Preparing your Personal Device to be secure enough to work with ENMU content

The following is a guideline established to help ensure your own personal device is secure enough while working remotely to be able to safely carry out tasks such as using VPN, One Drive, Remote Desktop, etc.

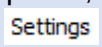
- You must have an Antivirus. ENMU ITS encourages the selection of Bitdefender to this end, since that is what is used for university machines and thus most able to provide troubleshooting for, thought Avast or AVG would also work. ENMU ITS also encourages you to consider purchasing the paid version of one of these three for even better security, but the decision to procure a paid version is at the user's discretion.

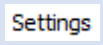
- Windows Firewall must be enabled.

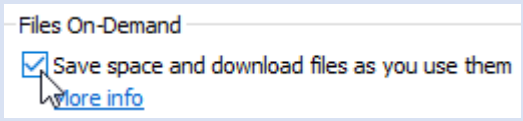
- Install Malwarebytes and run it once a month.

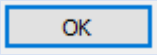
- The machine must have a user name and password, no auto login. The password should also be 10 characters long and have a symbol and a number.

- One Drive needs to have 'Files on Demand' setting checked.
  To do so on a Windows machine:
  - In the File Explorer, Right Click on 

  - Left Click on 

  - Now Left Click on the 

    Tab
  - make sure the 'Files on Demand' box is checked:
    

  - If not, check it by Left Clicking then Left Click 

- Keep in mind at all times that if there is any FERPA data connected to or present on the machine, the entire machine must be protected as if it was sensitive data and be safeguarded to a FERPA standard.

- This document will evolve as Cyber Security best practices in the industry do.

To see additional tutorials, or download this tutorial, visit

ENMU ITS Work From Home

If you need any assistance or have questions, please contact the Help Desk
via Teams by clicking Here
via phone at: **575-562-4357**
via email at: **Help.Desk@enmu.edu**

–ENMU Portales ITS Technical Trainer