

Just a little history on Ransomware to avoid any confusion that may have been spread lately.

Ransomware attacks have been around since 1996, so they are hardly new. Ransomware infect Windows and Apple PCS alike, as do many other viruses. This virus often comes as many computer viruses do, via a user opening and downloading a unknown document usually via email, or by a user being lured to a website which infects you if you go and visit that site (known as a drive by) Thankfully users can mitigate their exposure to ransomware if they keep their browser and windows updated. Modern browsers will often attempt to stop you from going to a risky site with a big stern warning. PC users usually only get in trouble by drive byes if they are going to the shady dark part of the web and doing things they probably shouldn't be doing anyway.

To find out more about ransomware you can visit sites such as wikipedia

<https://en.wikipedia.org/wiki/Ransomware>

As for what ransomware has to do with our Powerpad and Powercomp, the answer is very little. Powerpad and Powercomp are stand alone programs that run on window based PC Devices such as laptops/desktops and tablets. Our software only speaks to vital software as to upload and download data so our exposure to the web is very limited.

So while no Windows Device is ever completely safe from viruses, using common sense and being vigilant to keep windows and your browser updated while also being careful around strange websites and emails will lessen your exposure and allow you to continue using windows devices as you have for decades. Windows after all has been used by and continues to be used by 1.5 billion users.