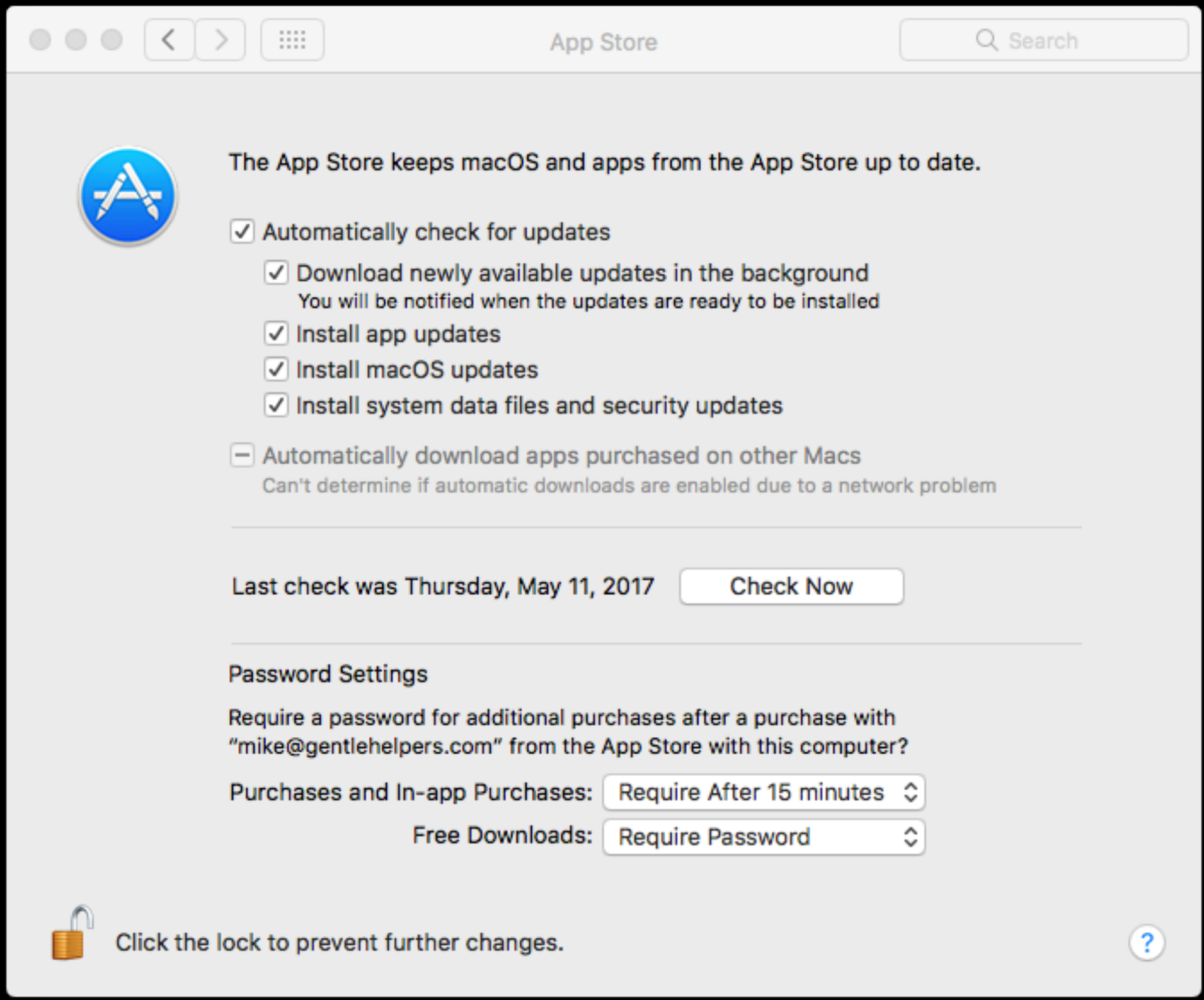
Update Operating System

- iOS 11.2.2
- macOS
  - 10.13.2, Supplemental Update
  - Security Update 2017-002 for 10.12
  - Security Update 2017-005 for 10.11
- tvOS 11.2

Installed App Running Malicious Code

- Get software from trusted sources
  - App Store
  - Secure (https://) developer site
  - Reputable retailer (Amazon, B&H Photo)
- Apply updates when available

Update Settings



Update Browsers

- Safari 11.0.2 for macOS 10.11+
- Firefox 57.04 for macOS 10.9+
- Chrome 64 when released 1/23

Turn on Site Isolation

Chrome

chrome://flags/#enable-site-per-process

Click on [Enable]

Firefox

about:config?filer=privacy.firstparty.isolate

Double-click to change value to true:

privacy.firstparty.isolate

Use Mail Application

- Viewing on webmail using browser could execute embedded javascript
- Microsoft Outlook creates HTML email

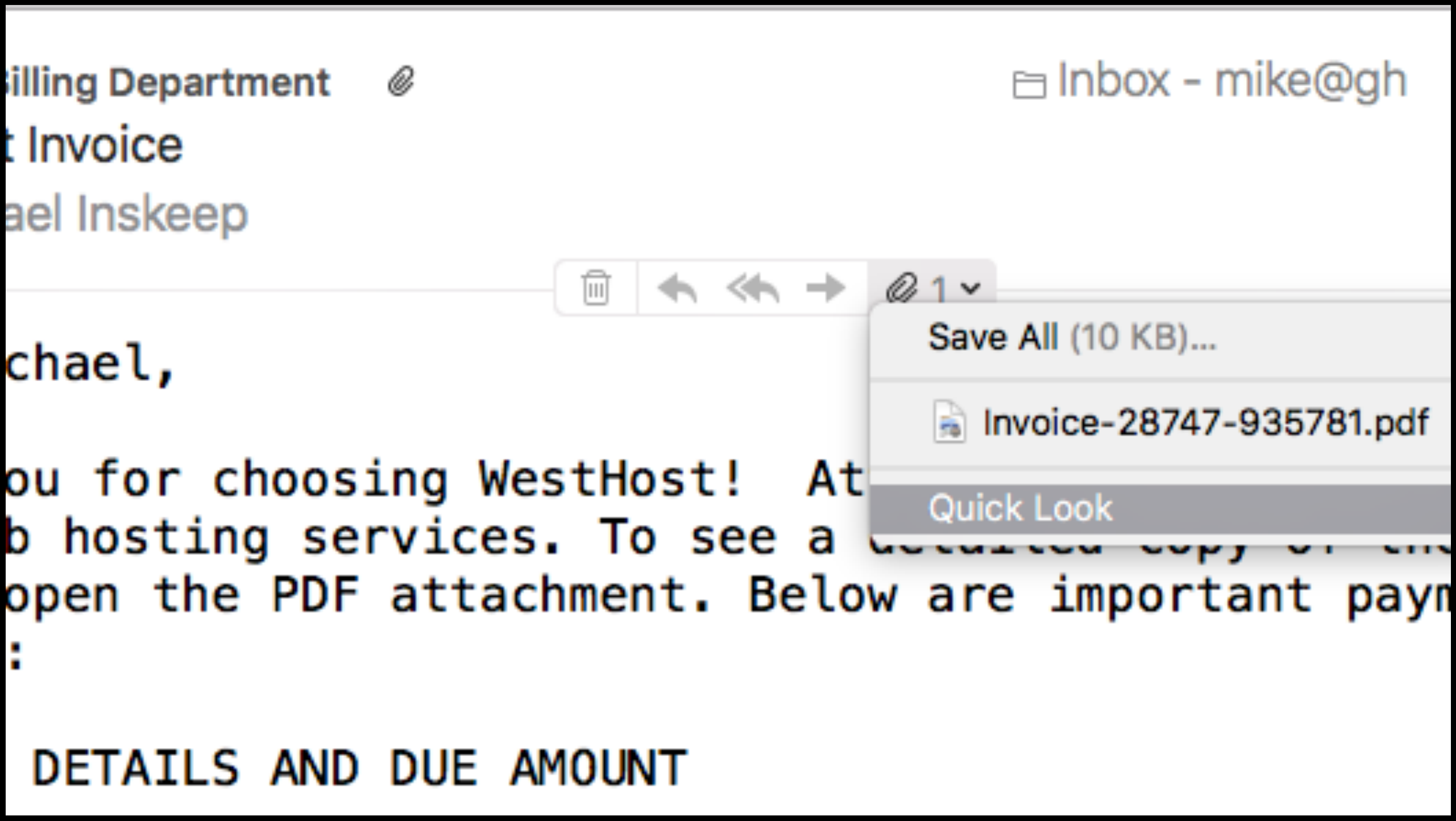
Beware of Email Links

- Slow down, pay attention.
- Confirm sender:
  - Hover over name
  - Click on the down arrow to the right
- Hover over link for URL (address)

Beware of Email Attachments

- Slow down, pay attention
- Confirm sender:
  - hover over name
  - click on the down arrow to the right
- Drag Word attachments to Pages to view

Use QuickLook



More Info

Researchers public info page:

https://meltdownattack.com/

Apple’s announcement:

https://support.apple.com/en-us/HT208394