



# Western Regional Center

## National Oceanic & Atmospheric Administration

U.S. Department of Commerce



## OCIO Systems Support Seattle IT Updates - February 2013

### Computer updates need computers off, not just locked

Systems Support has been working hard to keep our desktops up to date and secure. This involves remotely installing all the newest updates to Windows, Office, Flash, Java, Acrobat, and other programs.

Many divisions have replaced their old desktop computers with new laptops, and everyone is now using CAC authentication to logon to our machines. Both of these changes have made it more difficult to remotely install updates during the night.

During normal daily use, please **TURN OFF** your computer at the end of the day. This allows us to install updates when the computer is booting or to turn the computer on at night to install while you are not logged on. Just pulling your CAC leaves the system in a condition that prevents us from remotely updating it.

If we are installing a **SPECIAL** software update, we might send an email asking users to LOG OFF, but leave the computer at the "**PRESS Ctrl-Alt-Del to logon**" prompt. This allows the software to update during the night where it disrupts the least number of users.

Fully shutting down each night might involve a change in your preferred shutdown routine, but it will help us keep the machines secure without causing us to manually install the updates on the machines that are locked. We will notify you using email of any one-time changes for Special Updates with specific instructions.

If you have any questions, please call our Helpdesk at x6377 or email us at: [SeattleSSD.HelpDesk@noaa.gov](mailto:SeattleSSD.HelpDesk@noaa.gov).

### February Tech Tips

- **Phishing attacks**

Email phishing attacks use social engineering where criminals try to gather, or fish for, information that can be used for their gain. This can be information about your financial data (credit card numbers, banking information, tax information), or trying to get you to go to a website that might infect your computer. One of the most known phishing attacks is an email asking you for help getting millions of dollars out of some foreign country and you will get a large percentage of the money for your help.

In most cases, previewing a suspicious email is safe if viewed using a web-based email. Normally you must do something more than preview the email to cause a problem. Some clues that might indicate the email is an attack are:

- Emails that create a sense of urgency. "Limited time offer" or "Your purchase was denied"
- Emails that are addressed to "Dear Customer". Any company that you normally do business with should know your name.
- Emails with bad grammar and spelling mistakes. Most businesses will proofread messages before sending them.
- Be suspicious of emails with links. Many times you can hover your mouse pointer over a link to see where it is pointing. Just because the text says "[update.microsoft.com](#)" doesn't mean the link is actually pointing there. If the link uses a shortening service like "[tinyurl.com](#)" or "[bit.ly](#)" you don't know where the link is pointing and should be careful before clicking on it.
- Be suspicious of attachments that you were not expecting. Just because the email says it is from your friend doesn't mean a criminal hasn't already infected their machine and is using their address book to send out infected links and attachments.

If you have concerns or questions about an email, write back to the sender and ask if they truly sent it. The link to a cute cat video from your Aunt Emm might actually be a webpage to infect your computer.

If you have any questions, please call the Computer Helpdesk at 6377.  
Previous Tech Tips located at [www.wrc.noaa.gov/systems/techtips.htm](http://www.wrc.noaa.gov/systems/techtips.htm)