

The Kobayashi Maru Dilemma



Dr Morton Swimmer

Andrew Lee

Nick FitzGerald

Trend Micro

ESET

Independent Consultant



Introduction

- What is the Kobayashi Maru dilemma?
- A few Words of history
- Fighting back
- (Anti-)Postel Thesis
- Flash in the pan?



<https://www.youtube.com/watch?v=8N-H1lz3OJ4>

The Best Thing About Office 97...

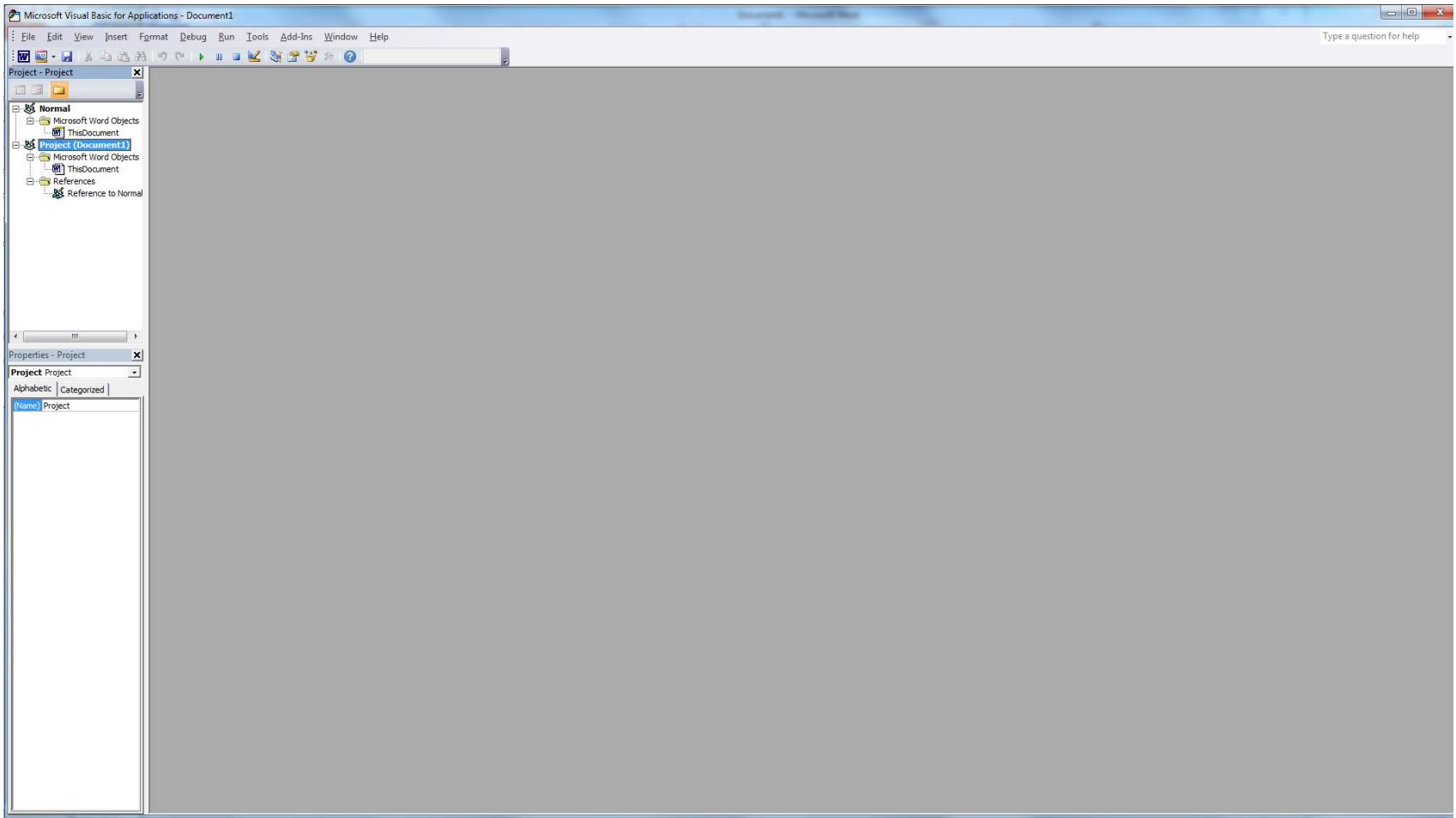
It looks like you're writing a letter.

Would you like help?

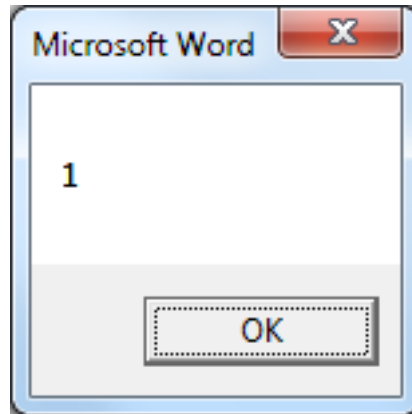
- Get help with writing the letter
- Just type the letter without help
- Don't show me this tip again



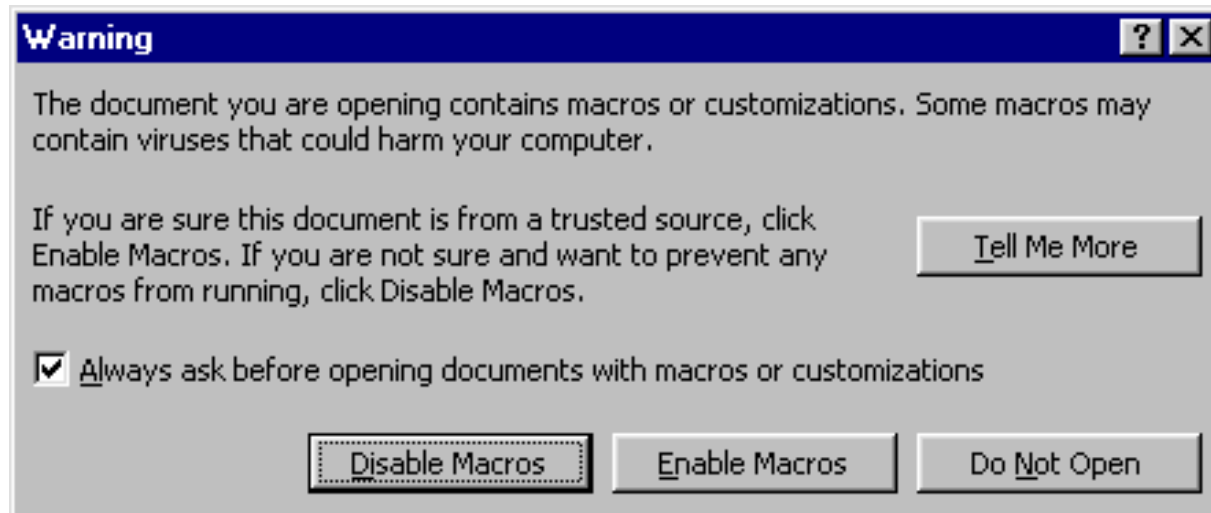
...OK, but Seriously



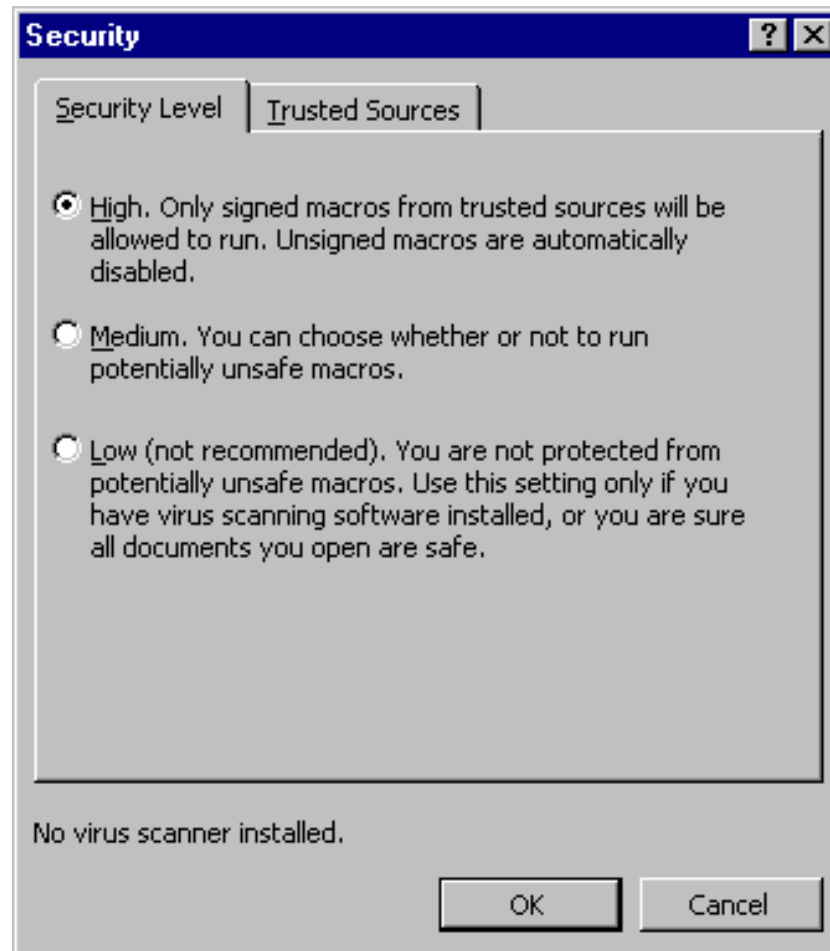
The Worst Thing About Office 97...



...OK, but Seriously



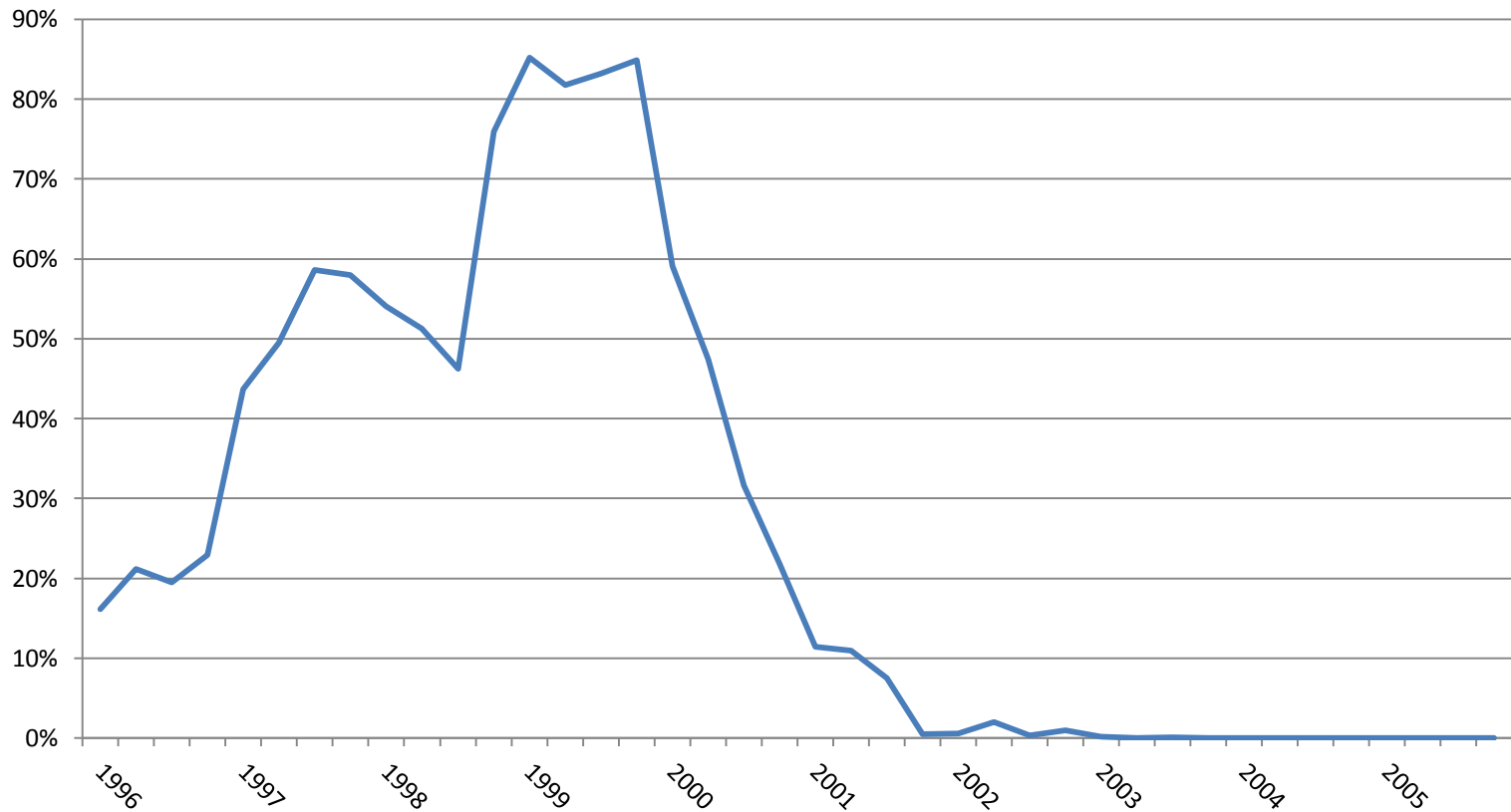
The Best Thing About Office 2000



And...



Prevalence of Macro Malware



*Data collated from Virus Bulletin "Prevalence Tables",
and kindly supplied by Szappanos Gabor, Sophos.*

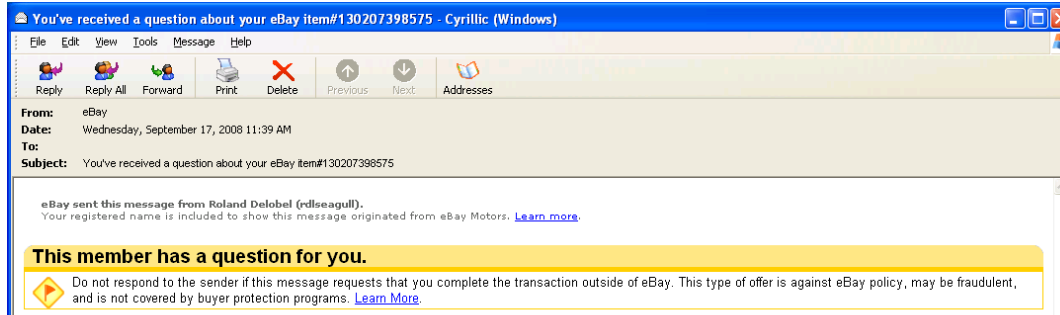
So...

- Good guys (Microsoft!?!?!? 😊) **1**
- Bad guys (macro malware writers) **Nil**

Other Security Game-changers?

- ASLR
- Encryption
- Two-factor Authentication
- CAPTCHA
- Tar-pitting
- Economics
 - Taggants
 - ChronoPay shutdown

What About Fighting Back?



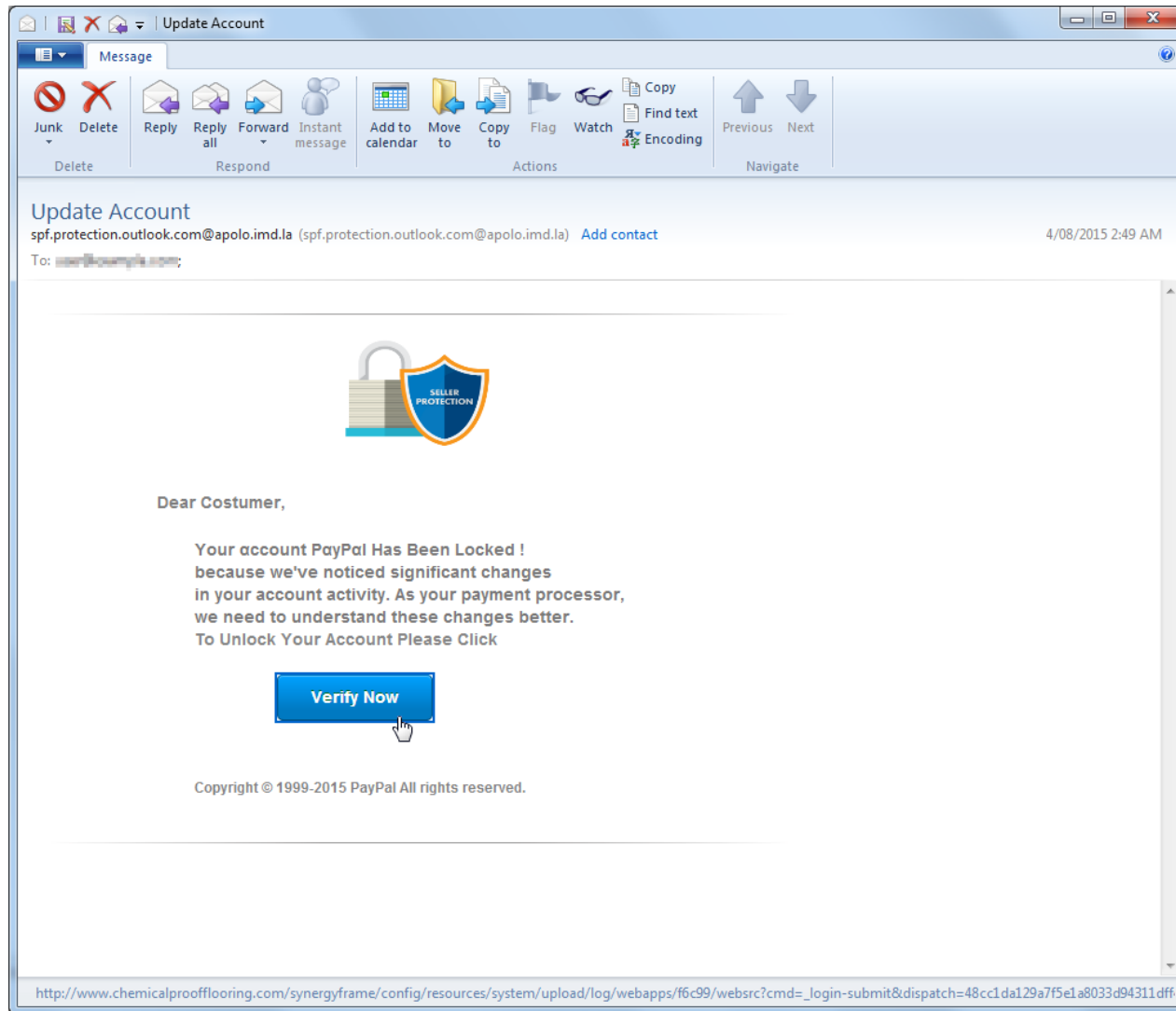
ftp://test:test@83.235.30.140/.ws/ehayISAPIdllSignInruhttpwwwwehaycomtrksidm.html



You Have User Credentials, So...

- Is it OK to delete the phishing page, or replace it with a “harmless” warning page?
- What about logging into the site’s hosting control panel and “just looking around”?
- What about copying other files than those accessible via FTP?
- What about changing the account password and/or owner’s email address?

What About Fighting Back?



The screenshot shows an Outlook window titled "Update Account". The message is from "spf.protection.outlook.com@apolo.imd.la" (spf.protection.outlook.com@apolo.imd.la) and is dated "4/08/2015 2:49 AM". The recipient is "user@company.com".

The message content includes a logo with a padlock and a shield labeled "SELLER PROTECTION". The text reads:

Dear Customer,

Your account PayPal Has Been Locked !
because we've noticed significant changes
in your account activity. As your payment processor,
we need to understand these changes better.
To Unlock Your Account Please Click

Below the text is a blue button labeled "Verify Now" with a mouse cursor pointing to it.

At the bottom of the message, it says: "Copyright © 1999-2015 PayPal All rights reserved."

The footer of the Outlook window shows a URL: http://www.chemicalproofflooring.com/synergyframe/config/resources/system/upload/log/webapps/f6c99/websrc?cmd=_login-submit&dispatch=48cc1da129a7f5e1a8033d94311.dff



Log in to your account

Email address

Password

Log In

[Forgot your email address or password?](#)

Sign Up for Free

We've got your back.

Shop with peace of mind with our Buyer Protection policy. You're protected if your eligible purchase doesn't arrive or match its description.

You're in control.

Simply add your credit or debit cards to start shopping. Plus, earn your card reward points on purchases at your favorite stores.

You Have the URL, So...

- Is it OK to “dig around” via directory traversal?
- You might find something interesting, like the phishing kit
- Or a data drop file
- Or you might even find a shell...
- ...if so, is it OK to use that to dig even deeper?

Demo...

- [switch to browser and demo on an offline copy of this phishing site – indexing was enabled exposing a web shell]

So, Was that OK?

- Dan Cuthbert convicted for “unauthorized access” under UK Computer Misuse Act for URL truncating
- Andrew Auernheimer (a.k.a. weev) – Automated a download of the AT&T list of iPad owners – exposing 114K records including Military, Celebrity and Government
 - Sentenced to 41 Months in Federal prison and a \$73K fine

Postel Thesis

- Jon Postel, original RFC Editor
- Formulated the **robustness principle** (often called **Postel's Law**) stating:
an implementation should be conservative in its sending behavior, and liberal in its receiving behavior
- Basically it is the “anti-engineering” thesis:
it's good enough if it works (for some undefined value of “works”)

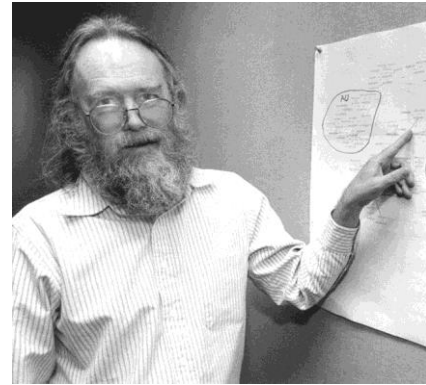


Photo by Irene Fertik, USC News Service.
Copyright 1994, USC.

Anti-Postel Thesis Examples

- Strict SMTP implementations drop a lot of spam *because of* their strictness
- Greylisting drops a lot of spam by not being “too willing” to be helpful

Other Anti-Postel Thesis Examples

- Any suggestions?

Google Freezes Flash Ads in Chrome


EXTREMETECH SEARCH [f](#) [t](#)

[Computing](#) [Mobile](#) [Internet](#) [Gaming](#) [Electronics](#) [Extreme](#) [Deals](#)

[HOME](#) > [COMPUTING](#) > [CHROME WILL SOON PAUSE AUTO-PLAYING FLASH ADS BY DEFAULT](#)

Chrome will soon pause auto-playing Flash ads by default

By Joel Hruska on June 6, 2015 at 10:24 am | [31 Comments](#)




Share This article

Chrome developers have announced that an upcoming version of Chrome will prevent video ads from automatically playing when a website loads. The new feature has already been pushed out to beta builds and can be manually enabled by opening Chrome's content settings and adjusting the plugin content options. This push comes as part of an overall effort to improve Chrome's performance on modern laptops.


Last year, Chrome was dinged by the discovery that the browser would set the CPU clock interval as low as 1ms, waking the chip far more often than is necessary in order to improve responsiveness, but at the cost of battery life. That issue was apparently fixed by a browser update earlier this year, but Google has evidently been looking for other ways to improve laptop power consumption. Auto-playing flash video, of course, isn't just a battery life issue — it's extremely annoying to have multiple tabs start playing their own audio streams automatically.

This new feature doesn't prevent the ad from loading, it just doesn't play the ad unless the user manually chooses to do. The feature is controlled from within Chrome's preferences, as shown below:


Promoted Stories



Wer hat schon einmal von Lungenhochdruck gehört?
[Mediaplanet](#)



7 Awesome German Words We Should Be Using In English
[Babbel](#)



Facebook CSO: Adobe Should Kill Flash



Alex Stamos
@alexstamos



It is time for Adobe to announce the end-of-life date for Flash and to ask the browsers to set killbits on the same day.

RETWEETS 2,450
FAVORITES 1,469



12:00 PM - 12 Jul 2015



Flurry of Flash Flaws Flanked in Firefox

NEWS

Mozilla blocks all Flash in Firefox after third zero-day



Automatically blocks even the current version of Flash patched July 8; users can sidestep the ban after seeing a warning



By Gregg Keizer

FOLLOW

Computerworld | Jul 14, 2015 3:19 AM PT

RELATED TOPICS

Security

Mozilla on Monday began blocking all versions of Adobe Flash Player from running automatically in its Firefox browser, reacting to news of even more zero-day vulnerabilities unearthed in a massive document cache pilfered from the Italian Hacking Team surveillance firm.

MORE LIKE THIS



Adobe patches Flash to quash last two zero-days unearthed in Hacking Team's...



EVERYBODY HATES FLASH
Adobe Flash must die, die, DIE. Firefox shoots gun loaded by Facebook (and...

Some perspective on Flash Player bugs

on IDG Answers →

If I buy a Chromebook and can't get to grips with OS can I convert to windows?

Facebook's Apr-Jun 2015 10-Q Filing

- **Risks Related to Our Business and Industry**

...rely on software that is highly technical, and if it contains undetected errors **or vulnerabilities**, our business could be adversely affected.

... Errors, **vulnerabilities**, or other design defects

Facebook's Apr-Jun 2015 10-Q Filing

Risks Related to Our Business and Industry

... For example, social games on Facebook rely on Adobe Flash, which games are currently responsible for substantially all of our Payments revenue. In July 2015, certain vulnerabilities discovered in Flash led to temporary interruption of support for Flash by popular web browsers. If similar interruptions occur in the future and disrupt our ability to provide social games to some or all of our users, our ability to generate Payments revenue would be harmed. ...

Amazon Advertising Joins In Too

[Home](#) > [Ad Specs and Policies](#)

Technical guidelines

Beginning September 1, 2015, Amazon no longer accepts Adobe Flash (swfs) for rendering display ads on Amazon.com, AAP, and various IAB standard placements across owned and operated domains.

This is driven by recent browser setting updates from Google Chrome, and existing browser settings from Mozilla Firefox and Apple Safari, that limits Flash display ad capabilities displayed on web pages. This change ensures customers continue to have a positive, consistent experience on Amazon, and that display ads function properly for optimal performance. Note that the updated policy does not impact video content or video advertising.

RIP Flash?



Questions?

Anything Further?

- Find Morton and chat
- Watch Martijn's blog for announcement next week