# Bug 1053890 - [UX] define user-experience when downloads are detected as malware

Prepared by Sevaan Franks and the Firefox UX team





Firefox uses Google's Safe Browsing tool to identify unsafe websites and notify users so they can protect themselves from harm. The service allows us to flag malicious downloads that can hurt users computers.

Now the Safe Browser program has expanded to also flag any "Potentially Unwanted" downloads that may be dangerous to users.

The work in this document shows a revised UX for malicious files, and introduces how potentially unwanted files should be handled as well.





# Note: Testing Malware Downloads

The European Institute for Computer Antivirus Research (EICAR) and Computer Antivirus Research Organization (CARO) have developed a test file to trigger malware alerts which can be downloaded here: <u>http://www.eicar.org/85-0-Download.html</u>



Instead of using real malware, which could do real damage, this test file allows people to test anti-virus software without having to use a real computer virus.



following error message in the downloads panel/window:



eicar\_com.zip llocked: May contain a virus or spyware — eicar.org — 11:0...

Show All Downloads

Right-clicking on the file allows a user to remove the item from their history, go to the download page, copy the download link, and clear the entire list of downloads.

**Problems**:

- We don't educate/inform the user as to why a download was blocked
- We don't offer a way to unblock the file

# If a user downloads a file that contain malware, Firefox blocks the file and displays the

# **Design Principles**

### Earn and keep my trust

Look legitimate and polished Perceived trustworthiness is just as important

Minimize scare tactics Provide measured facts instead

Protect me upfront If it keeps me safe, you don't need my permission

# Help me make a thoughtful decision

Use consistent emotional cues Positive cues emphasize safety, while negative ones, danger

Make safe choices easier to select Make it harder to put myself at risk

Lower the impact of making mistakes Reduce the pressure of making the "right" choice right now

Source: <u>A Guide to Crafting Meaningful Security and Privacy Experiences</u> by Larissa Co

### Respect my time and task

Focus on the impact to my task Spend less time explaining the technical issue

Flag threats; don't assume I notice The absence of positive indicators isn't enough

Avoid interrupting me Wait until I'm done or choose a safe default

## Offer control without harming me

When I have no choice, explain why Helping me understand stills gives me some control

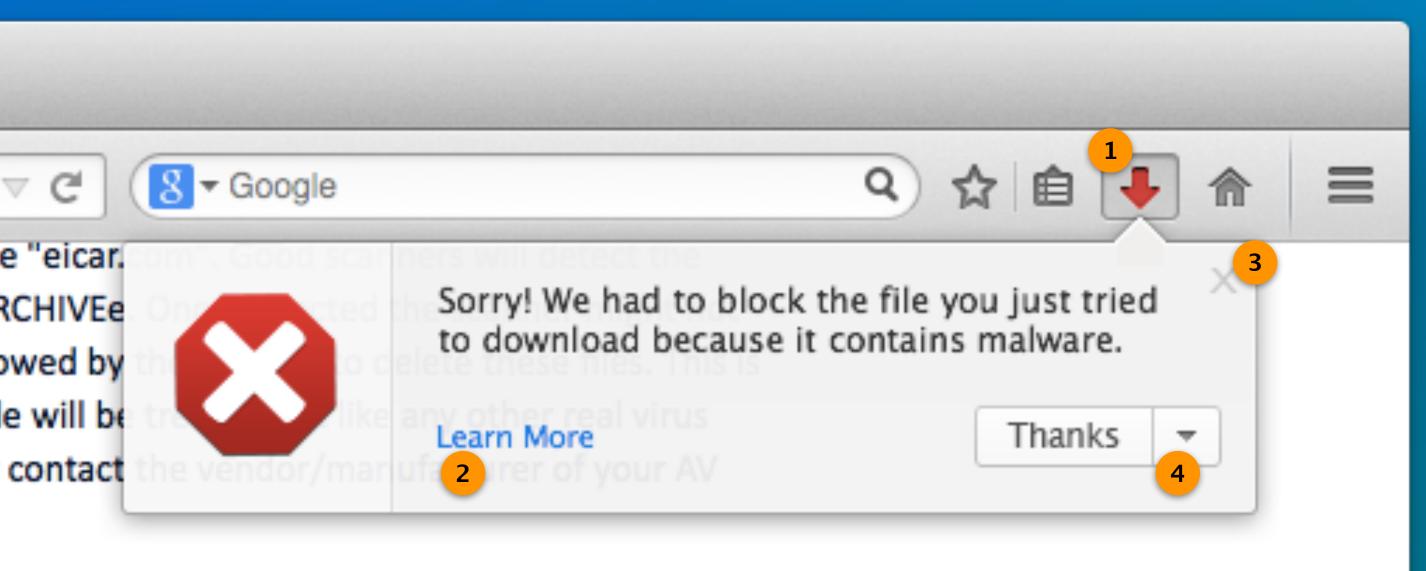
Make the effect of each option clear Novices want guidance, not a control panel

Give Pros configurable controls Technical users want precision and flexibility

# **Suggested Changes**

- user.
  - Currently, the user has no way of knowing a download was blocked until they go to open the file, at which point it is a surprise. The user should be informed right away.
- A "Learn More" link in the doorhanger should take users to a page which explains why/ how we handle malware blocking in Firefox.
- Highlight Downloads toolbar button red to indicate there is a contained alert.
- In the downloads panel the user should have a more apparent way to quickly delete the offending file.
- In the downloads panel the user should be able to "unblock" the malicious download.
  - This prompts a modal dialog the user must acknowledge which warns of the ramifications of "unblocking" the file.

# • When a download is blocked for containing malware, a doorhanger appears to alert the



er in combination with these files cause any WN RISK. Download these files only if you and will not provide any help to remove these f your AV scanner to seek such help.



- 1. Icon turns red and pulses once when there is a malicious download in the list.
- 2. "Learn more" takes user to Mozilla help page regarding malicious and potentially unwanted downloads.
- 3. Dismisses doorhanger.
- 4. Dismisses doorhanger and opens download panel.
  - Sub-option: "Don't show me this alert again"



# Malicious Files in Download Panel (Before/After)



### eicar\_com.zip

Blocked: May contain a virus or spyware - eicar.org - 11:1...



### secret\_document.pdf

24.7 KB - mozilla.org - 10:55 AM

Q

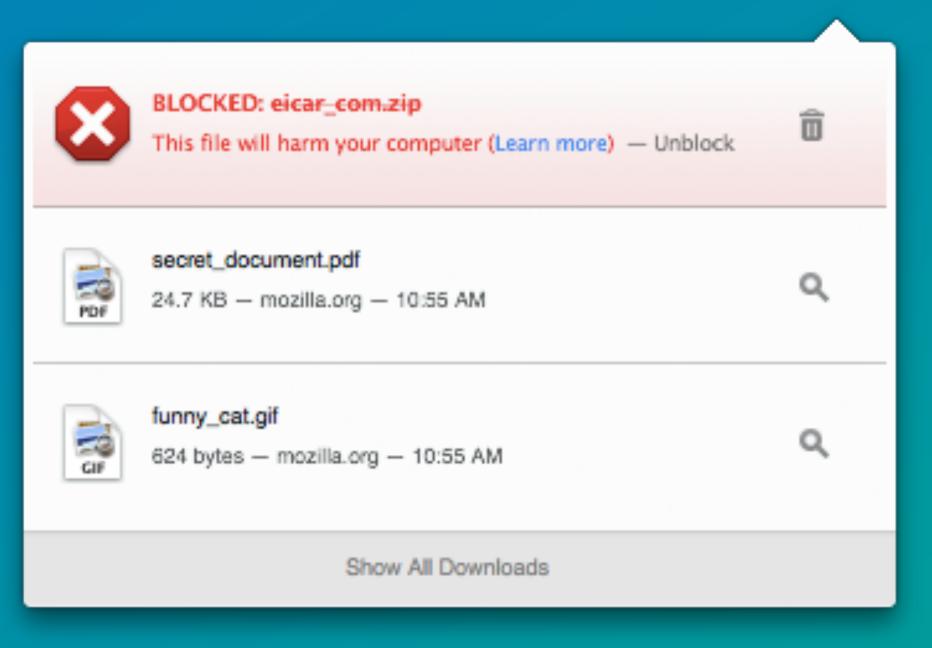
Q



### funny\_cat.gif

624 bytes - mozilla.org - 10:55 AM

Show All Downloads



### Malicious Files Download Panel Anatomy

					1.
8-	Google		Q ☆ 🗎 🛃	⋒≡	
ar.com". Ee. Once by the so be treat	8	4 BLOCKED: eicar_com.zip This file will harm your computer (Learn r	nore) – Unblock 2		2.
act the v	PDF	secret_document.pdf 24.7 KB — mozilla.org — 10:55 AM	Q		3.
ombinat	CIF	funny_cat.gif 624 bytes — mozilla.org — 10:55 AM	Q		4.
RISK. Do vill not p		Show All Downloads			
AV scanr	her to s	eek such help.			5.
					6.
	eicarco 308 By	om2.zip /tes			
	eicarco 308 By	om2.zip /tes			7.

Icon turns red and pulses when there is a malicious download in the list.

Red gradient draws eye and indicates the dangerous nature of the file.

Trash can icon allows user to quickly dispose of offending file.

File name is struck through, emphasizing that it is blocked.

Clear messaging: "This file will harm your computer"

"Learn more" takes user to Mozilla help page regarding malicious and potentially unwanted downloads.

Unblock link underlines on mouseover and triggers modal popup confirmation





## Malicious Files Modal Popup

+

European Exp... 10

nload.html



This file contains malware that will harm your computer.

The website you downloaded this file from may have been compromised. Firefox recommends searching for an alternative source to download this file, or you can try redownloading the file at a later time.



events as rss feed.

**BE UP TO DATE** 

EICAR News

EICAR Events

IMPORTANT NOTE EICAR cannot be held responsible when these files or your AV scanner in combination with these files cause any damage to your computer. YOU DOWNLOAD THESE FILES AT YOUR OWN RISK. Download these files only if you are sufficiently secure in the usage of your AV scanner. EICAR cannot and will not provide any help to remove these files from your computer. Please contact the manufacturer/vendor of your AV scanner to seek such help.

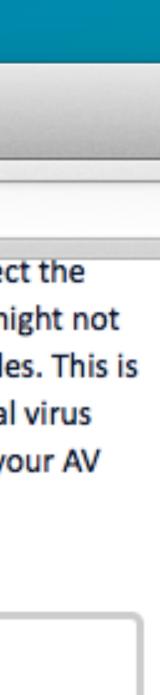
### Download area using the standard protocol http eicarcom2.zip eicar.com eicar.com.txt eicar\_com.zip 308 Bytes 68 Bytes 184 Bytes 68 Bytes Download area using the secure, SSL enabled protocol https eicarcom2.zip eicar.com.txt eicar\_com.zip eicar.com 68 Bytes 184 Bytes 308 Bytes 68 Bytes

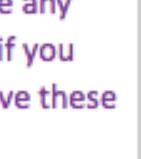
### Are you sure you want to unblock this file?

Unblock anyway Keep me safe



file "eicar.com". Good scanners will detect the ARCHIVEe. Once detected the scanner might not allowed by the scanner to delete these files. This is t file will be treated just like any other real virus or contact the vendor/manufacturer of your AV





## **Unblocked Malicious Files in Download Panel**

	Google		Q ☆ 🗎 🗜	
ar.com". /Ee. Once by the se be treat	ZIP	eicar_com.zip 186 bytes — eicar.org — 10:55AM	Q	
act the v	PDF	secret_document.pdf 24.7 KB — mozilla.org — 10:55 AM	Q	
ombinat	GIF	funny_cat.gif 624 bytes — mozilla.org — 10:55 AM	Q	
RISK. Do will not p	er to se	Show All Downloads eek such help.		
AV SCAIII		ek such help.		



When a user unblocks a malicious file, the download icon is no longer highlighted red and the row in the download panel changes format to look like a normal download.

The only addition is a badge on the download icon which indicates to the user that the download was previously flagged.

Hovering over the icon prompts a tool-tip stating that the file was flagged:

This file was flagged as being malicious







































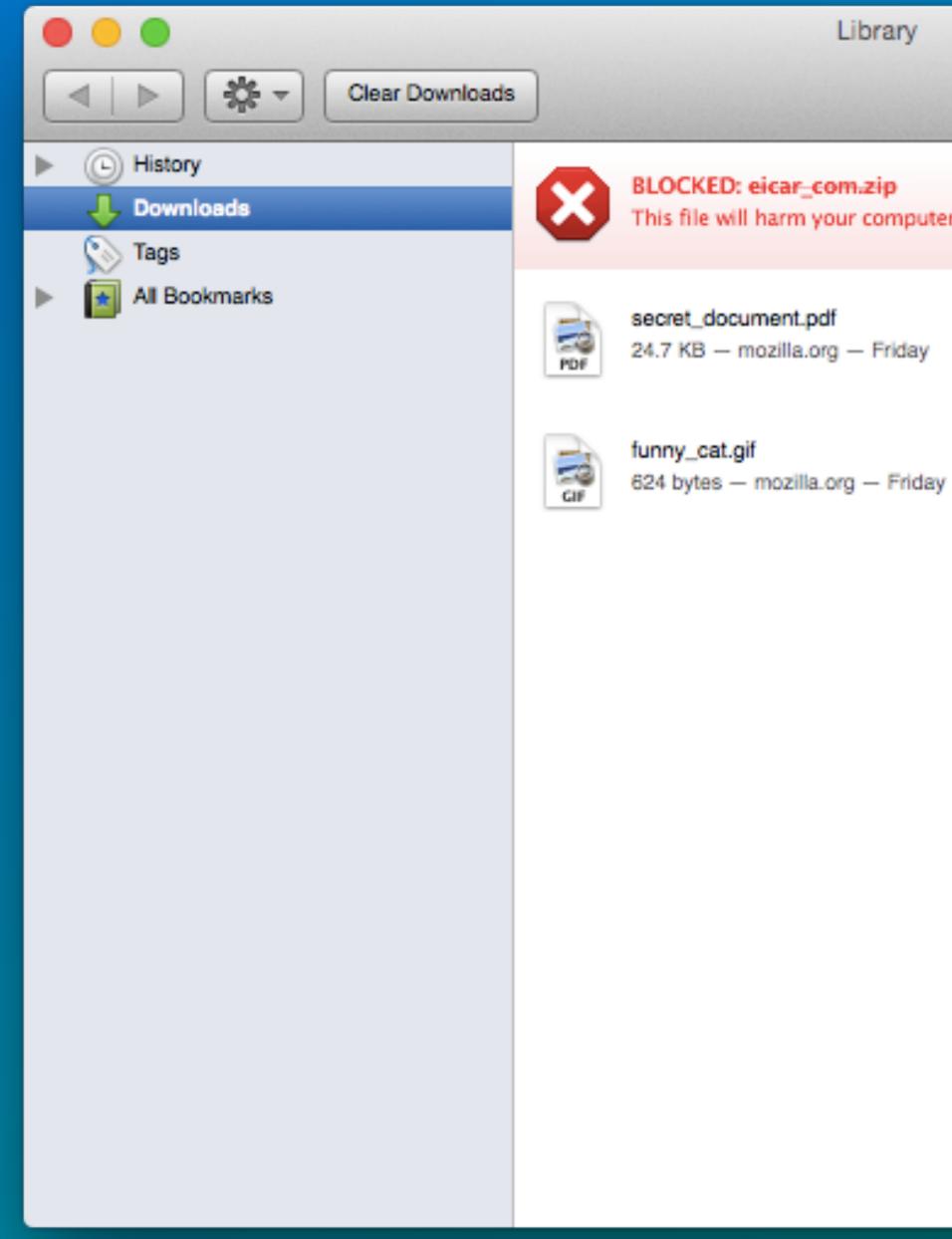








# Download Library (Blocked Malicious Files)



### mozilla

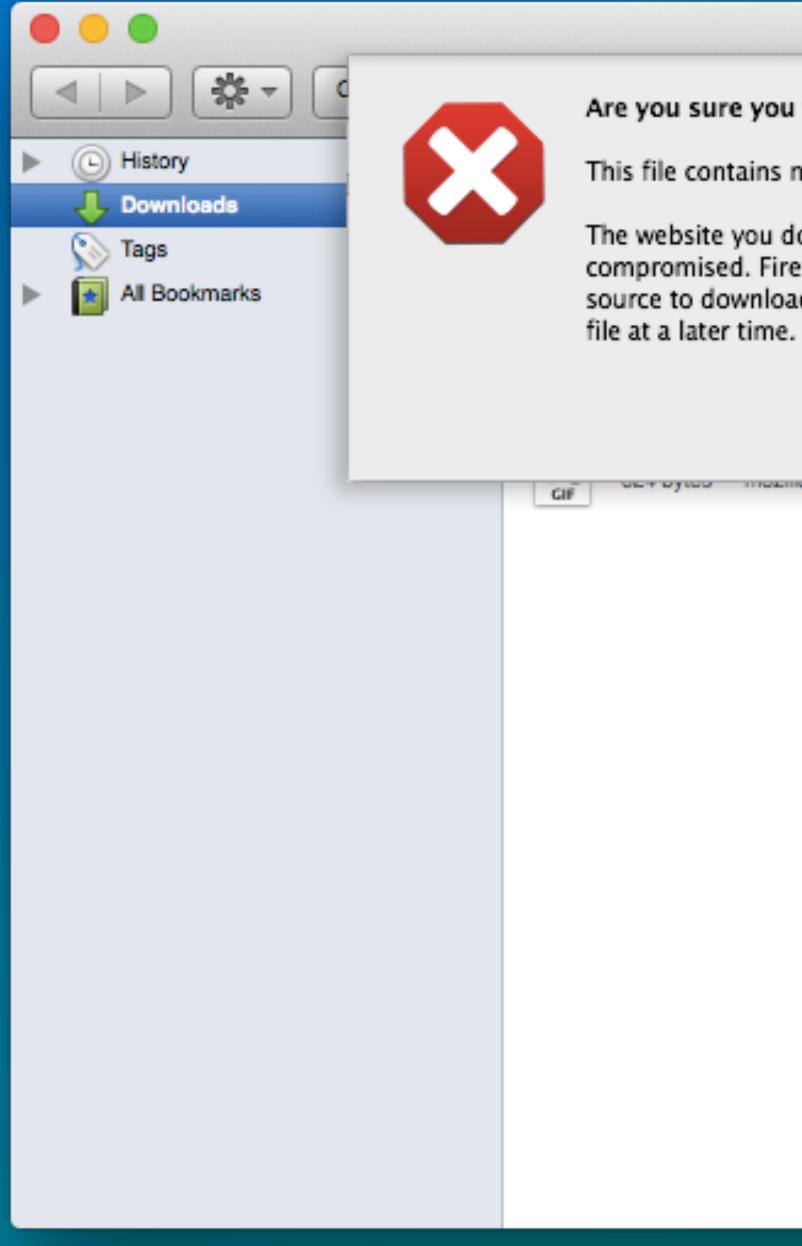
Ô

Q

Q

# Library Q Search Downloads This file will harm your computer (Learn more) - Unblock

# **Download Library (Malicious Files Modal)**



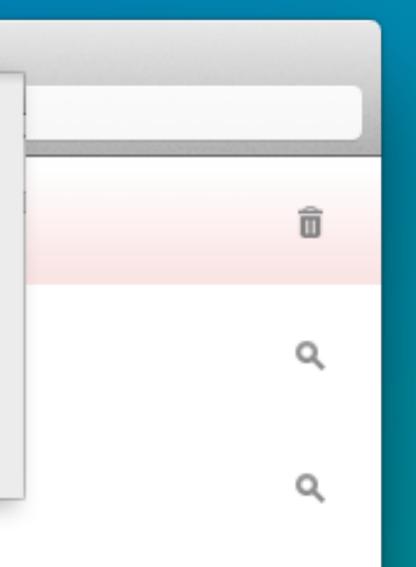
### Library

Are you sure you want to unblock this file?

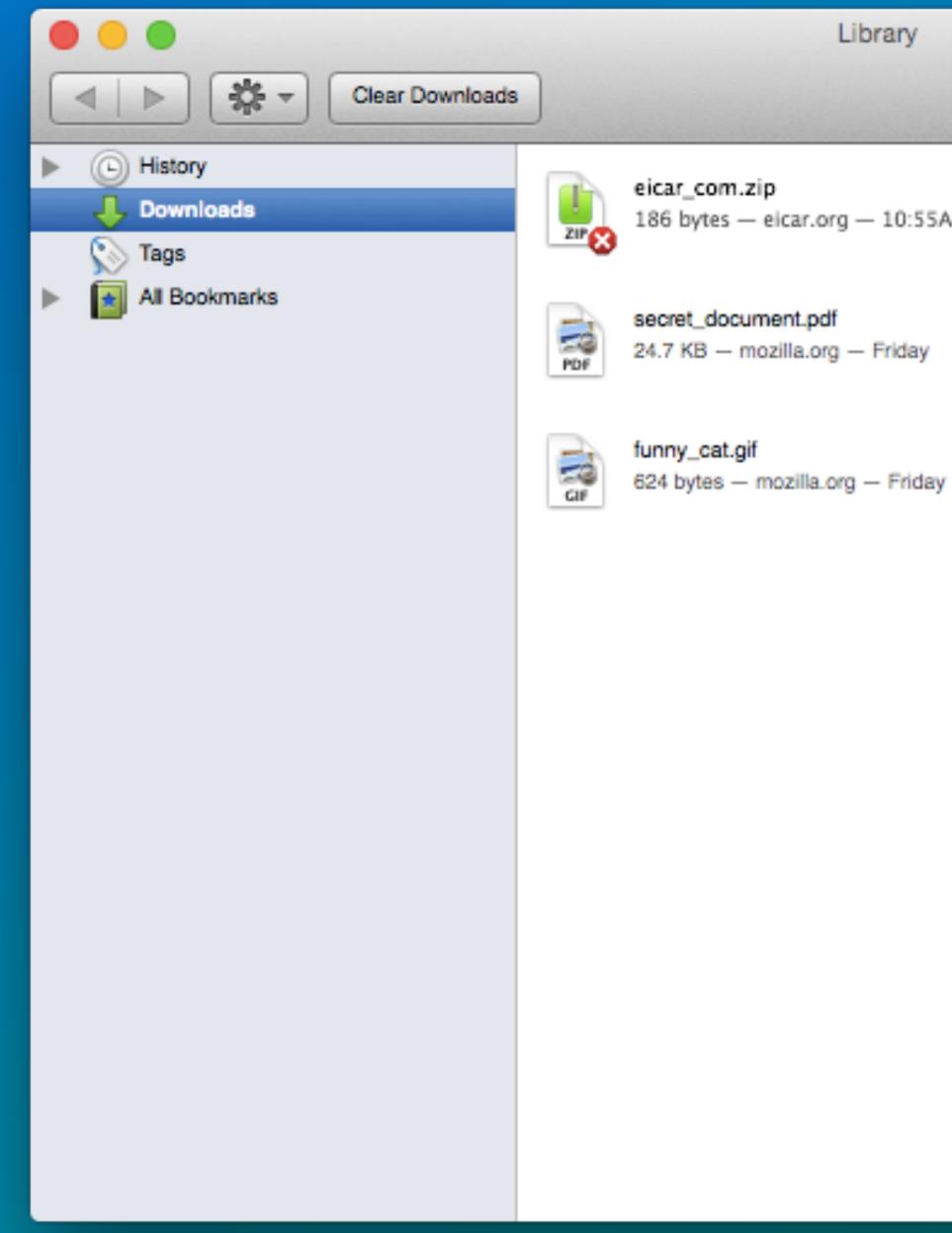
This file contains malware that will harm your computer.

The website you downloaded this file from may have been compromised. Firefox recommends searching for an alternative source to download this file, or you can try redownloading the file at a later time.

Unblock anyway	Keep me safe
org maay	



# **Download Library (Unblocked Malicious Files)**



## mozilla

# Library Q Search Downloads Q 186 bytes - eicar.org - 10:55AM Q Q

⊽ C' ] (8

downloaded run your AV scanner. It should detect at least the file "eicar. in the single zip ARCHIVEe and may be even in the double zip ARCHIVEe you any access to the file(s) anymore. You might not even be allowed by d by the scanner which puts the file into quarantaine. The test file will be ed file. Read the user's manual of your AV scanner what to do or contact er.

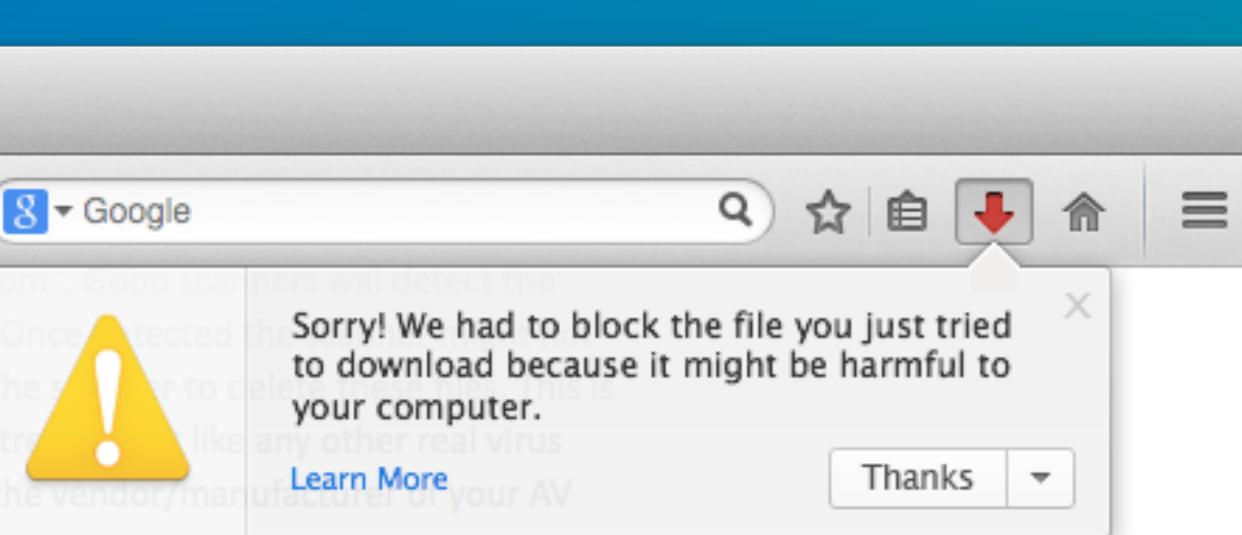
# DRTANT NOTE

R cannot be held responsible when these files or your AV scanner in combination with these files cause any age to your computer. YOU DOWNLOAD THESE FILES AT YOUR OWN RISK. Download these files only if you ufficiently secure in the usage of your AV scanner. EICAR cannot and will not provide any help to remove these from your computer. Please contact the manufacturer/vendor of your AV scanner to seek such help.

# nload area using the standard protocol http/

.com	eicar.com.txt
	•••••
ytes	68 Bytes









mozilla

# Potentially Unwanted Files in Download Panel



BLOCKED: eicar\_com.z This file may harm your o



secret\_document.pdf

24.7 KB - mozilla.org -



funny\_cat.gif

624 bytes - mozilla.org -

Shov

Note: Text colour changed to orange to represent that this is one-step down from a 100% malicious file (red text)

zip computer (Learn more) — Unblock	Î
10:55 AM	Q
- 10:55 AM	Q
v All Downloads	

### **Potentially Unwanted Files Modal Popup**

+

European Exp... 10

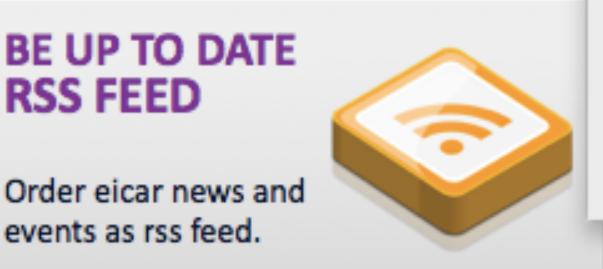
nload.html



### Are you sure you want to unblock this file?

This file could harm your computer and/or make unwanted changes to Firefox.

The website you downloaded this file from may have been compromised. Firefox recommends searching for an alternative source to download this file, or you can try redownloading the file at a later time.



Order eicar news and events as rss feed.

EICAR News

RSS FEED

EICAR Events

IMPORTANT NOTE EICAR cannot be held responsible when these files or your AV scanner in combination with these files cause any damage to your computer. YOU DOWNLOAD THESE FILES AT YOUR OWN RISK. Download these files only if you are sufficiently secure in the usage of your AV scanner. EICAR cannot and will not provide any help to remove these files from your computer. Please contact the manufacturer/vendor of your AV scanner to seek such help.

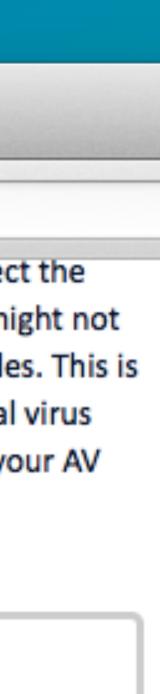
### Download area using the standard protocol http eicarcom2.zip eicar.com eicar.com.txt eicar\_com.zip 308 Bytes 68 Bytes 184 Bytes 68 Bytes Download area using the secure, SSL enabled protocol https eicarcom2.zip eicar.com eicar.com.txt eicar\_com.zip 68 Bytes 184 Bytes 308 Bytes 68 Bytes

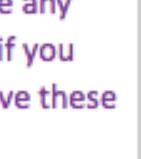
Unblock anyway

Keep me safe

### 8 - Google C

file "eicar.com". Good scanners will detect the ARCHIVEe. Once detected the scanner might not allowed by the scanner to delete these files. This is t file will be treated just like any other real virus or contact the vendor/manufacturer of your AV





# Unblocked Potentially Unwanted Files in Download Panel



eicar\_com.zip

186 bytes — eicar.org —



secret\_document.pdf

24.7 KB - mozilla.org -



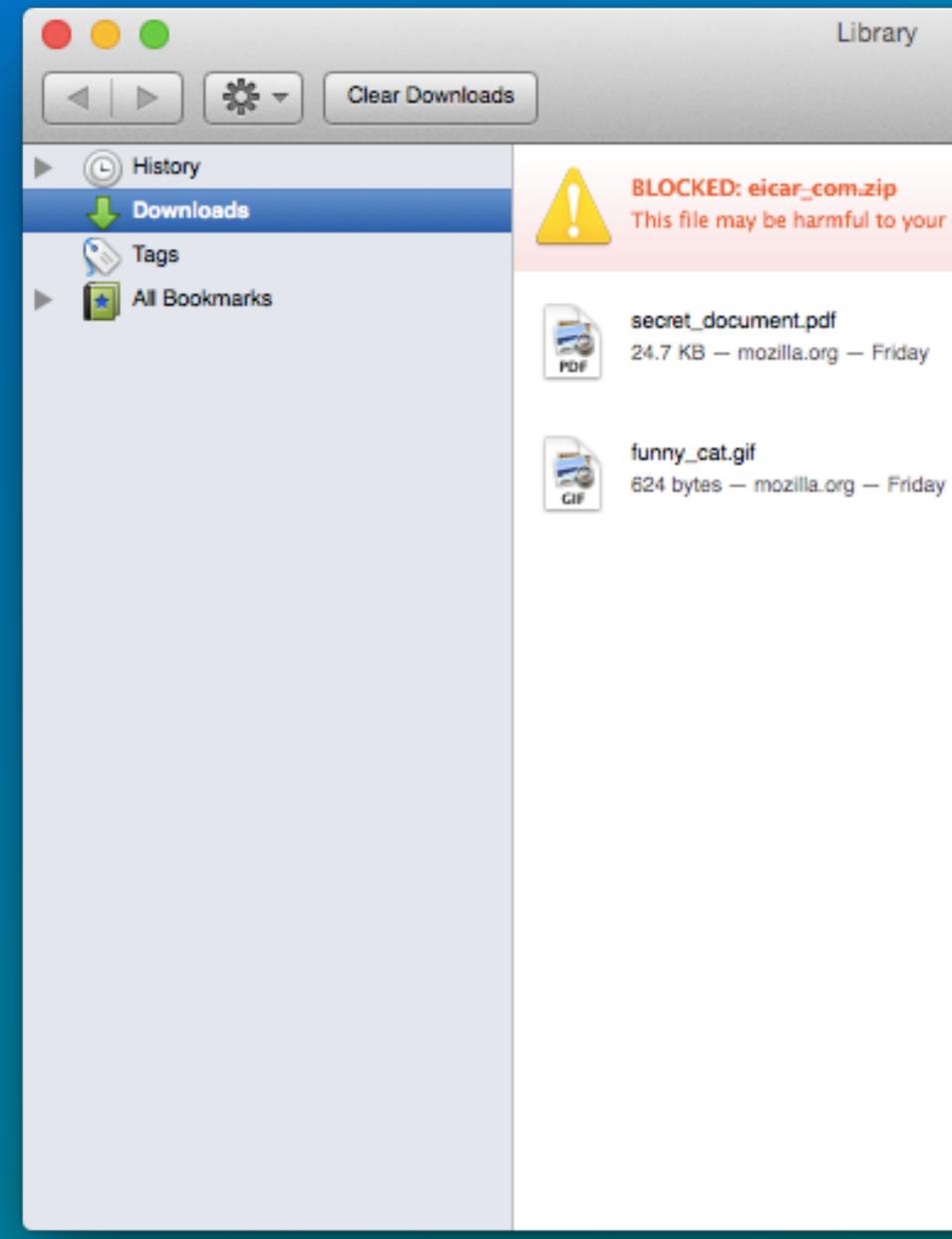
funny\_cat.gif

624 bytes - mozilla.org -

Shov

- 10:55AM	Q
10:55 AM	Q
- 10:55 AM	Q
v All Downloads	

# Download Library (Blocked Potentially Unwanted Files)



### mozilla

Ô

Q

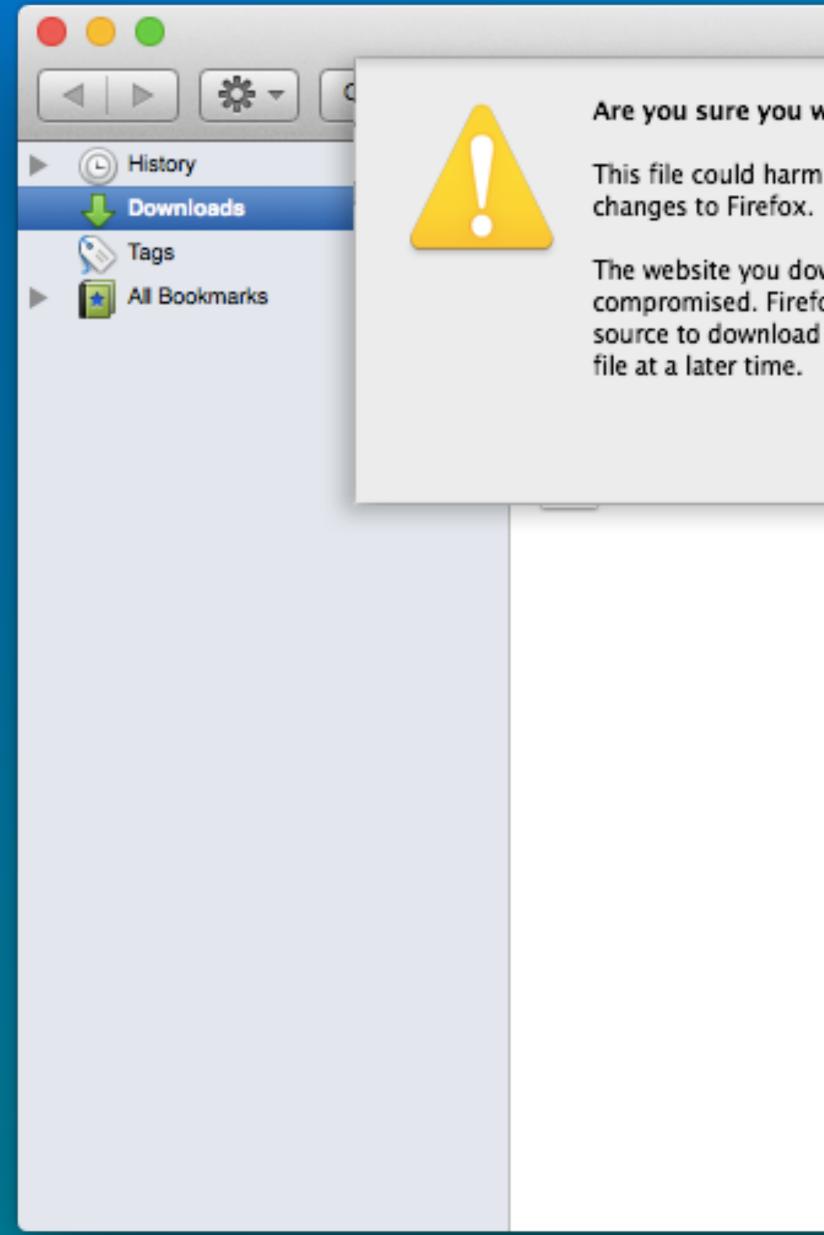
Q

### Library

### Q Search Downloads

This file may be harmful to your computer (Learn more) — Unblock

## Download Library (Potentially Unwanted Files Modal)



## mozilla

### Library

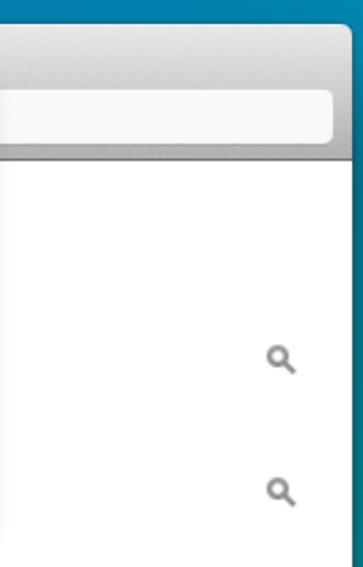
Are you sure you want to unblock this file?

This file could harm your computer and/or make unwanted changes to Firefox.

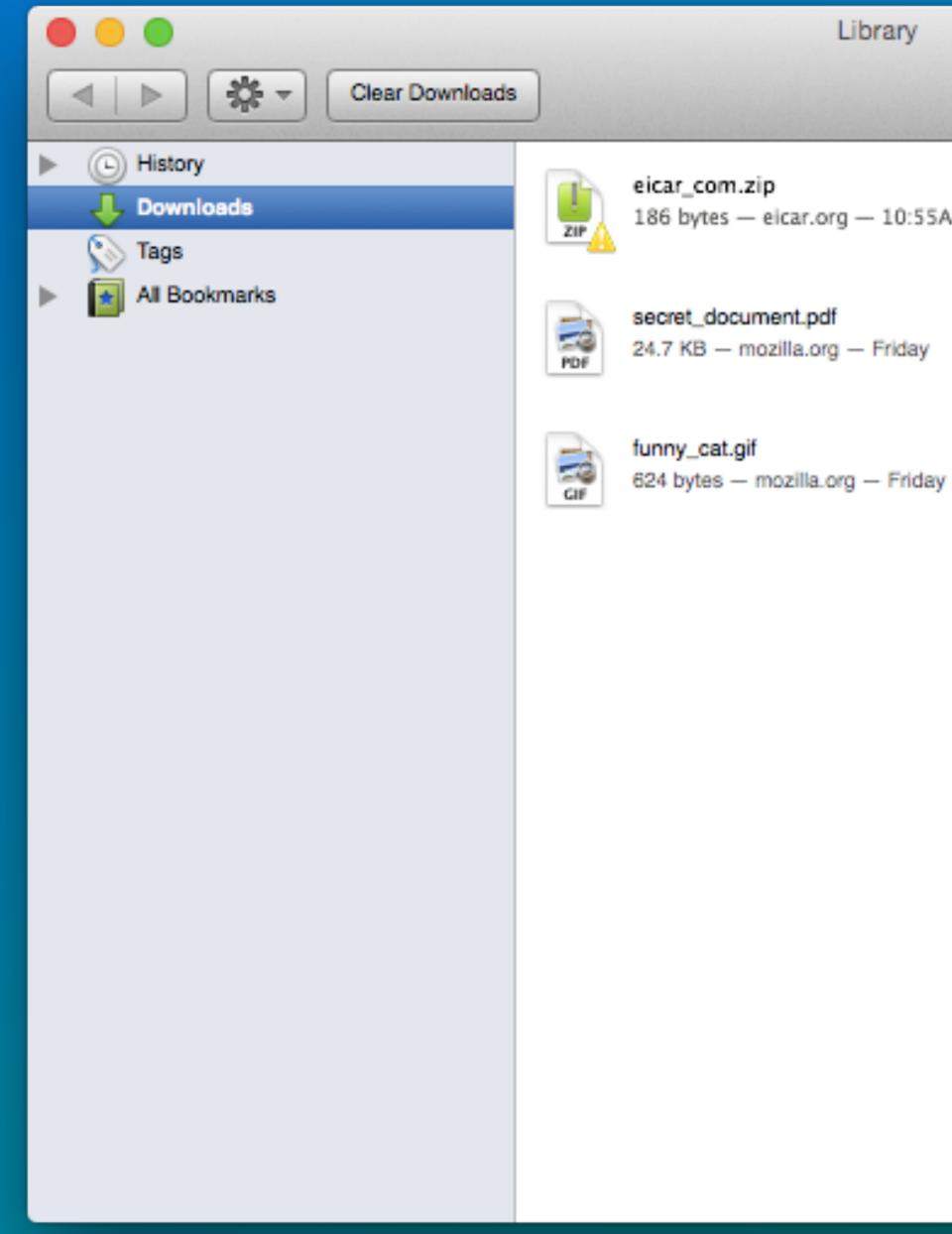
The website you downloaded this file from may have been compromised. Firefox recommends searching for an alternative source to download this file, or you can try redownloading the

Unblock anyway

Keep me safe



# Download Library (Unblocked Potentially Unwanted Files)



## mozilla

# Library Q Search Downloads Q 186 bytes - eicar.org - 10:55AM Q Q

∠ G

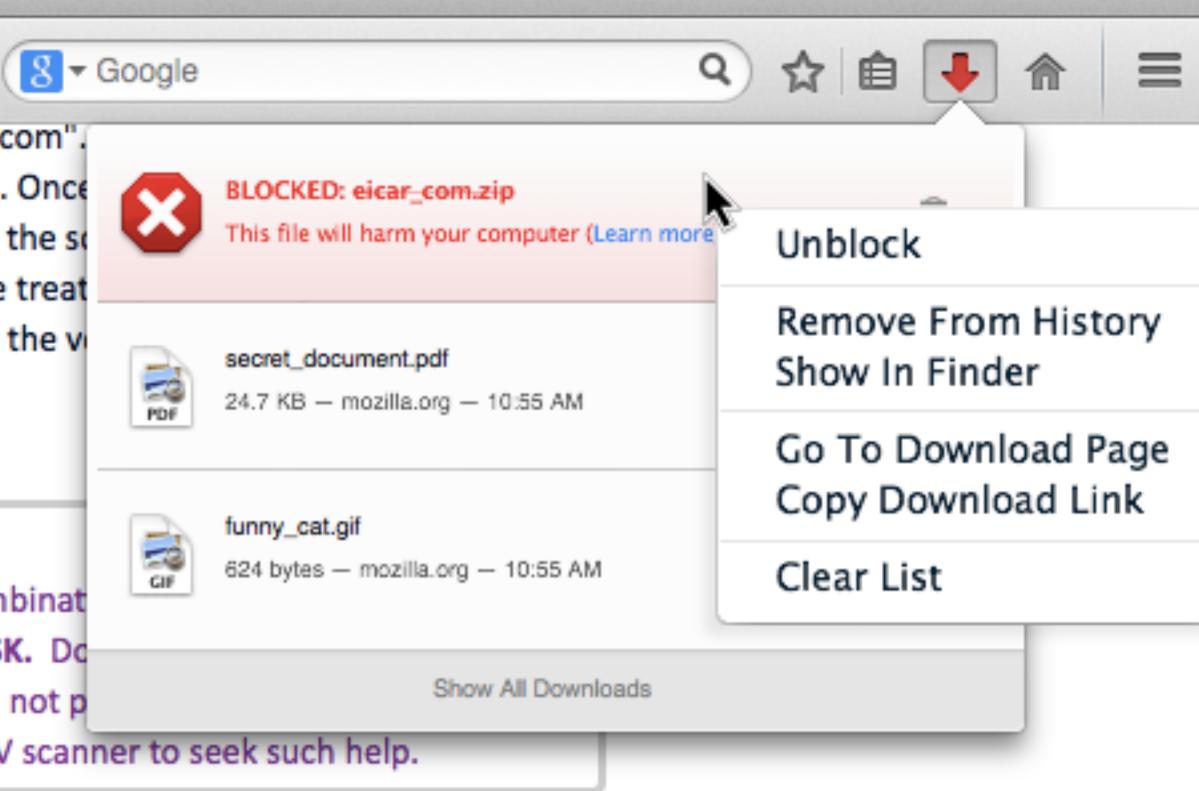
Once downloaded run your AV scanner. It should detect at least the file "eicar.com". 'virus' in the single zip ARCHIVEe and may be even in the double zip ARCHIVEe. Once allow you any access to the file(s) anymore. You might not even be allowed by the so caused by the scanner which puts the file into quarantaine. The test file will be treat infected file. Read the user's manual of your AV scanner what to do or contact the v scanner.

### IMPORTANT NOTE

EICAR cannot be held responsible when these files or your AV scanner in combinat damage to your computer. YOU DOWNLOAD THESE FILES AT YOUR OWN RISK. Do are sufficiently secure in the usage of your AV scanner. EICAR cannot and will not p files from your computer. Please contact the manufacturer/vendor of your AV scanner to seek such help.

Download area	a using the standard prot	ocol http
eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes
Download area	a using the secure, SSL en	nabled protocol https

alaar aana tu







# Malicious Downloads Strings

- Learn more
- Thanks
- Dismiss
- Don't show me this alert again
- Blocked
- This file will harm your computer (Learn more) Unblock
- Are you sure you want to unblock this file?

This file contains malware that will harm your computer.

The website you downloaded this file from may have been compromised. Firefox recommends searching for an alternative source to download this file, or you can try redownloading the file at a later time.

- Unblock Anyway
- Keep Me Safe

# • Sorry! We had to block the file you just tried to download because it contains malware.

# **Potentially Unwanted Downloads Strings**

- Learn more
- Thanks
- Dismiss
- Don't show me this alert again
- Blocked
- This file may be harm your computer (Learn more) Unblock
- Are you sure you want to unblock this file?

This file could harm your computer and/or make unwanted changes to Firefox.

The website you downloaded this file from may have been compromised. Firefox recommends searching for an alternative source to download this file, or you can try redownloading the file at a later time.

- Unblock Anyway
- Keep Me Safe

• Sorry! We had to block the file you just tried to download because it contains malware.



IRC: @sevaan in #UX on IRC Email: sfranks@mozilla.com Twitter: @sevaanfranks



# Questions? Comments? Suggestions?