

As the Technology Alerts on the main page are updated, the former alerts will be archived on this page.

Contents

- [1 Alert 05/08/2008 - 04/14/09](#)
- [2 Alert 03/08/2007 - 04/11/07](#)
- [3 Alert 01/29/2007 - 03/08/2007](#)
- [4 Alert 11/16/2006 - 01/29/07](#)
- [5 Alert 10/19/2006 - 11/16/2006](#)
- [6 Alert 08/2006 - 10/19/2006](#)

Alert 05/08/2008 - 04/14/09

Dealing with Office 2007 Documents

Updated 5/8/08



Many new computers are coming with Office 2007 pre-installed. As a result, students may be using the newer version of MS Office. Some instructors may run into problems with students submitting work in the newer Office 2007 format.

If you don't already have Office 2007, [Click Here](#) for some suggestions on how to work with Office 2007 documents.

We **are** currently deploying Office 2007 on new computer installs for faculty and staff. We are also "pushing" Office 2007 out to existing computers on campus.

Faculty and staff may also request that Office 2007 be installed on their office computers. The interface to Office 2007 is quite different from previous versions, so expect a learning curve.

Please [Contact Us](#) if you have questions about this.

[**Click here to view previous Tech Alerts**](#)

Alert 03/08/2007 - 04/11/07



Dial Up Access Being Phased Out

03/08/07

At the end of March 2007, Mesa Community College will be shutting down its aging dial-up equipment. If you are currently a dial-up user, please make plans to switch either a different dial-up provider or a high speed internet provider. This shutdown should only affect faculty and staff - we do not and have not provided dial-up access for students.

If you have any questions please [Contact Us](#).

Alert 01/29/2007 - 03/08/2007



MCC Under Attack by a Series of Viruses

01/29/07

As you may or may not know, many of MCC's computers have been hit with a series of computer viruses. We are in the process of trying to contain and eradicate these threats. These viruses will only affect Microsoft Windows (PC's) - not Macintosh computers running OS X.

Computers that are infected with these viruses may experience the following symptoms:

- Loss of internet connectivity shortly after turning the computer on
- Loss of ability to print
- Loss of ability to reach on-campus servers
- Strange error messages referencing "buffer overflows"

Due to the severity of these attacks, all service technicians have been re-tasked to focus solely on the containment and elimination of these problems. During the next week, this will be their focus. Unfortunately, this means that ANY task that is not immediately related to these viruses will be put on hold. Please [contact TSS](#) with any computer related problems you may have. TSS analysts will be able to determine if your problem is virus-related or not. Most minor problems can be handled immediately by a TSS analyst over the phone. If TSS logs a service call for your particular problem, please be sure to ask them for the service call ID number - in case you have questions or more info related to this problem at a future date.

We appreciate your patience at this time. Please know that the entire IT department is working to alleviate these problems.

If you have any questions please [Contact Us](#).

Alert 11/16/2006 - 01/29/07



Working to Reduce Spam

11/16/2006

With the ever increasing amount of spam that the MCC servers are trying to filter, the IT department is going to need to make some changes in how email is sent from the MCC network. Most users will not even notice the change, but we want you to be aware in case you begin to have problems.

On **December 1st 2006** we will be requiring all outbound email to go through either MCC's or District's email servers. This means you will only be able to send email using the District or MCC email systems. This change will affect users who are using mail clients such as Thunderbird, Mozilla, or Outlook and trying to send out email from non MCC or District accounts (for example, your personal Cox email account). This will not affect web based mail services such as Google, Yahoo, etc.

You may be asking why we are taking this measure. If a computer (or several computers) on campus has been compromised by malware, viruses, or trojans this computer can then become what is known as a "zombie" ([Click here for a definition of a Zombie](#)). These computers can do a number of things, one of which is send more spam email messages. So, by requiring all computers on campus to send all email only through officially sanctioned email servers we can better detect these zombies and keep them from sending spam.

If you have any questions please [Contact Us](#).

Alert 10/19/2006 - 11/16/2006



Spam Email on the Rise

October 19th, 2006

In August of 2006, global email volume was at about 50 billion messages per day. This is expected to rise to 100 billion messages per day in 2008. Over the past year global spam volumes have **TRIPLED**. In the past six weeks alone, there has been a 50% increase in spam email. Right now, MCC's email servers receive over

Previous_Technology_Alerts

100,000 messages per day. Approximately 87% of those messages are spam and are immediately quarantined or deleted.

Both MCC and MEMO email systems have anti-spam devices in place to help reduce the amount of spam that users get. However, spammers are constantly changing the ways that spam messages are created and distributed. As a result, you may see an increase in the amount of spam that reaches your inbox. Please be assured that the anti-spam devices are still functioning. Both MCC's email team and the District MEMO team are constantly working with our anti-spam vendor to help reduce the amount of spam that reaches your inbox.

Alert 08/2006 - 10/19/2006

In order to conform with password guidelines defined by district you may need to change your My MCC password if you have not recently done so.

Password Requirements:

1. Your password must contain at least one lowercase letter.
2. Your password must contain at least one uppercase letter.
3. Your password must contain at least one number.
4. Your password cannot contain any special characters.
5. Your password must be exactly seven or eight characters in length.

Please log in to the [MyMCC portal](#) and use the Change Password tool under the My Tools tab.

Alternately, you can use the [Forgotten Password Utility](#) to change your password.

Passwords that did not conform to the new guidelines have been automatically locked out as of **September 5, 2006**.

If you have not changed your password before that date, you will need to use the [Forgotten Password Utility](#) to reset your password.

Please note that when you change your password, it will take a minimum of 20 minutes before the new password will work.

If you have questions about this process please contact the Technology Support Services call center at 480-461-7217, or email us at tss@mcmail.maricopa.edu
