



Iain Nash @iain_nash *Fri Feb 25 09:37:23 +0000 2022*

There seems to be a lot of questions on Twitter about what can people do to help the people in the Ukraine, and to help ensure they don't get caught up if there is a spill-over from a cyber operation. Here is a little ■ which may help

Update your computers, phones and any other devices that you have. Update your antivirus. Don't click links you don't know, especially if they promise something 'exciting'.

Think about your IoT and routers. There have been cyberattacks over the past few days aimed at stopping Ukrainians from getting access to information and financial services. These are carried out by hacked IoT devices and routers.

The chances of YOUR devices being part of this are very very small, but not zero. If you want to help stop the spread of Fear, Uncertainty and Doubt, think about making sure your devices aren't contributing to the Russian war effort.

Ideally factory reset any devices you have. This will remove any malware which has made its way on to the device. It will also remove any data on the device, so save what you need first on another device. Once this is done, apply any updates which are available.

If your device can't receive updates, or you need to go looking for them, think about getting a new device. Make sure your username and password are unique to the device. If they are 'admin' or 'password', or something similar, change them

It is not easy to tell if your device has become part of a botnet, but in the very small chance that it has, take the time now to refresh your devices and don't let your products become part of a criminal gang or Russian war effort.

You can read a little more about this here (this link is OK to click!): <https://t.co/6oKBBRQ1UO>