

# Office 365 ATP

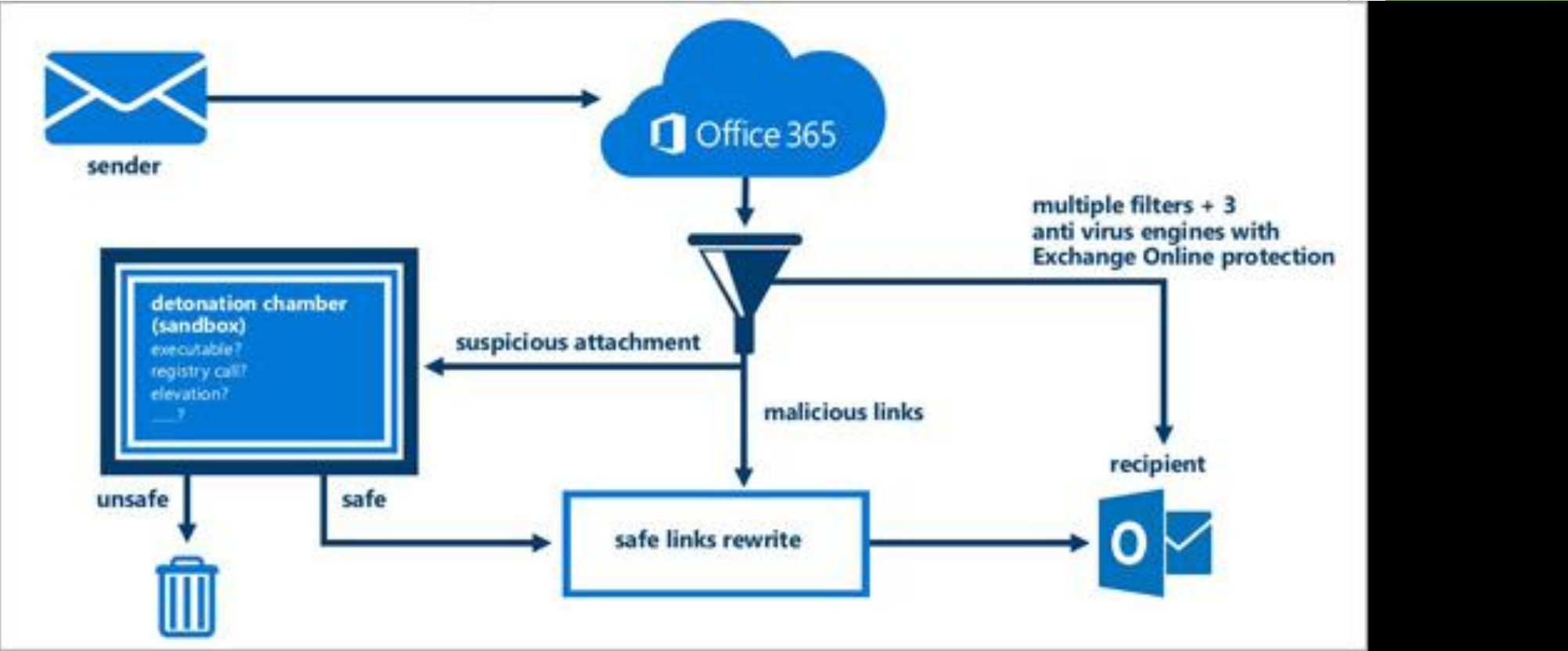
Advanced Threat Protection

From Microsoft

# What is ATP?

- ▶ Protects your email in real time against unknown and sophisticated attacks
  - ▶ Scans and blocks malicious attachments and links that otherwise may be undetected
- ▶ Provides rich reporting and tracks links in messages
  - ▶ We will gain critical insights into who is being targeted within the state and the category of attacks you are facing.
- ▶ We own it!
  - ▶ SITSD added ATP licensing to the State of Montana Microsoft Enterprise Agreement during the 2017 Renewal
  - ▶ It is user based and compliments the SPE E3 subscription

# Here's how it works



# What will you see when you hover over a link in email?

- ▶ Links are stripped and replaced with safelinks.protection.outlook.com.



The screenshot shows an email interface with a dark header bar containing "Bing Maps" and "Action Items". A red ZDNet logo is visible on the right. A hover tooltip is displayed over a link, showing the following text:

```
https://na01.safelinks.protection.outlook.com/?  
url=http://enews.zdnet.com/ct/43373057:  
w-du5renn:m:1:716680996:  
ec8fa06d73c81bb75d50f36539b58eab:r:  
20092556086505491304590427043252&data=0  
2|01|jtuman@mt.  
gov|f06b72c8f1c64fe30abf08d4cf84861d|07a94c  
98f30f4abbbd7ed63f8720dc02|0|0|63636161546  
8738196&sdata=8ka7qqrftomlb6avn/  
iehxfq+fwuzdlvs0bn+nbwxce=&reserved=0  
Click or tap to follow link.
```

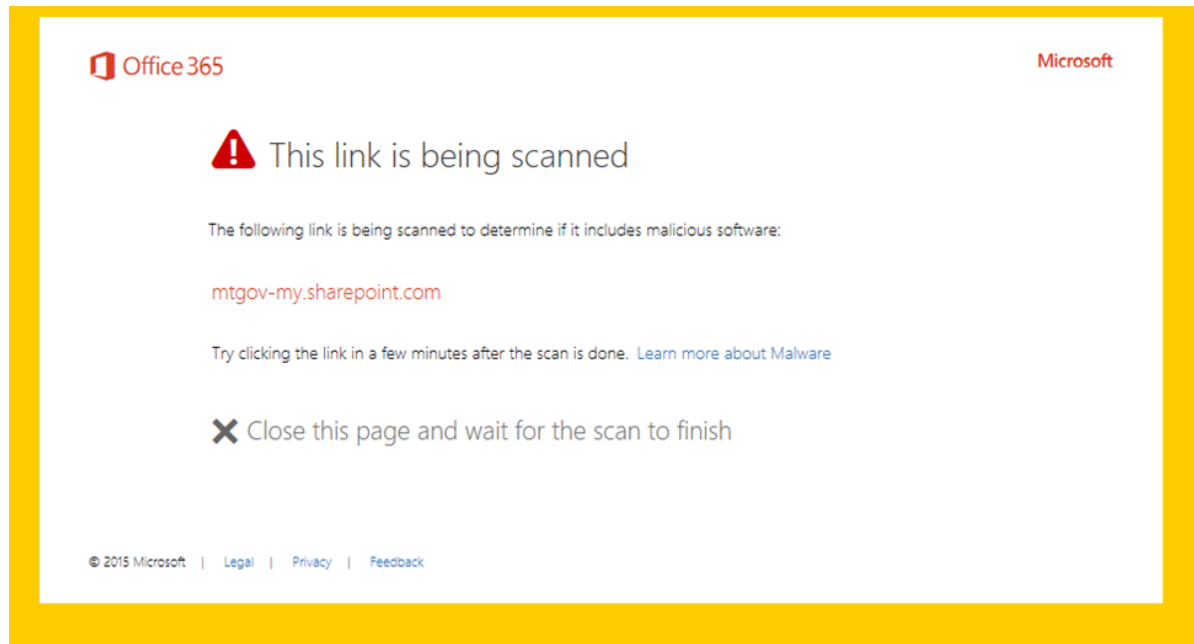
Below the tooltip, the main content of the email is visible, featuring the ZDNet logo and the text:

**ZDNet Must-Read News**  
July 20, 2017

**Justice Department, Europol tout AlphaBay takedown, but 'keenly aware' challenges remain**

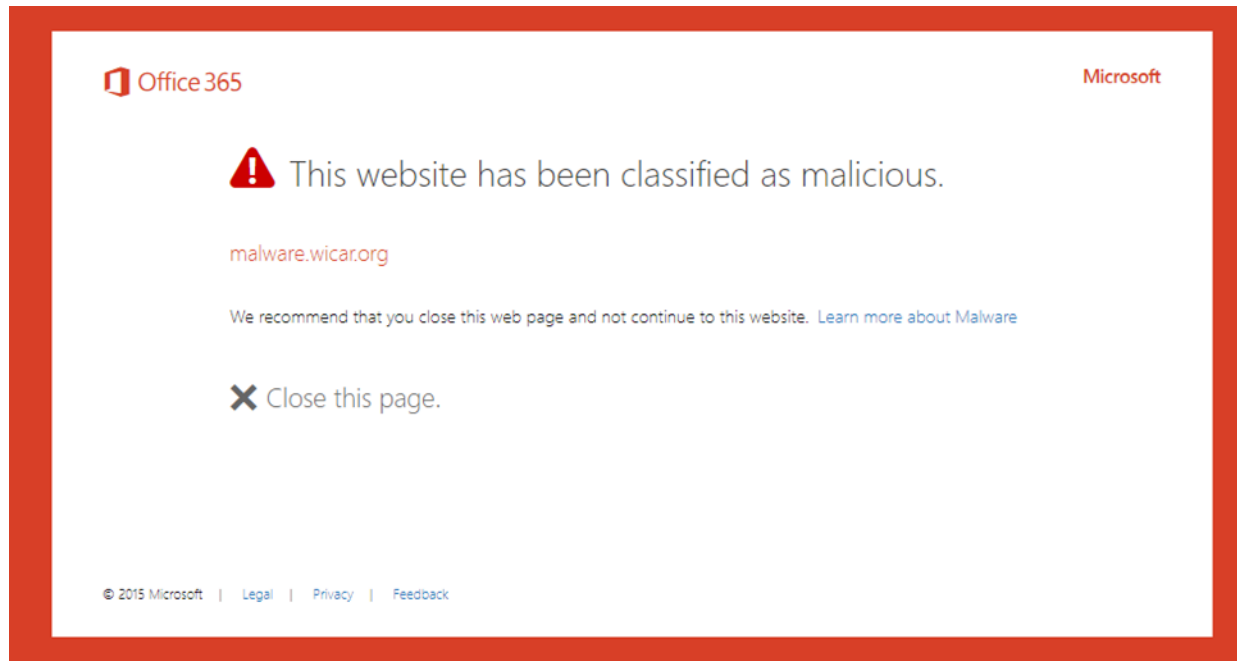
# Managing user expectations

- ▶ E-mails from external sources (including emails from sharing One Drive files between state employees) are scanned. If a user clicks on a hyperlink when a new e-mail arrives and ATP has not been able to scan it, they will be directed to this page in their browser.



- ▶ Although not typical, ATP may delay messages that contain attachments up to 30 minutes. This also applies to e-mail that contain images or signature lines, which are considered as attachments.

# What happens when a malicious attachment or link is found?



# Timelines

- ▶ SITSD went live with ATP 8/7/2017
  - ▶ No reported issues
- ▶ All mailboxes 10/2/2017

ATP



Questions?