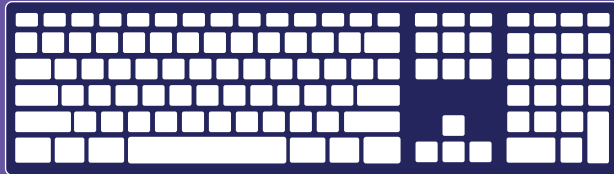


PROTECTING YOUR COMPUTER



How to protect your computer from spyware, document online harassment, and maximize your privacy.

PREVENTING SPYWARE INSTALLATION

On a computer, spyware generally takes the form of a software program running in stealth mode, which makes it difficult to detect or uninstall. It can log every kind of computer activity. Spyware can be installed on your computer using either physical or Internet access.

- 1 DON'T OPEN** suspicious emails and file attachments, as these can carry spyware.
- 2 INSTALL** anti-virus and anti-spyware programs and opt-in to automatic updates and scans.
- 3 BE SUSPICIOUS** of a perpetrator installing a new keyboard / cord / software or updating a computer.
- 4 INSTALL AND ENABLE** a firewall:
Windows XP, 7, 8, 8.1, and 10 include Windows Firewall, which is enabled by default.
On a Mac, the firewall is not enabled by default. To enable it, go to System Preferences > Security > Firewall and choose what mode you would like the firewall to use.

DOCUMENTING

TAKING A SCREENSHOT

On a PC computer, press the Print Screen (or Prt Scr) key. Using a Mac computer, press Command, Shift, and 3 at the same time. Now open a document and click Paste. From there, you can either save the document itself, or you can right click the photo to save it as an image file.

SAVING EMAILS

If you must forward, print, or screenshot an email, be sure to also save the email header, which stores the sender's IP address. It is hidden by default, but you can open it in the message's settings.



1140 N. Hudson Ave, Oklahoma City, OK 73103
405.552.1010 | www.palomarokc.org
Ask for Bekah for tech help.

Palomar and its logo are trademarks of Oklahoma City Family Justice Center, Inc.

 facebook.com/okcfjc

 [@palomarokc](https://twitter.com/palomarokc)





 [@palomarokc](https://instagram.com/palomarokc)

PROTECTING YOUR COMPUTER

INCREASING BROWSER PRIVACY

CLEARING YOUR HISTORY

PRIVATE BROWSING

 Google Chrome	Menu > History > Clear browsing data or Remove selected items	Menu > New Incognito Window
 Internet Explorer	Tools > Internet Options > General > Delete	Tools > Safety > InPrivate Browsing
 Mozilla Firefox	Library > History > Clear Recent History > Select time range > Clear Now	Menu > New Private Window
 Safari 8	History > Clear History and Website Data > Select time period > Clear History	File > New Private Window

USING OPEN / PUBLIC WIFI

USING HTTPS

Ensure that the sites you use on a public network use HTTPS. Communicating with HTTPS encrypts the content of the web page but not the address. Safe activities include web services requiring a username and password. Activities that aren't private even with HTTPS are those which include the information being viewed in the web address.

USING A VPN

The safest method of using a public network is through a Virtual Private Network, which disguises your location, your browsing content, and the information's destination. Generally, you must subscribe to a VPN service on a monthly basis.