Security Reminders for Work At Home
Computers and Data

WHEN IN TRANSIT, DO NOT LEAVE THE COMPUTER IN YOUR VEHICLE. ESPECIALLY WHEN YOU GO TO THE GROCERY STORE. THIS IS A TIME WHEN THIEVES TAKE ADVANTAGE.

Using a personally owned computer for *Work At Home*:

1. You should have **malware/antivirus protection** on the computer. Malwarebytes is free for a while however, you can obtain low cost software from collegebuys.org. The built-in malware protection on Windows OS is just a start and we urge everyone to purchase additional malware/antivirus software when using the Windows operating system.

2. Do not store any work data on your personally owned device. Please use your Office 365 OneDrive. You can access Office 365 and OneDrive through MyPortal.

For those who have a loaner college/district laptop, or may be taking the assigned desktop computer home for *work at home, and* a reminder for those who already have an assigned laptop:

You need to **safeguard** the **data** on the hard drive. Meaning, you should **back up the data** to your Office 365 OneDrive or if you *must* save to an external USB drive, it *must* to be locked up when not in use (under your control).

Do not let anyone else use the assigned district/college computer:

1. Do not let others use this district/college computer to prevent sensitive information from being exposed to others or worse yet altered. Others could go to web sites with malware or worse yet, **ransomware.**

AND *always* Verify Before You Trust!