# Weekly Tech Tips helpdesk@robertstechs.com •319-364-3004

### Did You Know?



There are multiple ways to "restart" a computer? However, the most beneficial way is to do a full restart of the machine. This is not a restart of an application or a logoff. Click the Start button, hover over the arrow next to Shut Down and select Restart. Do this before you leave at night so your computer will be ready in the morning.

### <u>Let Us Reward</u> <u>You!</u>

Do you know of a business struggling with their IT needs? If so, we've got the solution! Go to www.robertstechs.com and refer them under our "About Us" section! They'll receive a free Network Assessment with no strings attached, and if they become a client, you'll be rewarded as well!

## **Computer Security**

RTS handles all of the protection for computers, including spam, antivirus, malware, and other intrusion protection. If there is ever a question on support, please notify us IMMEDIATELY to clarify. Never call the number on the screen if a pop up says you must contact them for an issue. Call RTS right away at 319-364-3004 so we can resolve the issue. Never allow someone to have remote access to a machine unless they are a verified RTS employee. Normally a complete restart of the computer will resolve the problem, but we'll run a scan to verify no damage has occurred.

E-mail spam filtering provides a filter to eliminate many spam emails, but things can still get through. Never open an attachment unless the sender is a known address and the attachment is expected.

### Keyboard Shortcuts

#### Microsoft Word Keyboard Shortcuts

- To open a document, press Ctrl + O
- To save a document, press Ctrl + S
  - To close a document, press Ctrl + W
- To select all, press Ctrl + A

•

- To bold text, press Ctrl + B
- To italicize text, press Ctrl + I
- To underline text, press Ctrl + U



Many of the phishing schemes mask as sent from UPS or other well-known vendors and the attachment looks like an invoice or shipment tracking. Another common type is an e-mail with only a URL (web address) in the text. Attachments which end with .exe or .zip are extremely suspect. All of these items should be deleted. If you try to open an attachment and it won't open, do NOT send it to a coworker to try to open. Contact RTS to mitigate any damage done. Call immediately if you suspect your machine has been infected. Do not wait until RTS stops by to check on things. This may be too late.

### **RTS Contact Info**

871 Shaver Rd NE Cedar Rapids, IA 52402

319-364-3004 helpdesk@robertstechs.com

