Published on *University of Colorado* (https://www.cu.edu)



# Oudated 2015 [1]

# Outdated?

Stephan thought that setting up his new computer was taking too long. So he skipped a few steps including enabling automatic updates. But when a fellow employee's Internet access was blocked because his computer was a danger to the campus network, Stephan realized the errors of his ways.



So Stephan went back to the programs that allowed automatic updates and enabled them, and now also monitors for updates for his other applications and applies them as soon prudent.

Learn more about the recommendatio and policies that are designed to keep your computer up to date, and the campus network safe, at:

## Protection In The Real World

Physically protecting your data is often overlooked (and its importance underestimated) in favor of more technical and dramatic issues such as hacking, viruses, Trojans, and spyware [2]. However, breaches of physical security can be carried out with little or no technical knowledge on the part of an attacker. Moreover, accidents and natural disasters are a part of everyday life, and in the long term, are inevitable. Taking simple steps in your day-to-day routine can help safely manage when and where your data is exposed to unnecessary risk.

- **Laptops and Portable Disks -** Laptops and handheld computers pose special physical security risks. A thief can easily steal the entire computer, including any data stored on its disk as well as network logon passwords that may be saved. If employees use laptops at their desks, they should take them with them when they leave or secure them to a permanent fixture with a cable lock. Portable USB Drives pose much more of a risk, since they can be easily forgotten or stolen. By fastening your drive to a keychain or locking safely in a drawer, you can easily protect your data and always know where it is at any given time. Many drives can be set up with security features like like a password lock and file encryption.

    Information on password protecting your drive can be found here [3].

    Information on different types of cable locks can be found here [4].

- **One Man's Trash...** - Although it might seem ridiculous, criminals can find and steal important data from a place where no sensible human would ever go: the garbage. Throwing away an old USB Drive or CD without wiping them first is a jackpot for a dumpster-diving thief. Since many buildings do not give the same protection to their trash that they give to their offices, dumpsters have become an attractive target for people searching for sensitive employee information. You shred your important documents before throwing them away, shouldn't you do the same for your digital data?
- **A Deadly Find -** You're walking into work one morning and you notice a small, battered USB drive lying in the parking lot. You suspect it was accidentally dropped by one of your coworkers, so once you're inside you plug it in to your computer to get some clues on the original owner's identity. However, unbeknownst to you, this is *exactly* what the original owner had planned from the beginning. The USB drive was loaded with deadly spyware that got to work the moment you plugged it into your machine. While you are sifting through its files trying to find out who to contact, it's sifting through yours, transmitting your information (and the University's) right back to the cyber criminal that planted the thumb drive in the parking lot the night before. Anonymous drives should be treated with caution, especially if they're found in suspicious places. To avoid confusion, don't forget to label yours with the appropriate contact information so it can be safely

returned if it's lost or stolen.








| **UCCS Help Desk** [5] | **CU Denver & Anschutz Help Desk** [6] | **CU Boulder Help** |
|---|---|---|
| 719.225.3536 | 303.724.4357 | 303.735.4357 |
| helpdesk@uccs.edu [8] | UCD-ITS-HELPDESK@ucdenver.edu [9] | help@colorado.ed |

---

**Source URL:**https://www.cu.edu/oudated-2015

**Links**
[1] https://www.cu.edu/oudated-2015 [2] https://www.cu.edu/ois/antivirus
[3] https://www.makeuseof.com/tag/how-to-password-protect-your-usb-stick-3-easy-ways/
[4] https://www.toptenreviews.com/computers/peripherals/ [5] http://www.uccs.edu/~helpdesk/
[6] https://www1.ucdenver.edu/offices/office-of-information-technology/ [7]
https://oit.colorado.edu/support/it-service-center [8] mailto:helpdesk@uccs.edu
[9] mailto:UCD-ITS-HELPDESK@ucdenver.edu [10] mailto:help@colorado.edu [11] mailto:help@cu.edu