COMODO
Creating Trust Online®

Comodo
Online Security

Software Version 2.0

User Guide

Guide Version 2.0 020719

Comodo Security Solutions
255 Broad Street
Clifton, NJ 07013

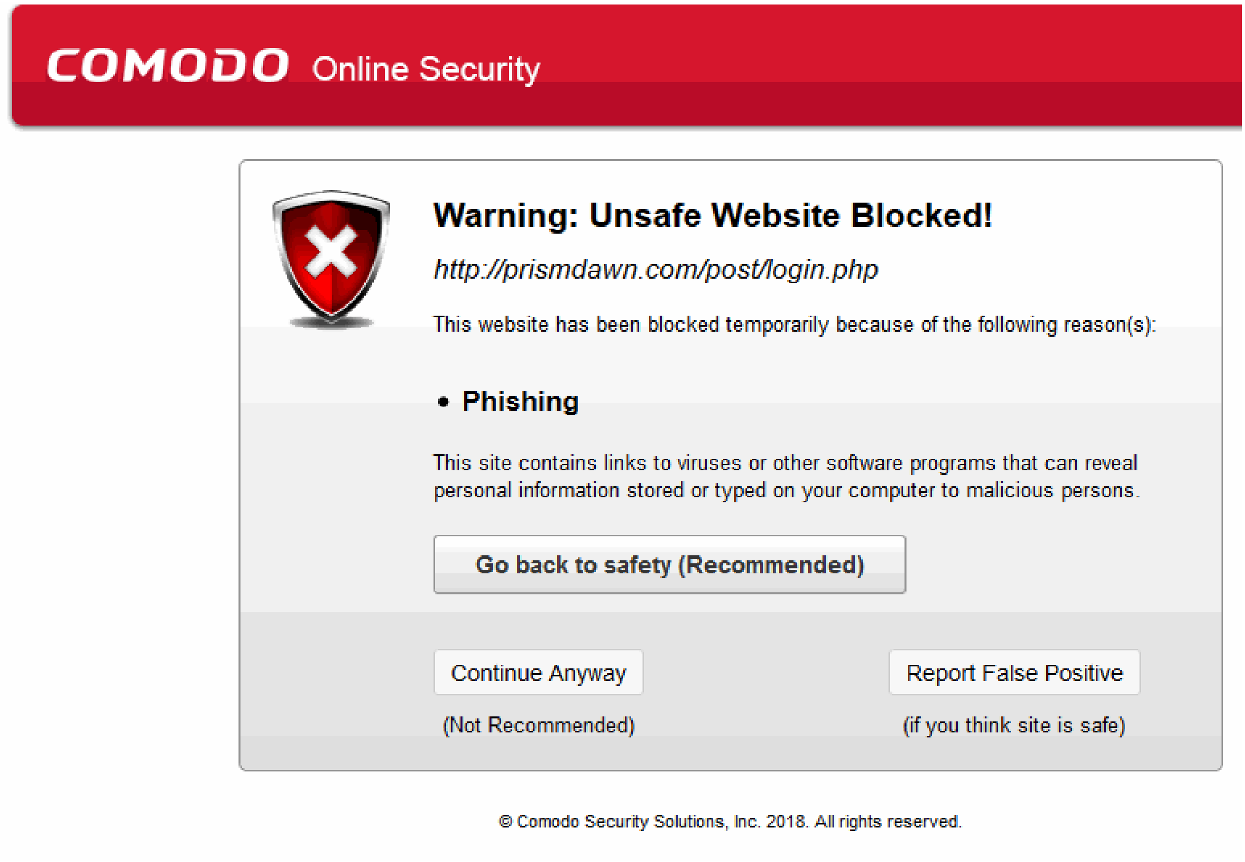
1 Introduction to Comodo Online Security

Comodo Online Security (COS) is a powerful web filtering extension for Chrome, Firefox and Internet Explorer. Completely free of charge, Comodo Online Security will block harmful websites before they have a chance to load, protecting you from malware, hackers and more.

Features:

- Instantly blocks dangerous and fraudulent websites
- Works with incognito, private and normal browsing modes
- Takes seconds to download and install
- Blocks sites which may have been missed by in-browser web filters
- No impact on browsing speed

After installation, COS will show the following alert whenever it blocks a harmful website:



Warning: Unsafe Website Blocked!

http://prismdawn.com/post/login.php

This website has been blocked temporarily because of the following reason(s):

- **Phishing**

This site contains links to viruses or other software programs that can reveal personal information stored or typed on your computer to malicious persons.

© Comodo Security Solutions, Inc. 2018. All rights reserved.

- **Go back to safety** – Will return you to the previous page
- **Continue Anyway** – Will ignore the warning and take you to the site. This is not recommended as you run a high risk of exposing your PC to attack
- **Report false positive** – Submit the URL of the site to Comodo for analysis. Use this option if you think it has been incorrectly classified as malicious.

The rest of this guide covers installation, use, and removal of the extension in Chrome, Firefox and Internet Explorer.

Installation and use:

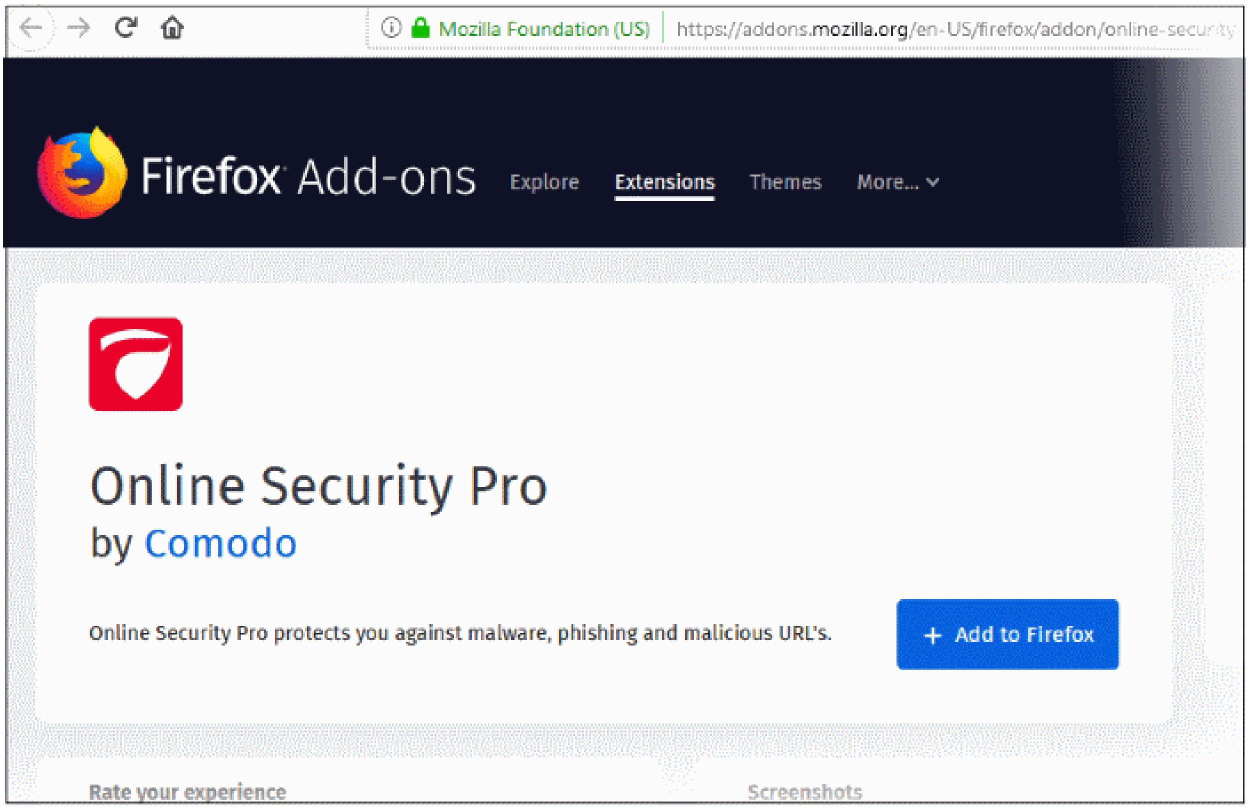
- Firefox
- Chrome
- Internet Explorer

Remove the extension:

- Firefox
- Chrome
- Internet Explorer

Firefox: Installation and use

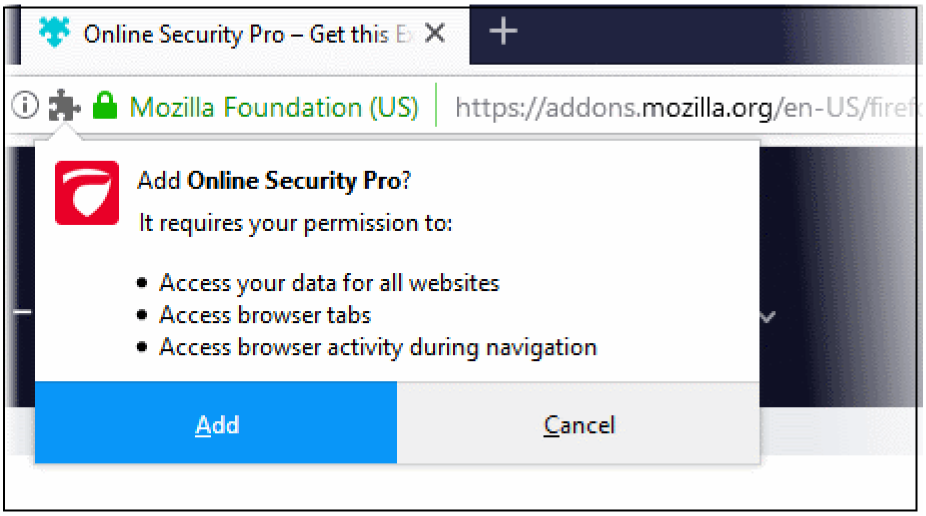
- Visit **https://antivirus.comodo.com/online-security.php**
- Click 'Download for Firefox'. This will open the Firefox add-on page for Comodo Online Security.
- Click 'Add to Firefox'



Online Security Pro
by Comodo

Online Security Pro protects you against malware, phishing and malicious URL's.

- Click 'Add' to start the installation

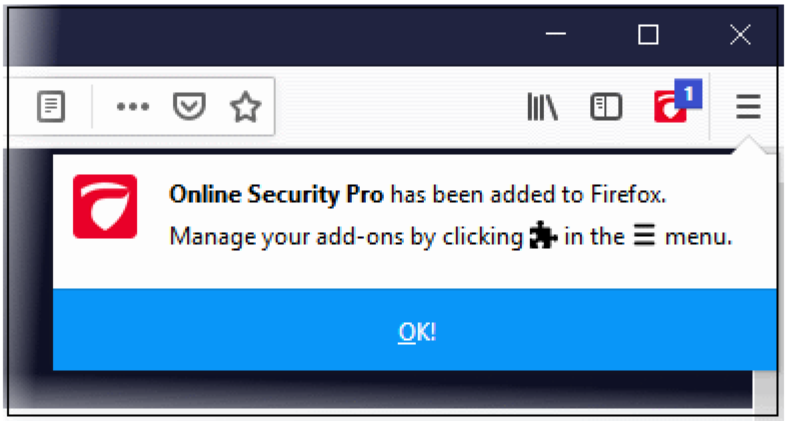

Online Security Pro – Get this E
Mozilla Foundation (US)
https://addons.mozilla.org/en-US/firef

Add **Online Security Pro**?

It requires your permission to:

- Access your data for all websites
- Access browser tabs
- Access browser activity during navigation

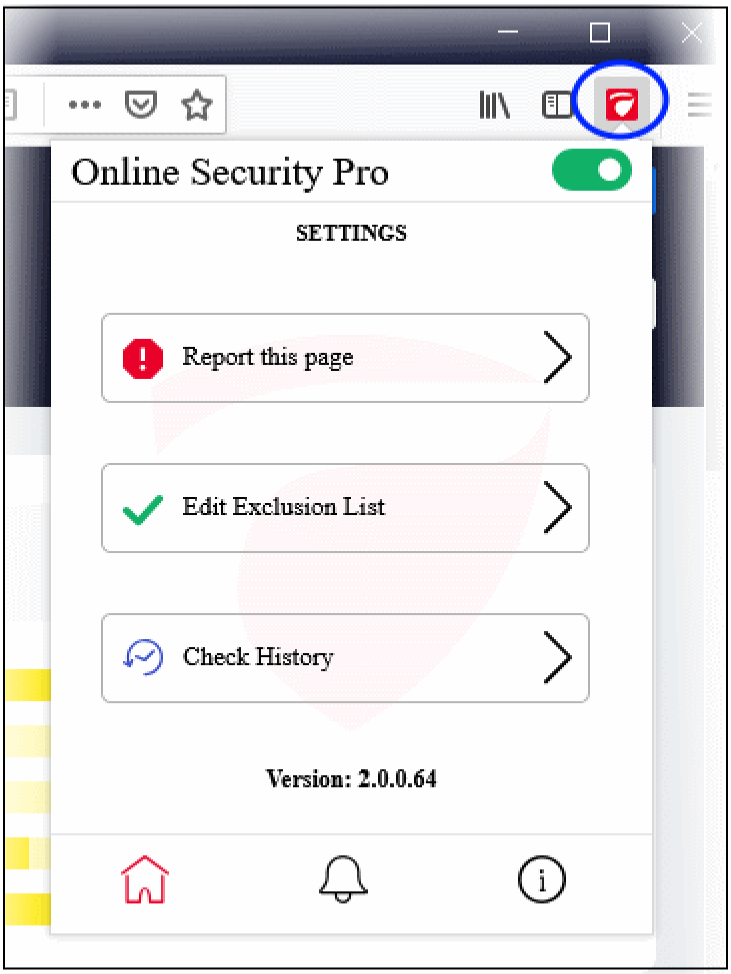
A success message is shown after installation:


Online Security Pro has been added to Firefox.

Manage your add-ons by clicking in the ☰ menu.

- Click 'OK' to finalize the installation:

The COS icon will appear at the top-right of Fire Fox:



Online Security Pro

SETTINGS

Report this page

Edit Exclusion List

Check History

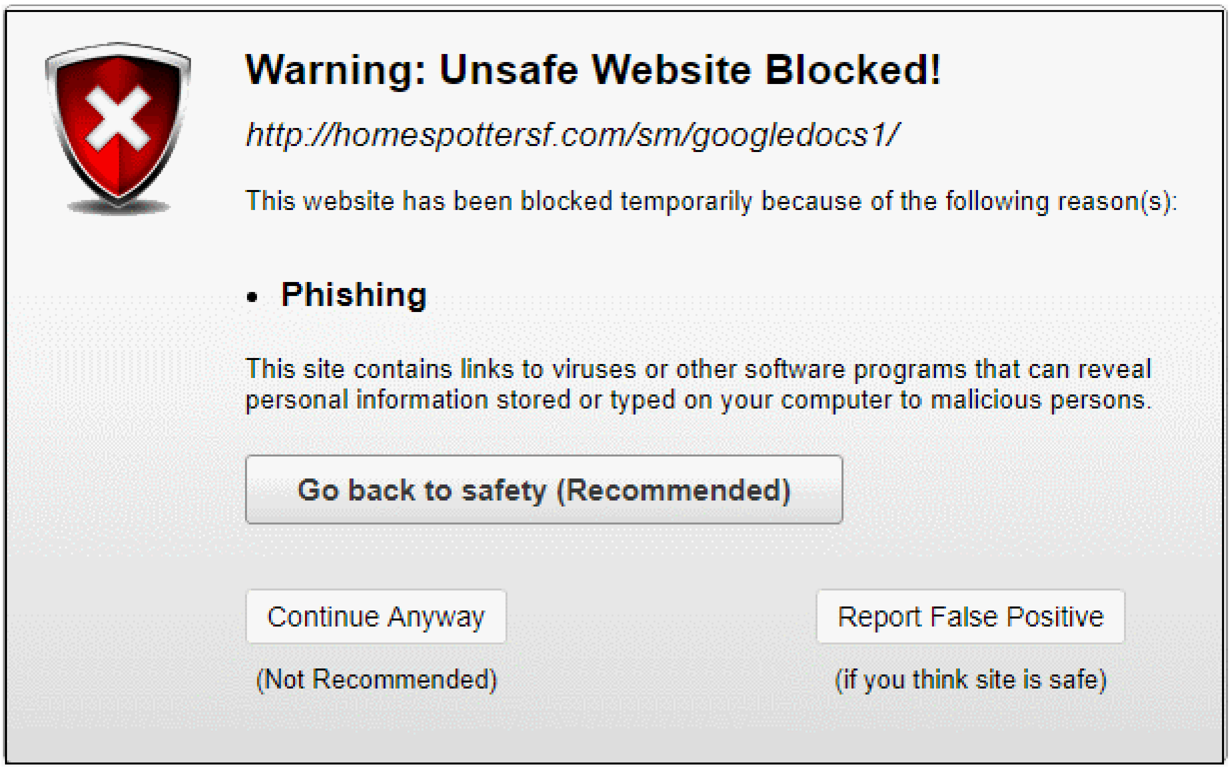
Version: 2.0.0.64

Click the COS icon to reveal the follow options:

- **Comodo Online Security Pro** - Enable or disable the COS web-filter. *(Default = Enabled)*
- **Home icon** – Open the COS settings page:
  - **Report this page** - Submit the URL of the site you currently visiting to Comodo for analysis.
    - You should do this if you think it might be hosting malware, or might be a fake/phishing website. Comodo will test the site and add it to our black list if we confirm it as malicious.
    - Click anywhere on the stripe to open the reporting page at **https://www.comodo.com/home/internet-security/submit.php**
    - The URL is pre-populated, so you just need to enter your email address and any comments you feel would be helpful (optional).
  - **Edit Exclusion List** – COS generates an alert whenever it detects a harmful website. If you choose 'Continue Anyway' at the alert then the site is added to the exclusions list. This means COS will not flag it as malicious on future visits. Click anywhere on the stripe to view/modify web sites on the exclusion list.
  - **Check History** – View a log of sites caught by COS, and the action taken by you.
- **Notifications** – Shows news about COS and allows you to rate the product
- **About** – Links to product pages, release notes and more.

COS Alert

COS shows an alert if the visited website is found to be unsafe:



Warning: Unsafe Website Blocked!

http://homespottersf.com/sm/googledocs1/

This website has been blocked temporarily because of the following reason(s):

- **Phishing**

This site contains links to viruses or other software programs that can reveal personal information stored or typed on your computer to malicious persons.

The alert tells you the name and type of the threat and includes the following options:

- **Go back to safety** – Closes the web page
- **Continue Anyway** – Ignores the alert and opens the web page. The URL is added to your **exclusions list** so no alert is shown the next time you visit.
- **Report False Positive** – Opens the report page at https://www.comodo.com/home/internet-security/submit.php. Use this form if you think COS has blocked a page that is safe/ is not harmful.

Report this page

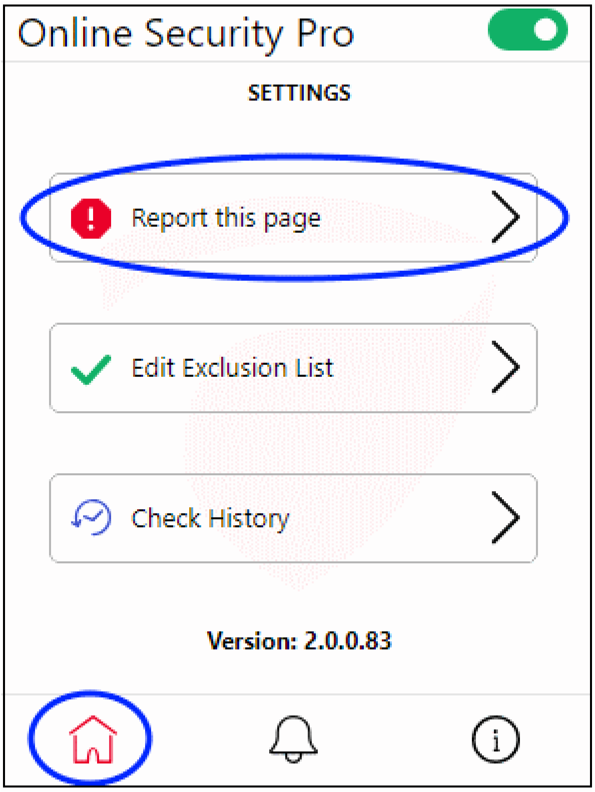
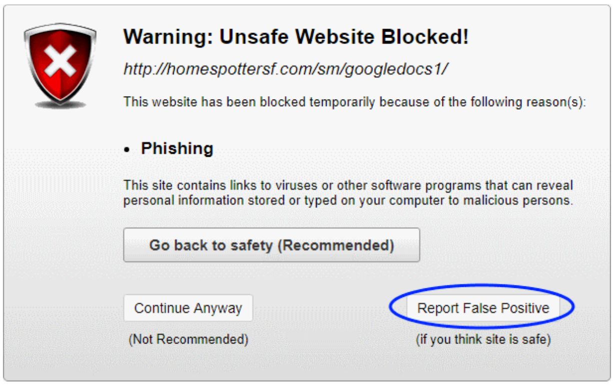
- Make sure you are on the page you want to report.
- If you just want to supply the URL of a new malicious site then we advise you go straight to **https://www.comodo.com/home/internet-security/submit.php** and complete the form.

To open the reporting screen:

- Click the COS button at top-right
- Click the 'Home' icon
- Click the 'Report this page' stripe

OR

- Click 'Report False Positive' in a COS alert

Online Security Pro

SETTINGS

Report this page

Edit Exclusion List

Check History

Version: 2.0.0.83

Warning: Unsafe Website Blocked!

http://homespottersf.com/sm/googledocs1/

This website has been blocked temporarily because of the following reason(s):

- **Phishing**

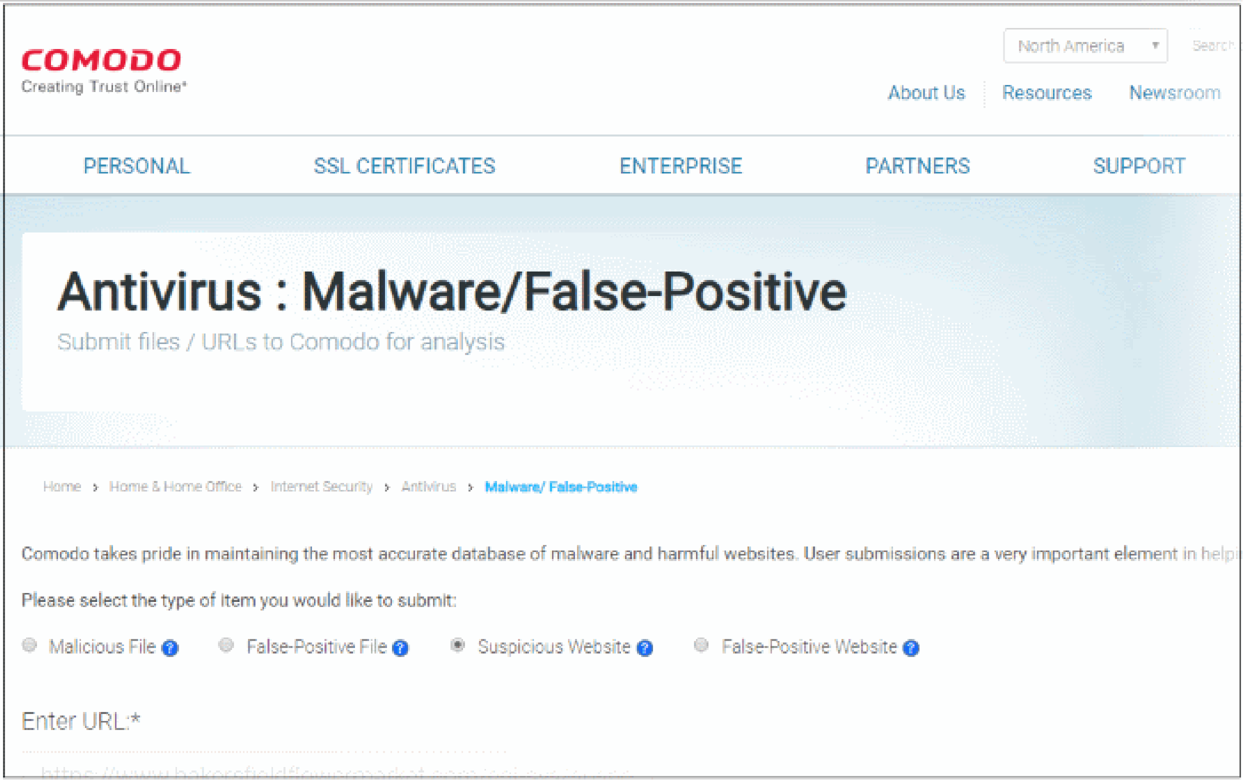
This site contains links to viruses or other software programs that can reveal personal information stored or typed on your computer to malicious persons.

Go back to safety (Recommended)

Continue Anyway
(Not Recommended)

Report False Positive
(if you think site is safe)

The 'Antivirus: Malware / False-Positive' screen will open at **https://www.comodo.com/home/internet-security/submit.php**



Antivirus : Malware/False-Positive

Submit files / URLs to Comodo for analysis

Home › Home & Home Office › Internet Security › Antivirus › Malware/ False-Positive

Comodo takes pride in maintaining the most accurate database of malware and harmful websites. User submissions are a very important element in help

Please select the type of item you would like to submit:

○ Malicious File ○ False-Positive File ● Suspicious Website ○ False-Positive Website

Enter URL:*

https://www.bakersfieldflowermarket.com/crl/pve/.../.aspx

- Enter the URL (if not already populated), your email address, and any comments you feel would be helpful.
- Click 'Submit'

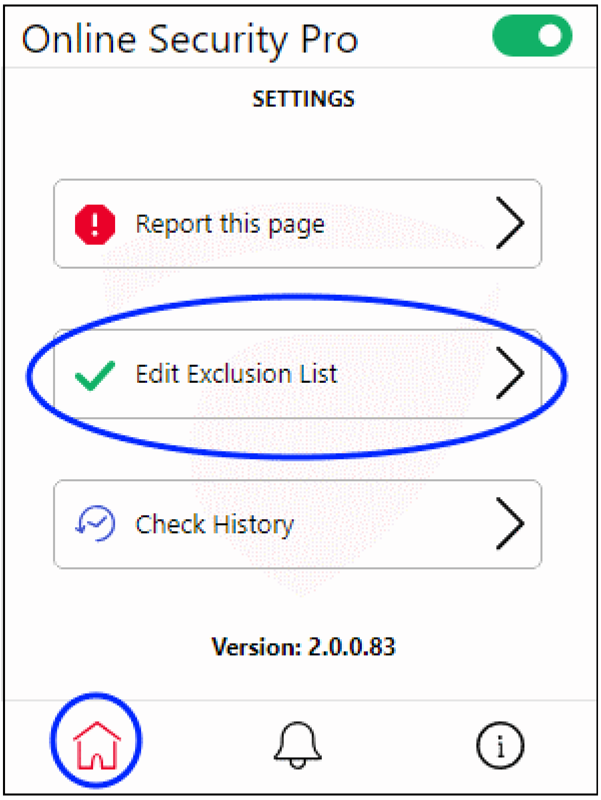
We will check if the reported site is malicious or safe and update our database as required.

Edit Exclusion List

This page shows websites that you have allowed even though COS flagged them as harmful. You can remove URLs from the exclusions list as required.

Open the exclusions list page:

- Click the COS app button at top-right
- Click the home icon, then the 'Edit Exclusion List' stripe

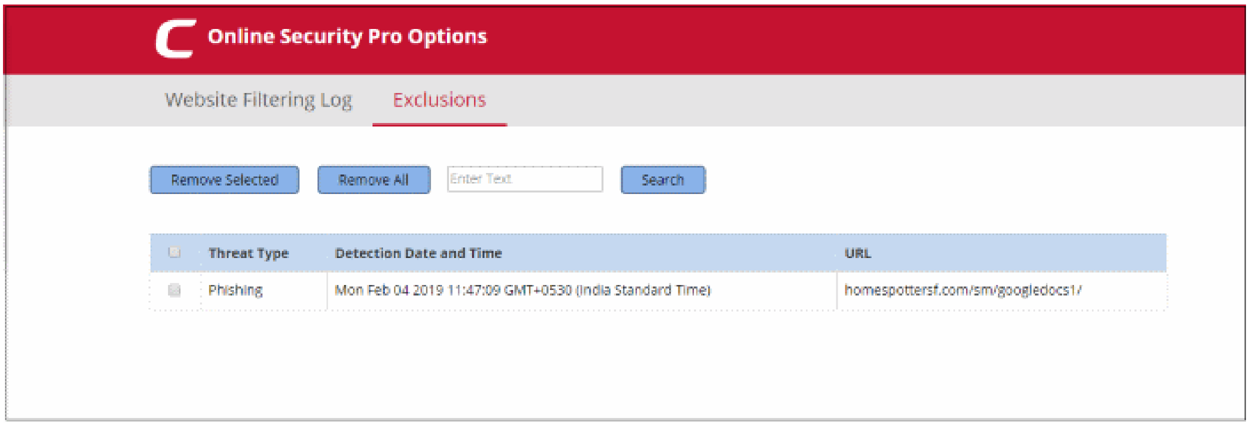


Online Security Pro

SETTINGS

Version: 2.0.0.83

This opens a list of websites that you have allowed:



Online Security Pro Options

□	Threat Type	Detection Date and Time	URL
□	Phishing	Mon Feb 04 2019 11:47:09 GMT+0530 (India Standard Time)	homespottersf.com/sm/googledocs1/

- **Threat type** – Category of attack found at the URL. Examples include 'Phishing' (fake/fraud websites) and 'Malware' (the site hosts viruses and other threats)
- **Detected Date and Time** - Date and time the threat was discovered by Comodo Online Security
- **URL** – The address of the site

- Use the search box to look for a particular site in the list

- Clear the box and click 'Search' again to reset the list

Remove a site from exclusions

- Select the check box next to the target site then click 'Remote Selected'
- Click 'Remove All' if you want to clear all exclusions.

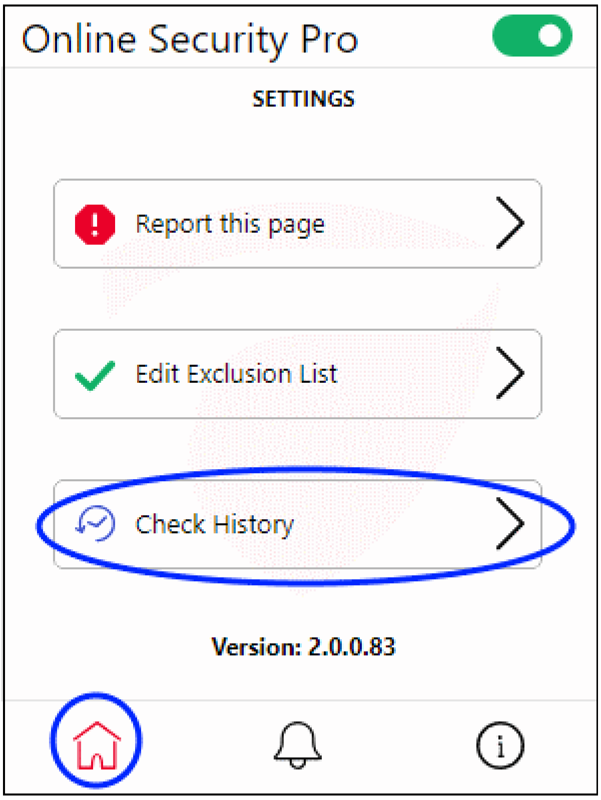
Note – After a website is removed from the list, alerts will be shown when you visit it again.

Check History

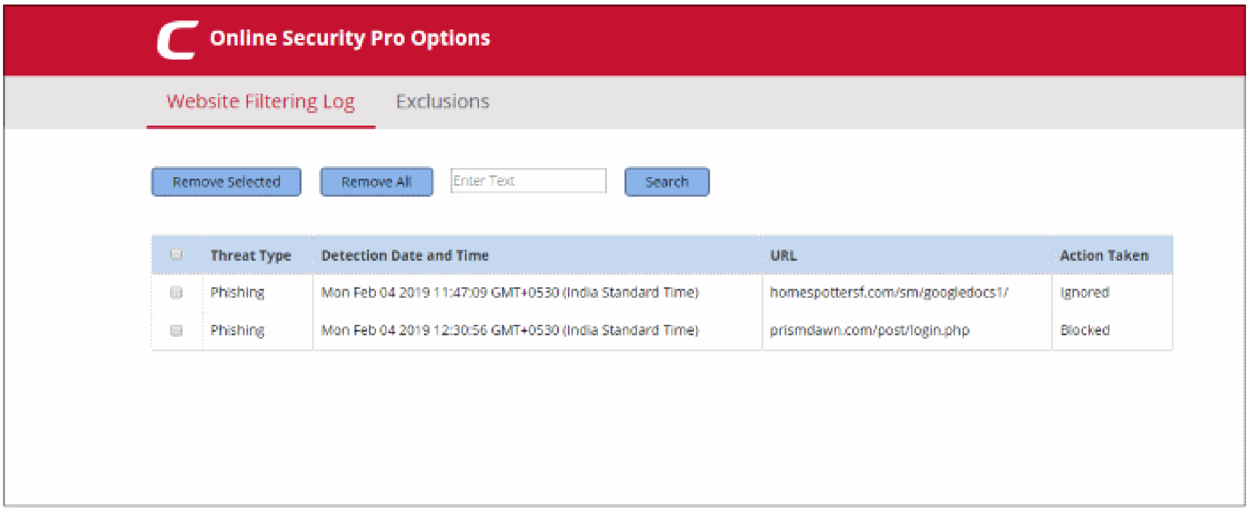
Website filtering log page shows the details of URLs that were blocked by COS and action taken by you.

To open the website filtering log page:

- Click COS home icon, then anywhere on the 'Check History' stripe



The 'Website Filtering Log' screen opens:



□	Threat Type	Detection Date and Time	URL	Action Taken
□	Phishing	Mon Feb 04 2019 11:47:09 GMT+0530 (India Standard Time)	homespottersf.com/sm/googledocs1/	Ignored
□	Phishing	Mon Feb 04 2019 12:30:56 GMT+0530 (India Standard Time)	prismdawn.com/post/login.php	Blocked

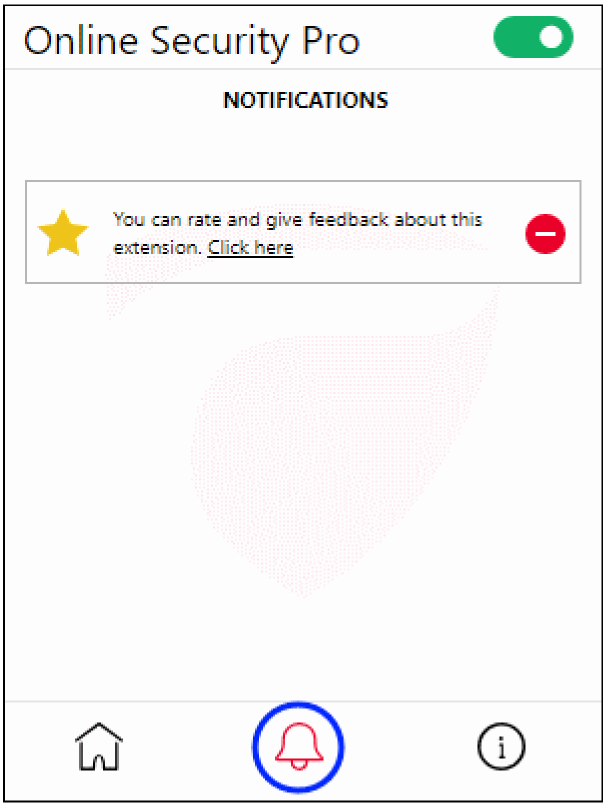
  - **Threat type** – Category of attack found at the URL. Examples include 'Phishing' (fake/fraud websites) and 'Malware' (the site hosts viruses and other threats)
  - **Detected Date and Time** - Date and time the threat was discovered by Comodo Online Security
  - **URL** – The address of the site
  - **Action Taken** – How you responded when you were alerted to the threat. If you clicked 'Continue Anyway' then this will say 'Ignored'.
- Use the search box to look for a particular site
  - Clear the box and click 'Search' again to reset the list

Remove a log record

- Select the check box next to the target site then click 'Remote Selected'
- Click 'Remove All' if you want to clear all logs

Notifications

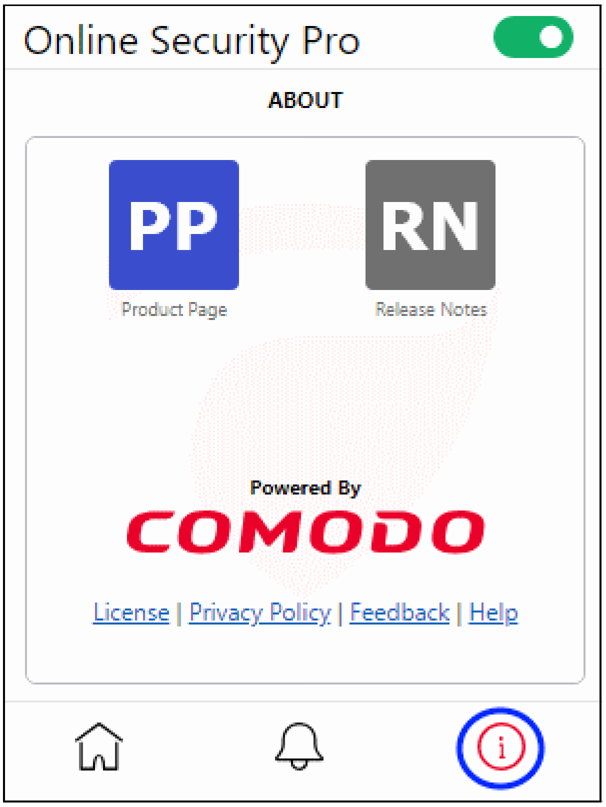
- Click the bell icon to view messages from Comodo. You can also leave feedback about COS from here.



You can rate and give feedback about this extension. Click here

About

- Click the 'About' icon:

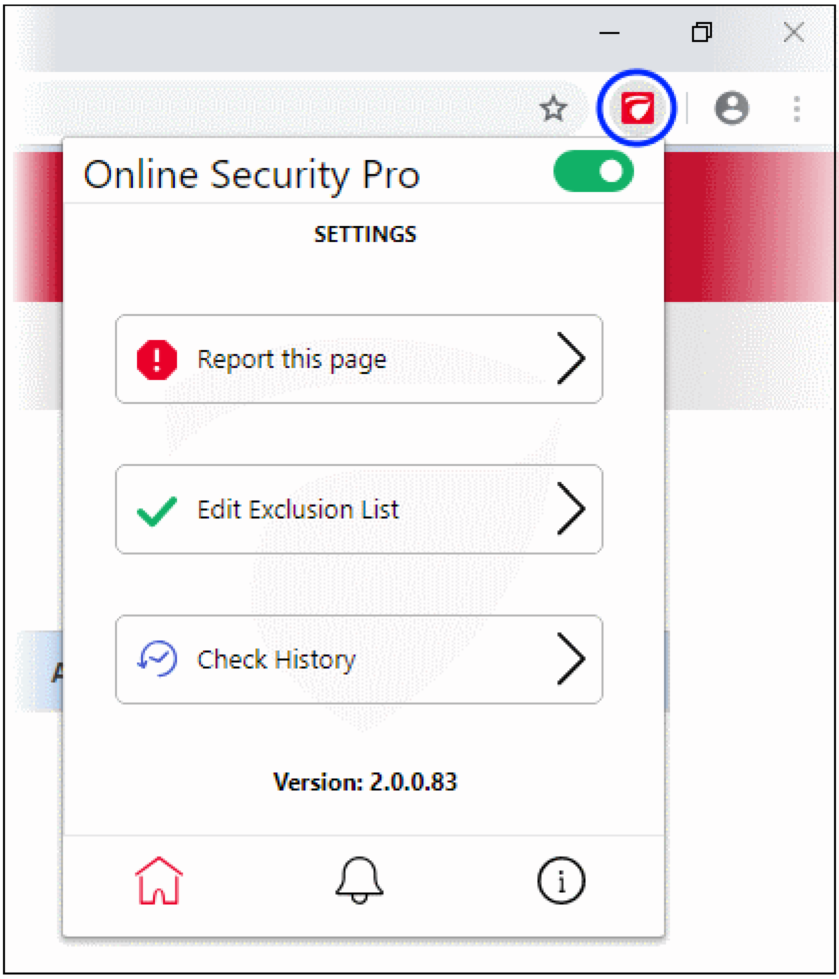


General information about the extension. This includes:

- Links to the release notes and the COS web-page
- Legal information
- A 'Feedback' link which lets you submit product suggestions and report bugs at the Comodo forum.
- Links to privacy policy and COS help page

Chrome: Installation and use

- Visit **https://antivirus.comodo.com/online-security.php**
- Click 'Download for Chrome'. This will open the Chrome extension page for Comodo Online Security
- Click 'Add to Chrome'
- Click 'Add extension' to start the installation
- After successful installation the COS icon will appear in the navigation bar.

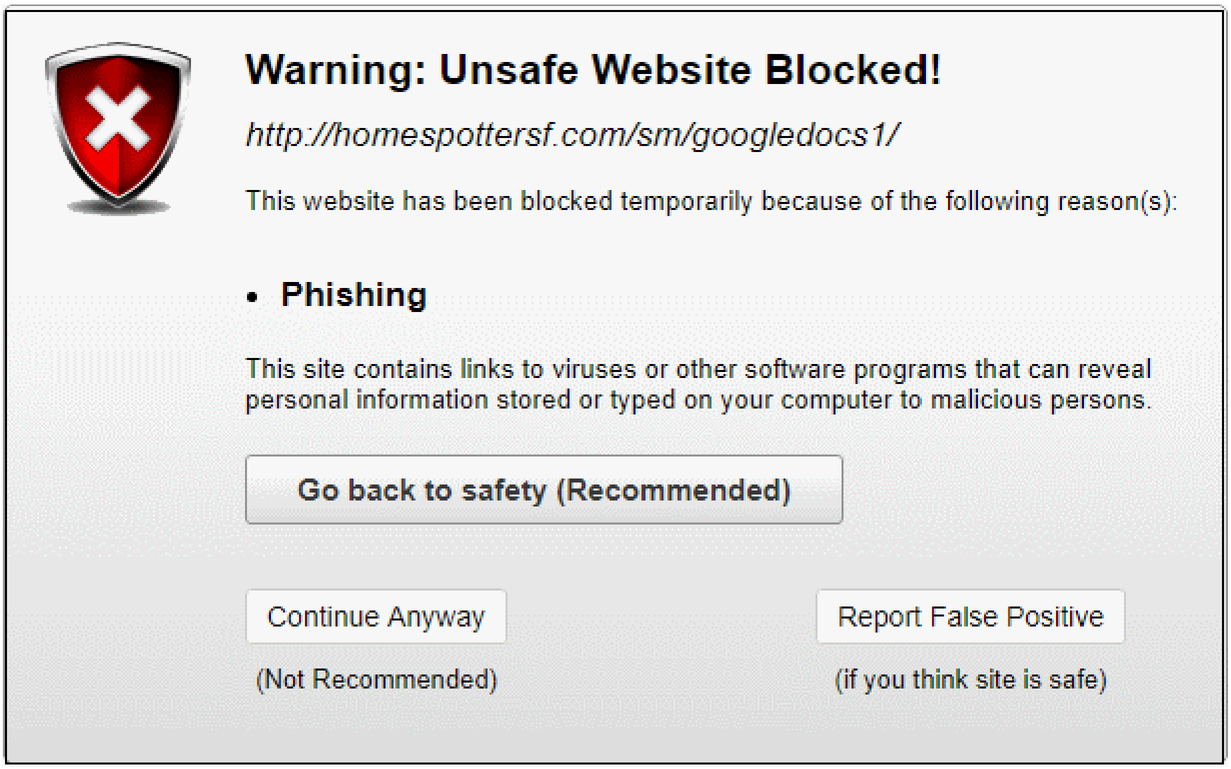


Click the COS icon to reveal the follow options:

- **Comodo Online Security Pro** - Enable or disable the COS web-filter. *(Default = Enabled)*
- **Home icon** – Opens the Settings page:
  - **Report this page** - Submit the URL of the site you currently visiting to Comodo for analysis.
    - You should do this if you think it might be hosting malware, or might be a fake/phishing website. Comodo will test the site and add it to our black list if we confirm it as malicious.
    - Click anywhere on the stripe to open the reporting page at **https://www.comodo.com/home/internet-security/submit.php**
    - The URL is pre-populated, so you just need to enter your email address and any comments you feel would be helpful (optional).
  - **Edit Exclusion List** – COS generates an alert whenever it detects a harmful website. If you choose 'Continue Anyway' at the alert then the site is added to the exclusions list. This means COS will not flag it as malicious on future visits. Click anywhere on the stripe to view/modify web sites on the exclusion list.
  - **Check History** – View a log of sites caught by COS, and the action taken by you.
- **Notifications** – Shows news about COS and allows you to rate the product
- **About** – Links to product pages, release notes and more.

COS Alert

COS shows an alert if the visited website is found to be unsafe:



Warning: Unsafe Website Blocked!

http://homespottersf.com/sm/googledocs1/

This website has been blocked temporarily because of the following reason(s):

- **Phishing**

This site contains links to viruses or other software programs that can reveal personal information stored or typed on your computer to malicious persons.

The alert tells you the name and type of the threat and includes the following options:

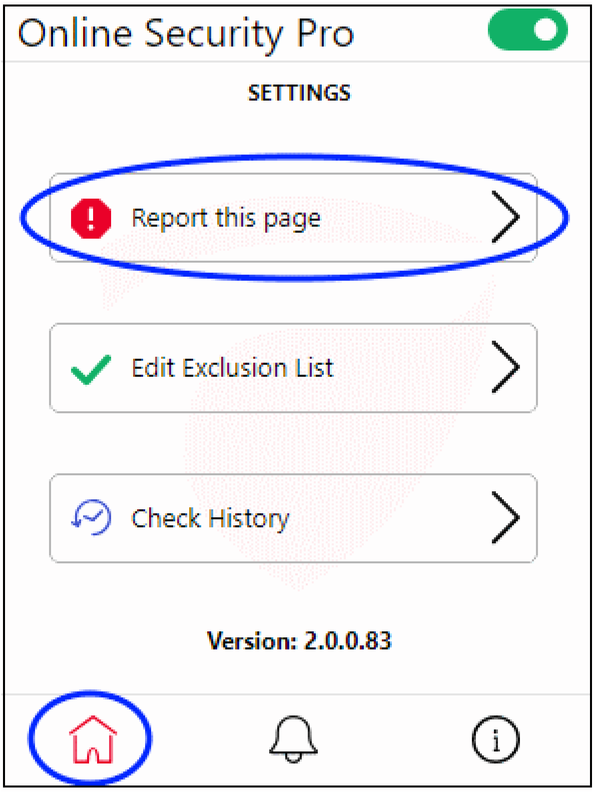
- **Go back to safety** – Closes the web page
- **Continue Anyway** – Ignores the alert and opens the web page. The URL is added to your **exclusions list** so no alert is shown the next time you visit.
- **Report False Positive** – Opens the **report page** at **https://www.comodo.com/home/internet-security/submit.php**. Use this form if you think COS has blocked a page that is safe/ is not harmful.

Report this page

- Make sure you are on the page you want to report.
- If you just want to supply the URL of a new malicious site then we advise you go straight to **https://www.comodo.com/home/internet-security/submit.php** and complete the form.
- To open the reporting screen:
- Click the COS button at top-right
- Click the 'Home' icon
- Click the 'Report this page' stripe

OR

- Click 'Report False Positive' in a COS alert



Online Security Pro

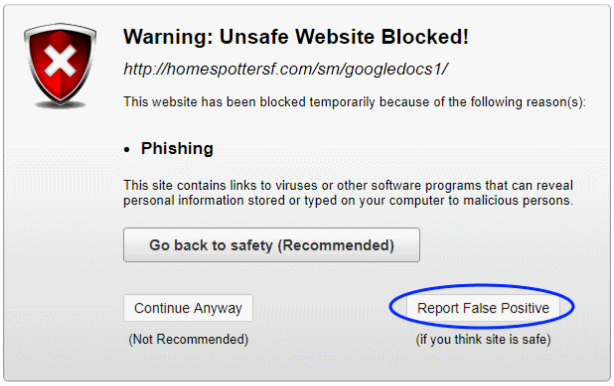
SETTINGS

Report this page

Edit Exclusion List

Check History

Version: 2.0.0.83



Warning: Unsafe Website Blocked!

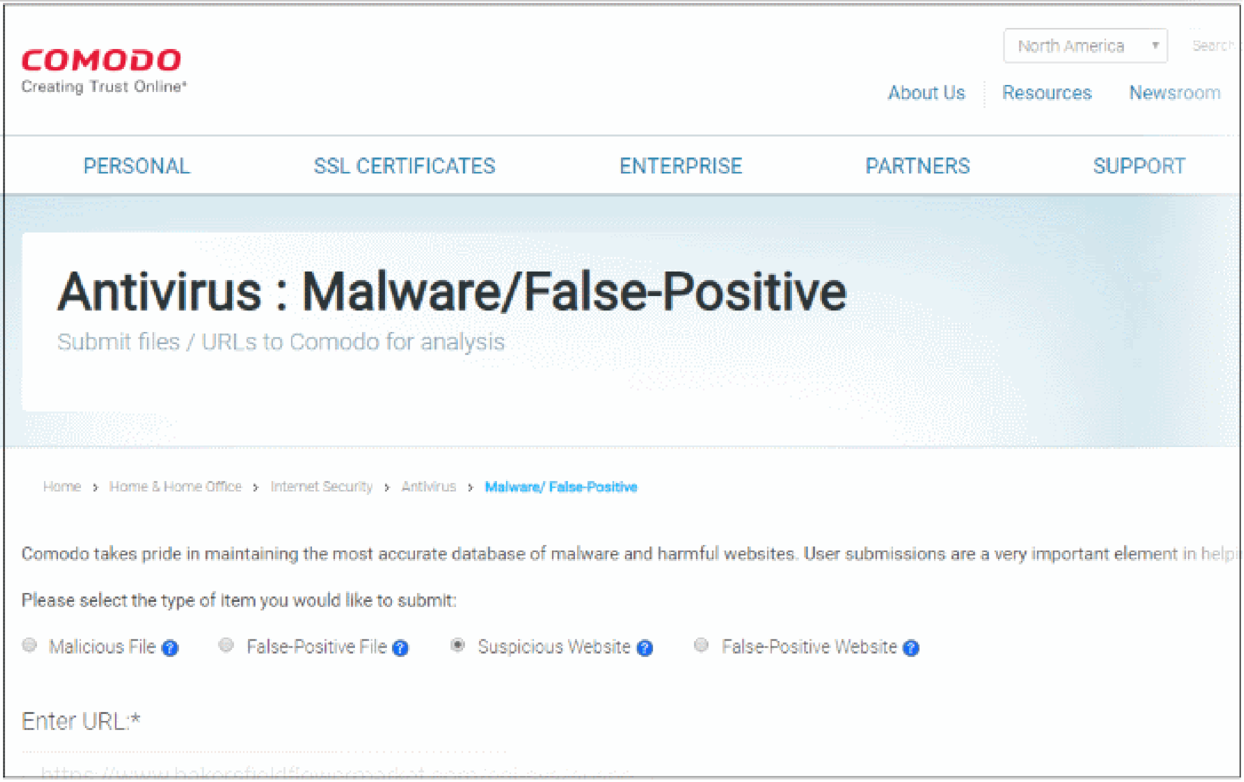
http://homespottersf.com/sm/googledocs1/

This website has been blocked temporarily because of the following reason(s):

- **Phishing**

This site contains links to viruses or other software programs that can reveal personal information stored or typed on your computer to malicious persons.

The 'Antivirus: Malware / False-Positive' screen will open at **https://www.comodo.com/home/internet-security/submit.php**



Antivirus : Malware/False-Positive

Submit files / URLs to Comodo for analysis

Home › Home & Home Office › Internet Security › Antivirus › Malware/ False-Positive

Comodo takes pride in maintaining the most accurate database of malware and harmful websites. User submissions are a very important element in helpi

Please select the type of item you would like to submit:

○ Malicious File ○ False-Positive File ● Suspicious Website ○ False-Positive Website

Enter URL:*

- Enter the URL (if not already populated), your email address, and any comments you feel would be helpful.
- Click 'Submit'

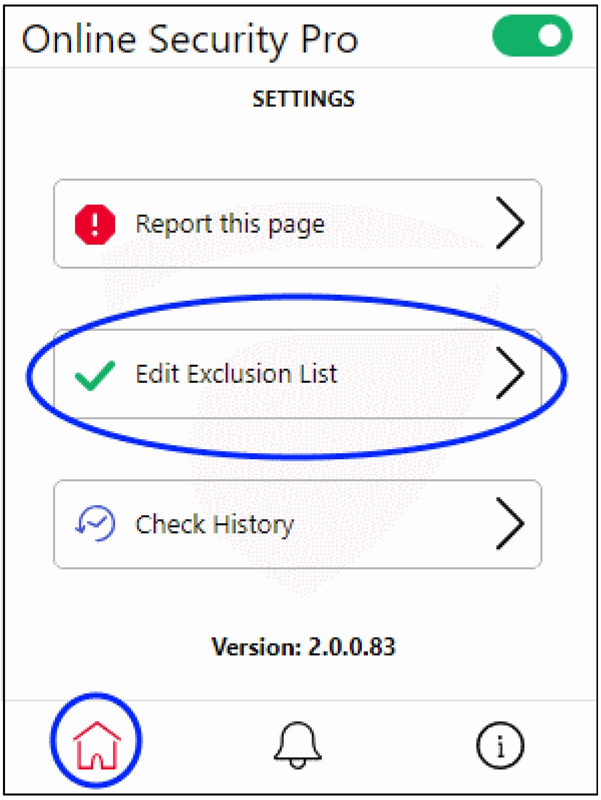
We will check if the reported site is malicious or safe and update our database as required.

Edit Exclusion List

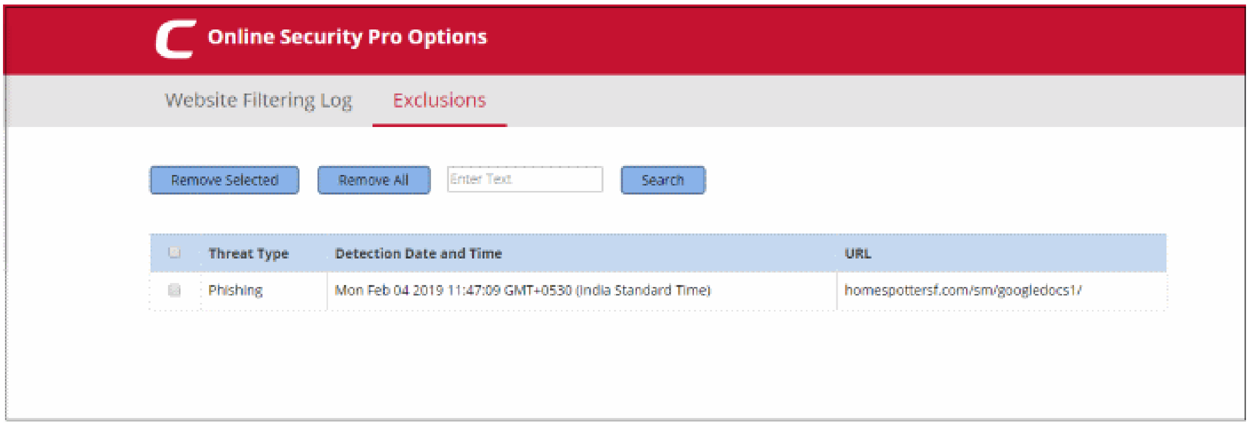
This page shows websites that you have allowed even though COS flagged them as harmful. You can remove URLs from the exclusions list as required.

Open the exclusions list page:

- Click the COS app button at top-right
- Click the home icon, then the 'Edit Exclusion List' stripe



This opens a list of websites that you have allowed:



□	Threat Type	Detection Date and Time	URL
□	Phishing	Mon Feb 04 2019 11:47:09 GMT+0530 (India Standard Time)	homespottersf.com/sm/googledocs1/

- **Threat type** – Category of attack found at the URL. Examples include 'Phishing' (fake/fraud websites) and 'Malware' (the site hosts viruses and other threats)
- **Detected Date and Time** - Date and time the threat was discovered by Comodo Online Security

   - **URL** – The address of the site
- Use the search box to look for a particular site in the list
   - Clear the box and click 'Search' again to reset the list

Remove a site from exclusions

- Select the check box next to the target site then click 'Remote Selected'
- Click 'Remove All' if you want to clear all exclusions.

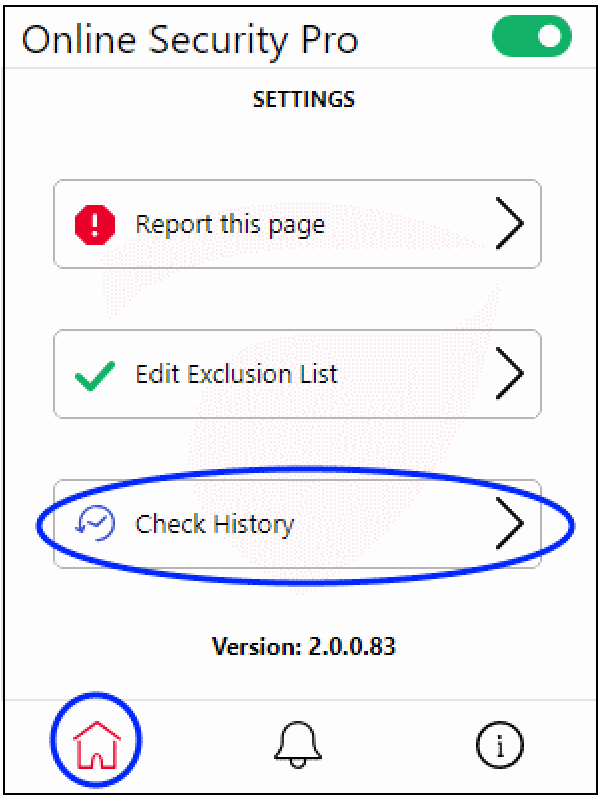
Note – After a website is removed from the list, alerts will be shown when you visit it again.

Check History

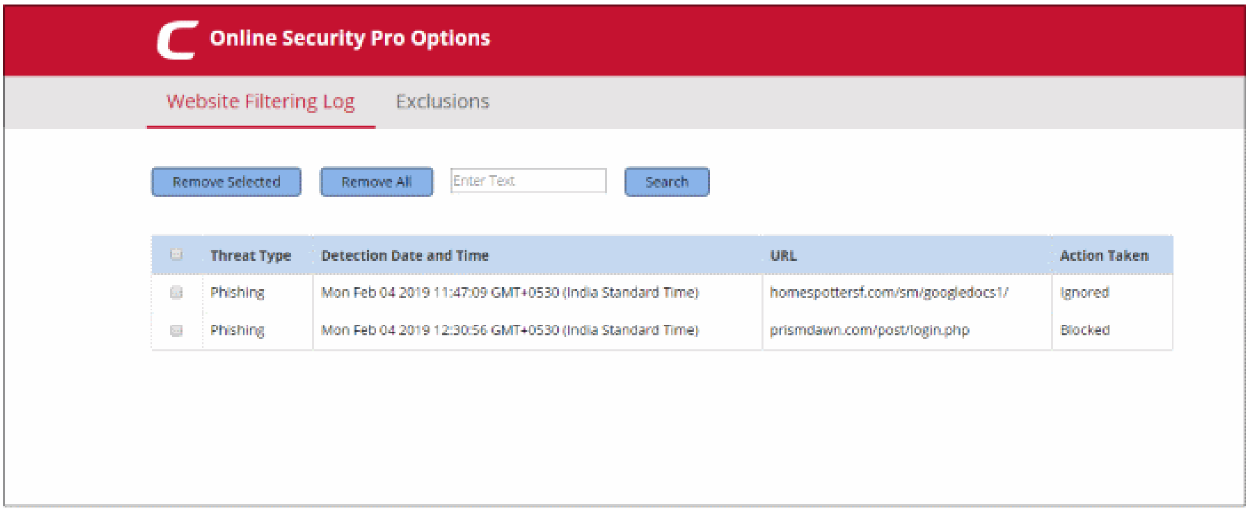
Website filtering log page shows the details of URLs that were blocked by COS and action taken by you.

To open the website filtering log page:

   - Click COS home icon, then anywhere on the 'Check History' stripe



The 'Website Filtering Log' screen opens:



□	Threat Type	Detection Date and Time	URL	Action Taken
□	Phishing	Mon Feb 04 2019 11:47:09 GMT+0530 (India Standard Time)	homespottersf.com/sm/googledocs1/	Ignored
□	Phishing	Mon Feb 04 2019 12:30:56 GMT+0530 (India Standard Time)	prismdawn.com/post/login.php	Blocked

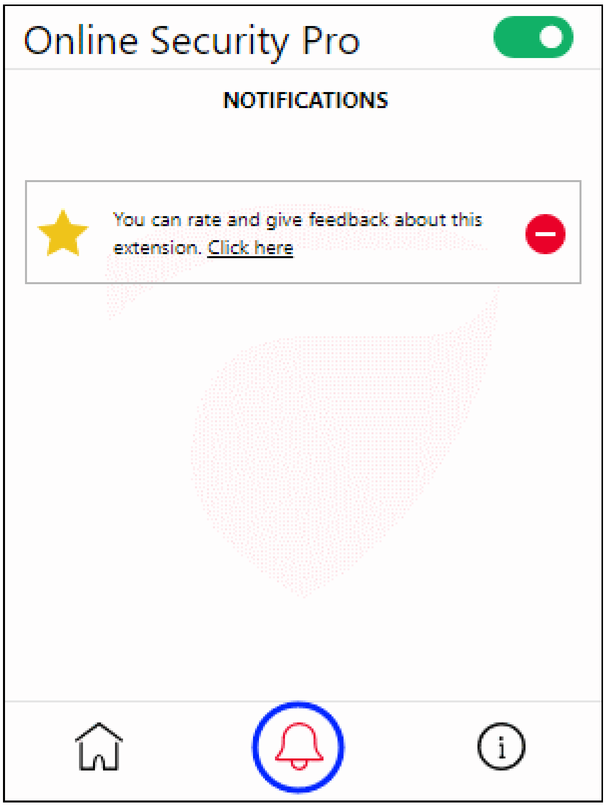
    - **Threat type –** Category of attack found at the URL. Examples include 'Phishing' (fake/fraud websites) and 'Malware' (the site hosts viruses and other threats)
    - **Detected Date and Time** - Date and time the threat was discovered by Comodo Online Security
    - **URL** – The address of the site
    - **Action Taken** – How you responded when you were alerted to the threat. If you clicked 'Continue Anyway' then this will say 'Ignored'.
- Use the search box to look for a particular site
    - Clear the box and click 'Search' again to reset the list

Remove a log record

- Select the check box next to the target site then click 'Remote Selected'
- Click 'Remove All' if you want to clear all logs

Notifications

- Click the bell icon to view messages from Comodo. You can also leave feedback about COS from here.



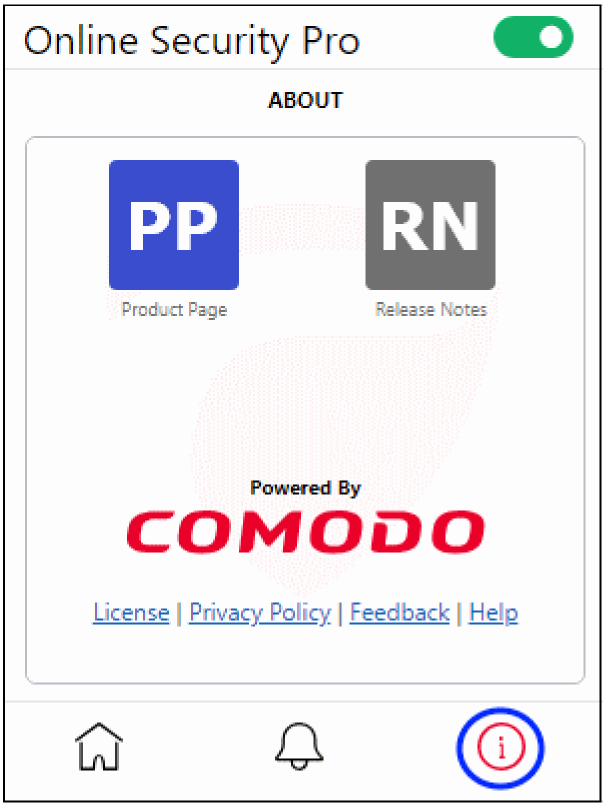
Online Security Pro

NOTIFICATIONS

You can rate and give feedback about this extension. Click here

About

- Click the 'About' icon:

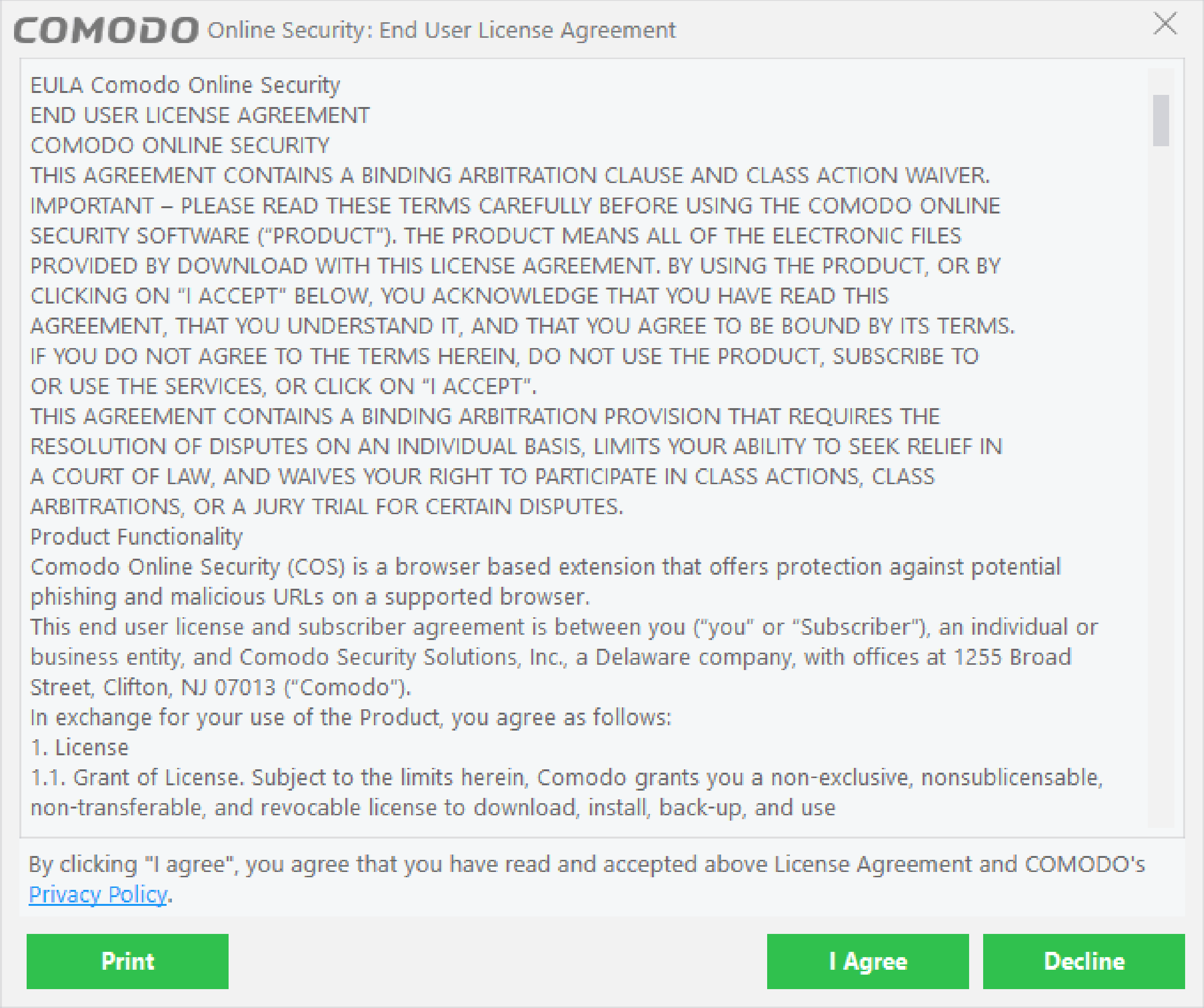


General information about the extension. This includes:

- Links to the release notes and the COS web-page
- Legal information
- A 'Feedback' link which lets you submit product suggestions and report bugs at the Comodo forum.
- Links to privacy policy and COS help page

Internet Explorer : Installation and use

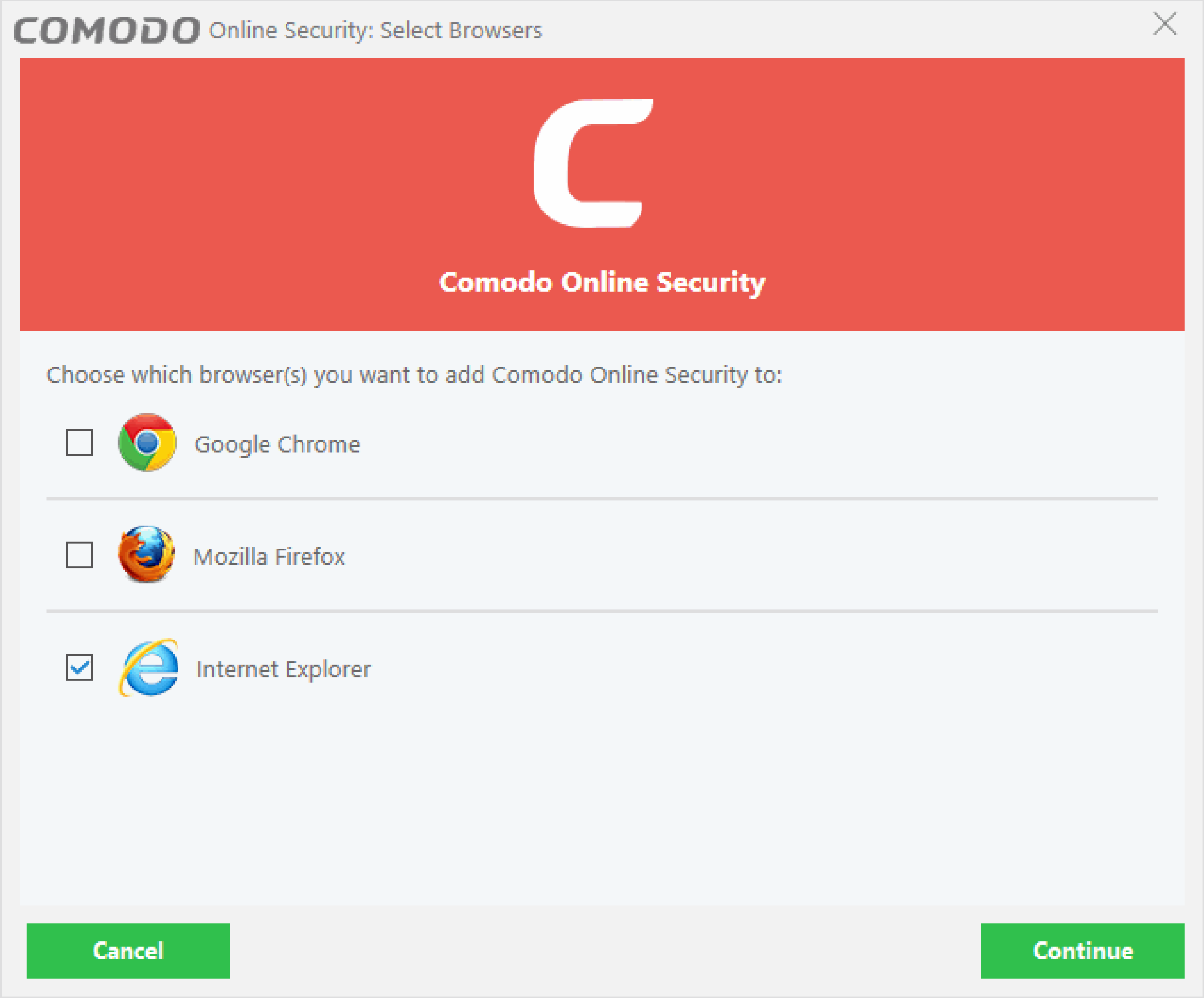
- Download COS from **https://download.comodo.com/cos/installers/cos_installer.exe**
- Run 'setup.exe' to start the installation
- Read and agree the EULA



EULA Comodo Online Security
END USER LICENSE AGREEMENT
COMODO ONLINE SECURITY
THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE AND CLASS ACTION WAIVER.
IMPORTANT – PLEASE READ THESE TERMS CAREFULLY BEFORE USING THE COMODO ONLINE SECURITY SOFTWARE ("PRODUCT"). THE PRODUCT MEANS ALL OF THE ELECTRONIC FILES PROVIDED BY DOWNLOAD WITH THIS LICENSE AGREEMENT. BY USING THE PRODUCT, OR BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS.
IF YOU DO NOT AGREE TO THE TERMS HEREIN, DO NOT USE THE PRODUCT, SUBSCRIBE TO OR USE THE SERVICES, OR CLICK ON "I ACCEPT".
THIS AGREEMENT CONTAINS A BINDING ARBITRATION PROVISION THAT REQUIRES THE RESOLUTION OF DISPUTES ON AN INDIVIDUAL BASIS, LIMITS YOUR ABILITY TO SEEK RELIEF IN A COURT OF LAW, AND WAIVES YOUR RIGHT TO PARTICIPATE IN CLASS ACTIONS, CLASS ARBITRATIONS, OR A JURY TRIAL FOR CERTAIN DISPUTES.
Product Functionality
Comodo Online Security (COS) is a browser based extension that offers protection against potential phishing and malicious URLs on a supported browser.
This end user license and subscriber agreement is between you ("you" or "Subscriber"), an individual or business entity, and Comodo Security Solutions, Inc., a Delaware company, with offices at 1255 Broad Street, Clifton, NJ 07013 ("Comodo").
In exchange for your use of the Product, you agree as follows:
1. License
1.1. Grant of License. Subject to the limits herein, Comodo grants you a non-exclusive, nonsublicensable, non-transferable, and revocable license to download, install, back-up, and use

By clicking "I agree", you agree that you have read and accepted above License Agreement and COMODO's Privacy Policy.

- Click 'Agree' to proceed the next step
- Select all browsers that you want to add the extension to:



COMODO Online Security: Select Browsers

Comodo Online Security

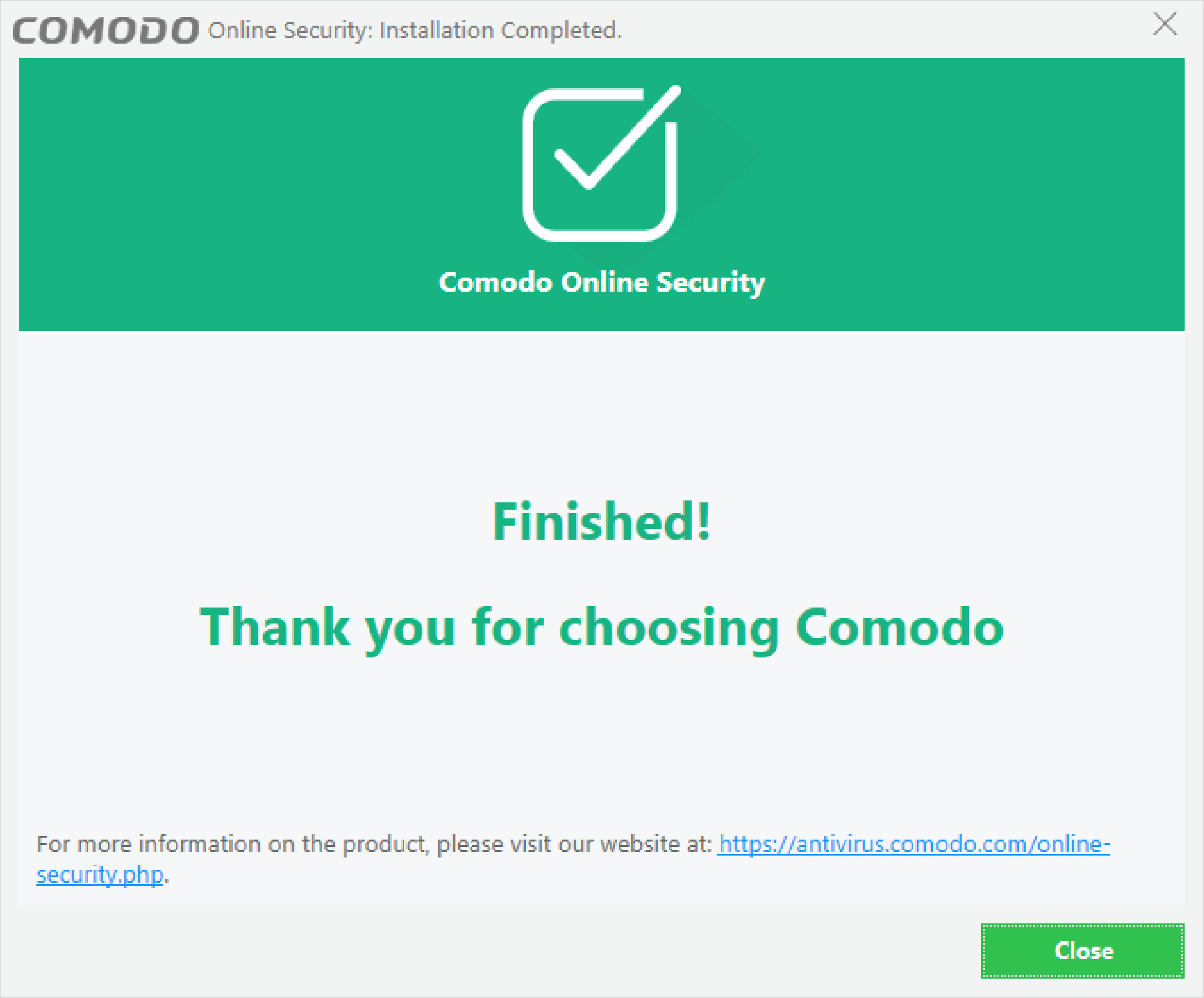
Choose which browser(s) you want to add Comodo Online Security to:

□ Google Chrome

□ Mozilla Firefox

☑ Internet Explorer

- Click 'Continue'



COMODO Online Security: Installation Completed.

Finished!

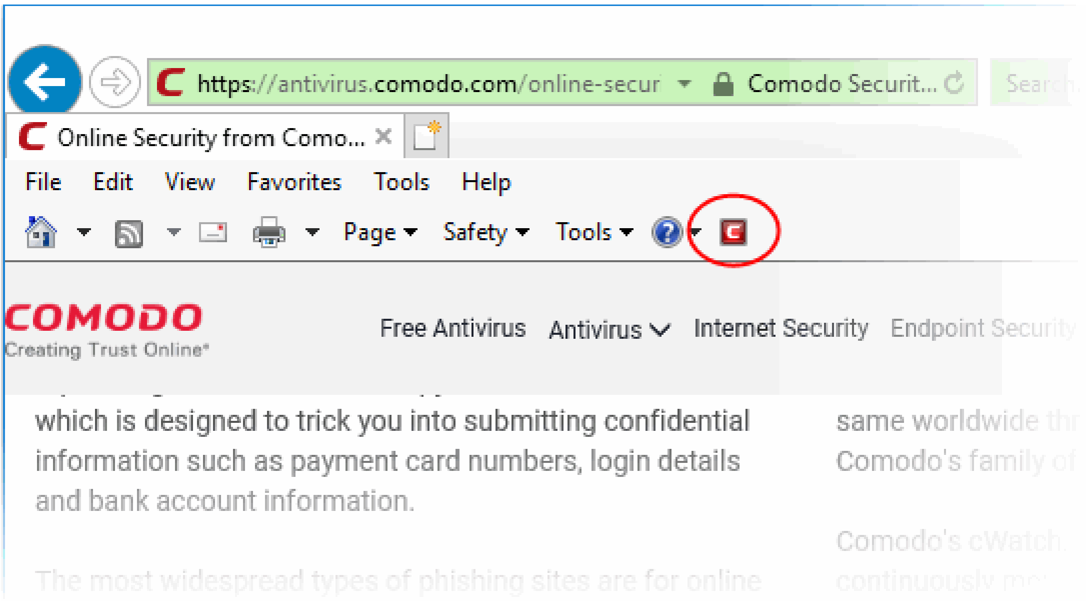
Thank you for choosing Comodo

For more information on the product, please visit our website at: https://antivirus.comodo.com/online-security.php.

- Click 'Close'.

Enable the 'Command bar' to view the COS icon:

- Click 'Tools' > 'View' > 'Command bar'

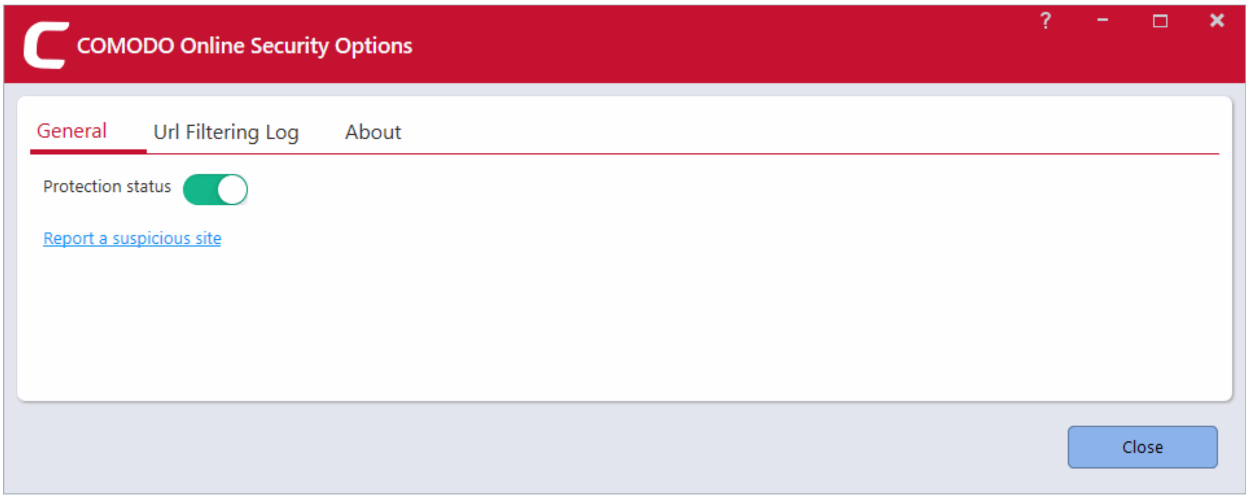


which is designed to trick you into submitting confidential information such as payment card numbers, login details and bank account information.

Click the COS icon to view the COS configuration interface. The interface contains links for general information, the URL filtering log and the 'About' section. These sections are covered in more detail below:

'General'

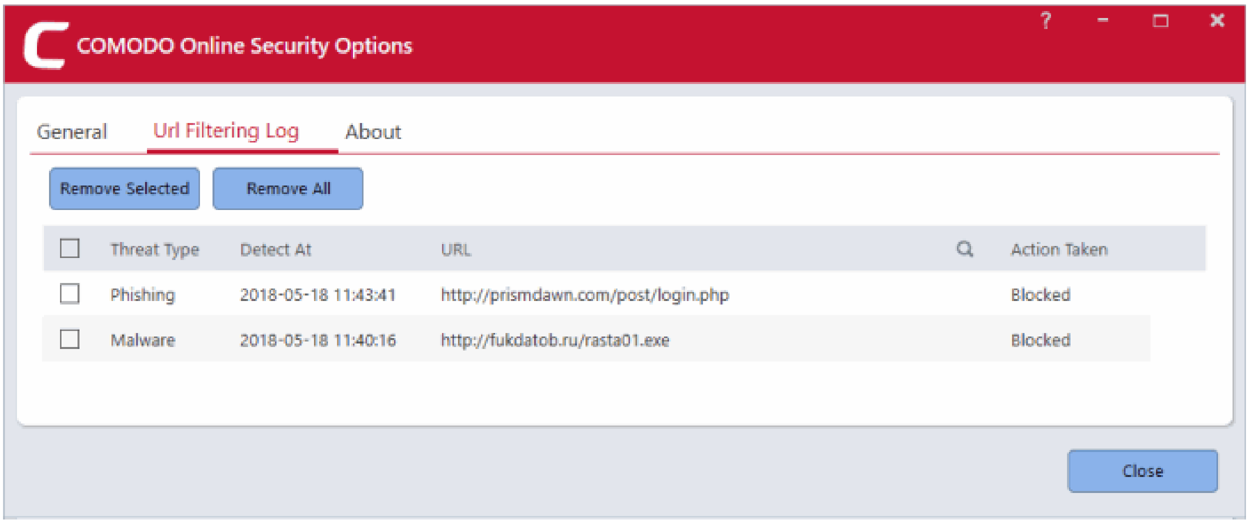
- **Protection status** - Enable or disable the COS web-filter. Default = Enabled
- **Report a suspicious site** - opens the COS submission page at **https://www.comodo.com/home/internet-security/submit.php**



Protection status: Enabled

Url Filtering Log'

Lists all websites blocked by Comodo Online Security.



□	Threat Type	Detect At	URL	Action Taken
□	Phishing	2018-05-18 11:43:41	http://prismdawn.com/post/login.php	Blocked
□	Malware	2018-05-18 11:40:16	http://fukdatob.ru/rasta01.exe	Blocked

- **Threat type -** Category of attack found at the URL. Examples include 'Phishing' (fake/fraud websites) and 'Malware' (the site hosts viruses and other threats).
- **Detected At -** Time and date the threat was discovered by Comodo Online Security.
- **URL -** The address of the site.
- **Action Taken -** How Comodo Online Security responded to the threat.

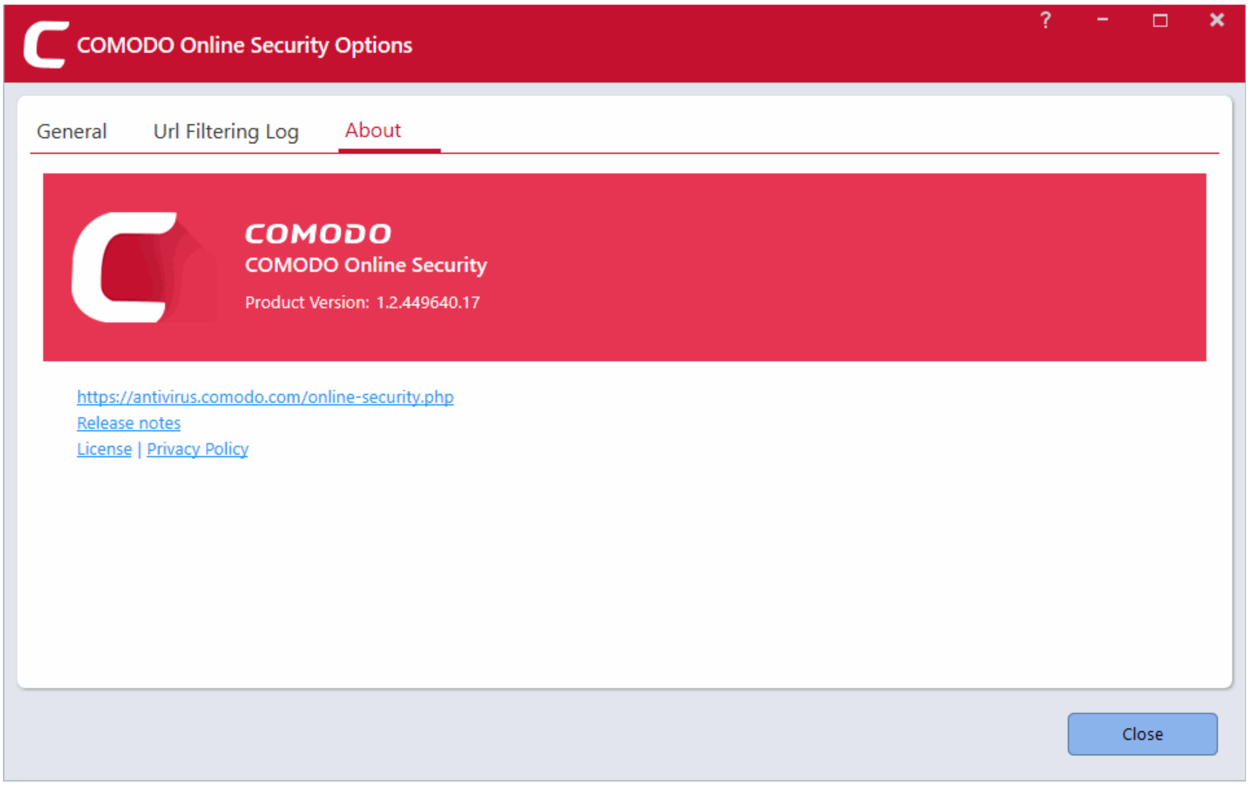
Use the 'Remove Selected' and 'Remove All' buttons to delete selected log entries. Use the 'Search' field to look for a particular log.

'About'

General information about the extension. This includes:

- The software version number
- Links to the release notes and the COS web-page

- Legal information
- A 'Feedback' link which lets you submit product suggestions and report bugs at the Comodo forum.

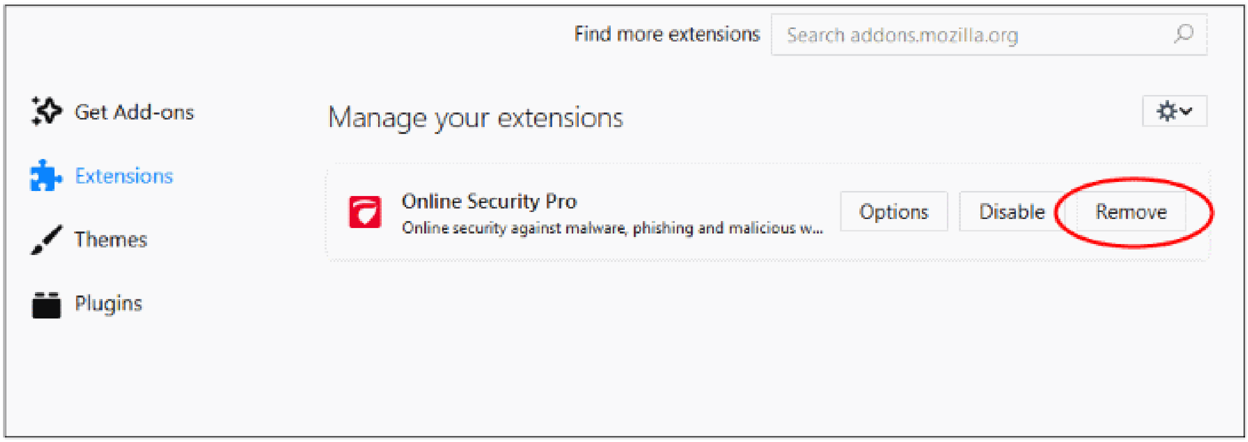


COMODO Online Security Options
? – □ ✕
General
Url Filtering Log
About
COMODO
COMODO Online Security
Product Version: 1.2.449640.17
https://antivirus.comodo.com/online-security.php
Release notes
License | Privacy Policy
Close

Remove extension from Firefox

- Open Firefox
- Click the hamburger menu at top-right
- Select 'Add-ons'

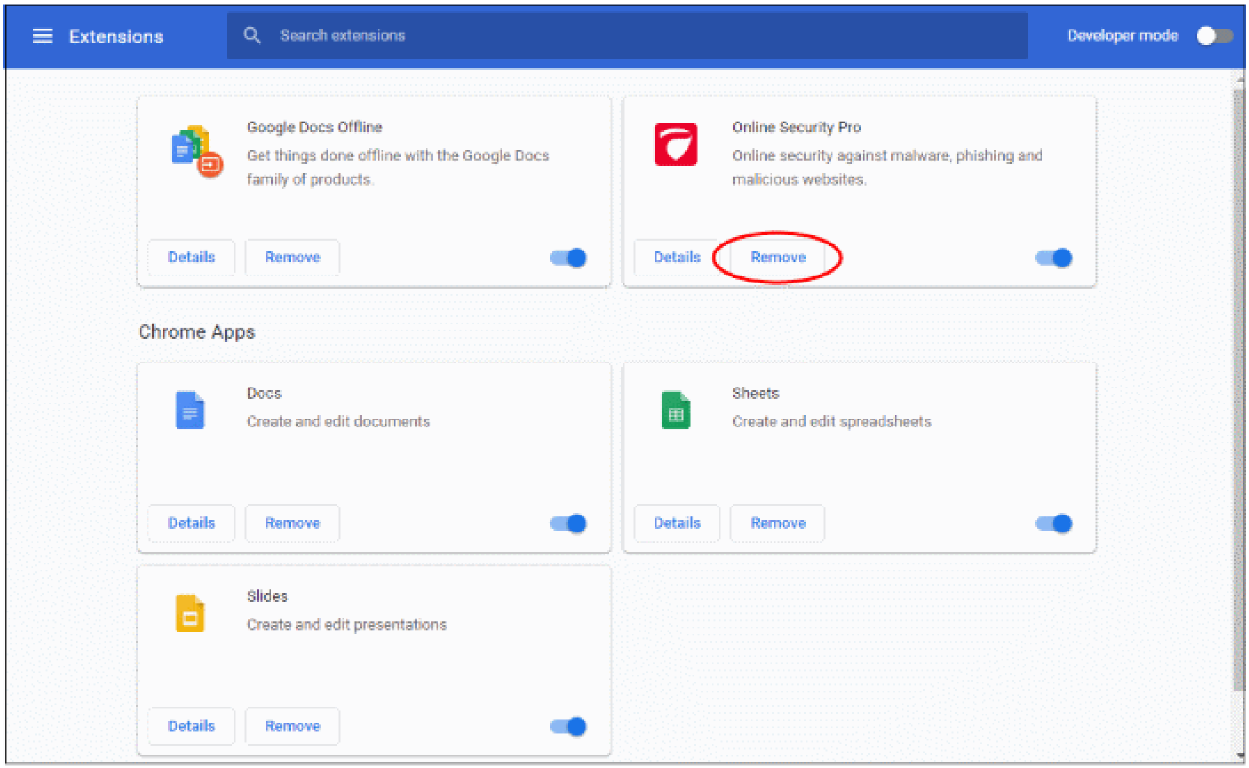
  OR
- Enter **about:addons** into your address bar and press return
- In the 'Extensions' tab, click 'Remove' button.



- Alternatively, click 'Disable' to temporarily pause protection.

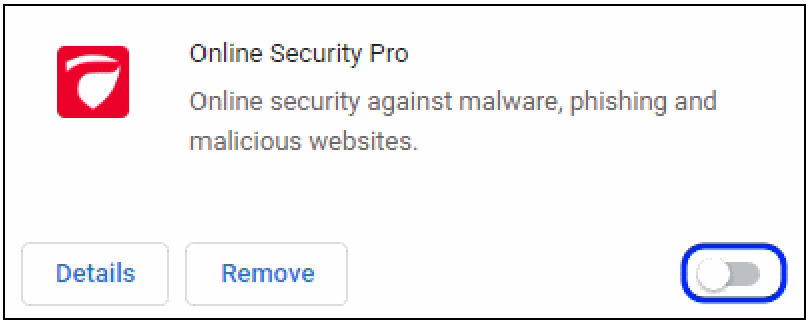
Remove extension from Chrome

- Open Chrome
- Click the hamburger menu at top-right
- Select 'More tools' > 'Extensions' tab
- Select 'Remove'.


Extensions
Search extensions
Developer mode
Google Docs Offline
Get things done offline with the Google Docs family of products.
Details
Remove
Online Security Pro
Online security against malware, phishing and malicious websites.
Details
Remove
Chrome Apps
Docs
Create and edit documents
Details
Remove
Sheets
Create and edit spreadsheets
Details
Remove
Slides
Create and edit presentations
Details
Remove

- Click 'Remove' in the confirmation dialog

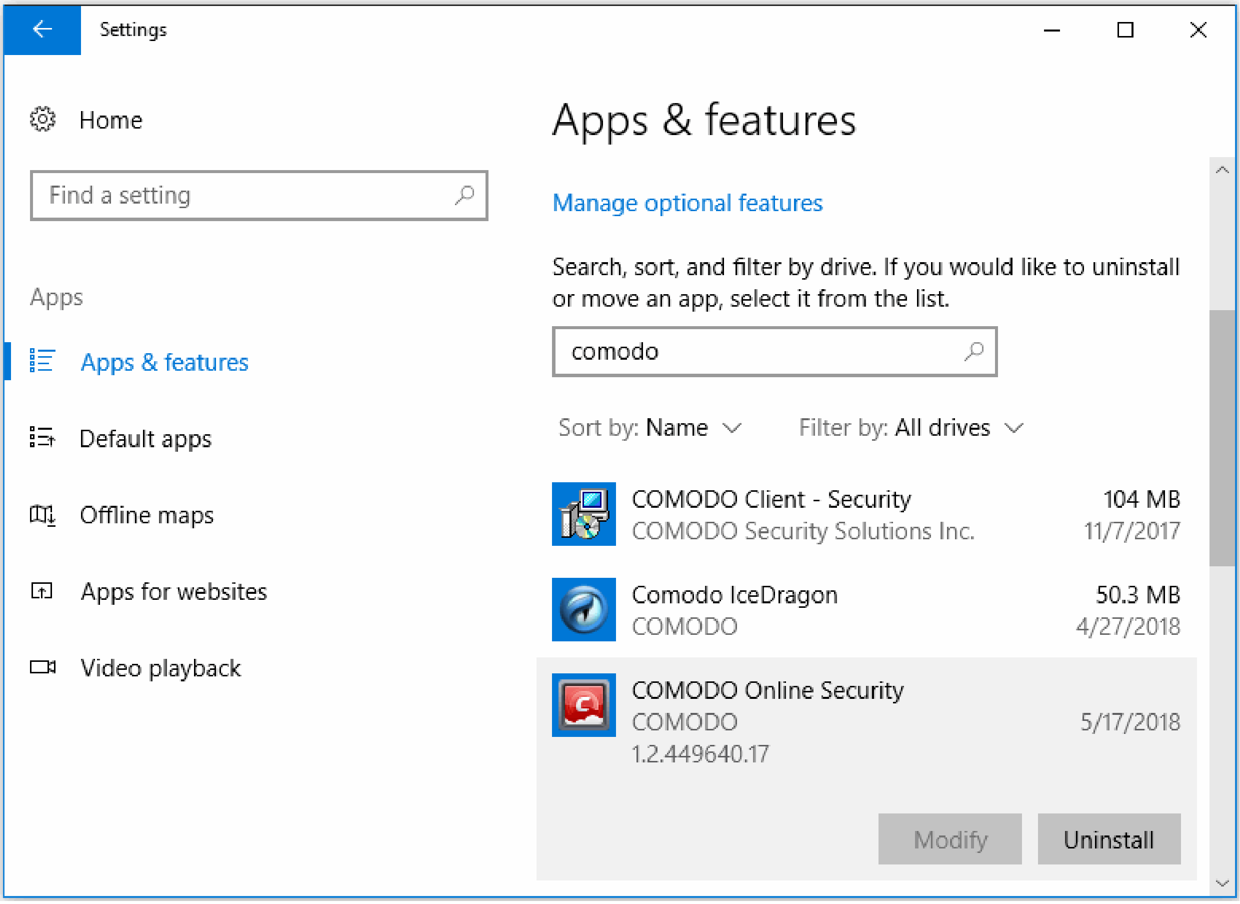
  OR
- Enter **chrome://extensions** into your address bar and press return
- Click the trash can icon on the right
- Alternatively, use the slider switch to disable COS


Online Security Pro
Online security against malware, phishing and malicious websites.
Details
Remove

Remove extension from Internet Explorer

- Open the Windows control panel and click 'Start' menu
- Select 'Settings' > Apps'
- Select 'Comodo Online Security'

- Click 'Uninstall' button



Settings

Home

Find a setting

Apps

Apps & features

Default apps

Offline maps

Apps for websites

Video playback

Apps & features

Manage optional features

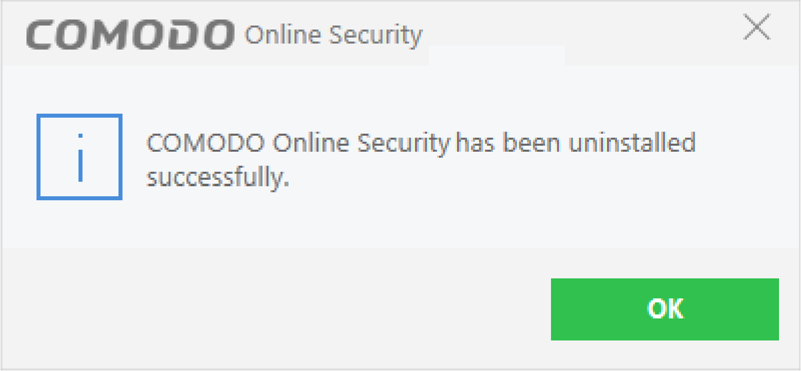
Search, sort, and filter by drive. If you would like to uninstall or move an app, select it from the list.

comodo

Sort by: Name   Filter by: All drives

COMODO Client - Security	COMODO Security Solutions Inc.	104 MB 11/7/2017
Comodo IceDragon	COMODO	50.3 MB 4/27/2018
COMODO Online Security	COMODO 1.2.449640.17	5/17/2018

- Confirm your removal by clicking the 'Uninstall' again



COMODO Online Security

COMODO Online Security has been uninstalled successfully.

- Click 'OK' to close the dialog.

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit comodo.com or our **blog**. You can also follow us on **Twitter** (@ComodoDesktop) or **LinkedIn**.

1255 Broad Street

Clifton, NJ 07013

Tel : +1.877.712.1309

Tel : +1.888.551.1531

https://www.comodo.com

Email: **EnterpriseSolutions@Comodo.com**