UNIVERSITY OF RIO GRANDE AND RIO GRANDE COMMUNITY COLLEGE

RioNET Safe Computing

Updates – Updates – Updates

Maintaining Your Computer: It is important to keep your computer in top working condition!

You MUST keep your computer up-to-date with the latest security & application updates.
RioNET requires all networked devices to be fully updated and clear of all malware.

- **Microsoft Windows Updates & Service Packs – Application Updates**
  Run Windows Updates from http://windowsupdate.microsoft.com
- Apple iOS, Google Chromebooks and Mobile Devices all have OS Updates
- **Application Updates**
  Keep all installed applications updated and uninstall legacy applications that are no longer supported (like Adobe Flash).
- **Driver Updates**
  A driver is software that allows your computer to communicate with hardware or devices. Without drivers, the hardware you connect to your computer—for example, a video card, printer, network card or a webcam—will not work properly.
  Drivers are best downloaded directly through Microsoft Updates or from the hardware manufacturer site and installed following their instructions.

Antivirus (Sometimes questioned as still being effective…)

You SHOULD have a licensed and valid antivirus program installed and active on your system. Check to see if it is installed properly and receiving regular updates. Newer versions of Microsoft Windows come pre-installed with Windows Defender, which updates at the same time Windows does.

Malware (Stand-alone Checkers)

Sometimes bad things get past your defenses, which can get cleaned by a stand-alone checker. Some install to your system while others can be portable and run from a USB flash drive.

- Microsoft Safety Scanner - https://www.microsoft.com/en-us/wdsi/products/scanner
- Emsisoft Free Emergency Toolkit - https://www.emsisoft.com/en/software/eek/
- Malwarebytes Antimalware https://www.malwarebytes.com/mwb-download/
- Norton Security Scan - https://security.symantec.com

UNIVERSITY OF RIO GRANDE AND RIO GRANDE COMMUNITY COLLEGE

Cleaning Browser History and Temp Files

Computers download and save files to re-use plus store history of web sites visited, browsing "cookies" and saved passwords.
While cookies & history can be helpful when returning to known friendly sites, browsers become clogged with too much digital debris and often the browsers get confused and behave badly.
Clearing Browser History and Temporary Files regularly is encouraged.

Browsers typically include, under Tools – Delete Browsing History OR Clear Recent History
The keyboard short-cut is CTRL+SHIFT+DEL (Command + ALT + E on MacOS Safari)

- CCleaner – https://www.ccleaner.com/
- USB Portable version https://www.ccleaner.com/ccleaner/builds

Use Private Browser Windows

Browsers keep track of your website visits and typically save information about your visit.
Private OR Incognito browser sessions do not save or track your visits and do not draw information from the browser's history.

- Typically uses CTRL + SHIFT + P

Toolbars and Downloads

Each time a user is prompted to download an update or installation file, that site will often package other applications to also download & install – AVOID these bundled packages!
Toolbars are a typical bundled package - many come with hidden dangers and sometimes malware.
Too many toolbars, all working at the same time, seriously slow computer speeds.
Malware could be spying or stealing your personal data and information.

- Uninstall ALL toolbars from the Programs applet in Control Panel or from CCleaner.
- Be attentive when doing updates that toolbars and Potentially Unwanted Programs are not included.

Safe Behavior

Surfing the Internet is both fun and informative, but can also expose users and computers to hidden dangers.
Users are encouraged to limit browsing to known familiar sites and those high on search engine results.
Today, many search engines and antivirus security products will screen for "Safe Sites".
Be extremely cautious of links and "hover-over' the link to check them out first for authenticity.
DELETE all suspicious e-mails from unknown senders – Beware of phishing & scams.
NEVER click on attachments or links within e-mail from unknown or suspect senders.
If a "Security" window pops-up and looks suspicious – power off and seek professional assistance.

Safe computing and computer maintenance is learned over time from experience and sometimes the hard way.
Ask for help from knowledgeable and experienced users.
Learn to be a safe user of network connected systems and mobile devices!

Campus Computing & Networking – support@rio.edu – 800-282-7201