

Mid South Area

Computer Support Newsletter

eAuthentication Questions and Answers

Computer Support Newsletter

This newsletter is published mainly to inform MSA employees of Information Technology (IT) news and happenings. Please remember to send all requests for IT help to: MSA-Helpdesk@ars.usda.gov

Inside this issue:

eAuthentication Questions and Answers 1

Microsoft Office 2007 and AgLearn 1

Outlook and Large File Attachments 2

From OCIO Cyber Security Staff 2

Flash Drive Removal 2

Microsoft Outlook Tips 3

More Tips and Tricks 3

FY09 Annual Security Awareness Training 3

Cyber Security Highlight 4

It is critical that all USDA-ARS employees be eAuthenticated and keep up with their user ID and password. This ID and password allows access to AgLearn, GovTrip, e-OPF, NFC Employee Personal Page and eventually Web TA, the new Time and Attendance system.

Q. Why does eAuthentication system require such complicated passwords?

A. eAuthentication protects web sites that involve submitting personal and private information as well as financial transactions via the Internet. eAuthentication security standards are consistent with those established by the National Institutes for Standards and Tech-

nology (NIST), which determines the standards for the Federal Government.

Q. Why is the complexity of my password important to Protecting Privacy at USDA?

A. The USDA eAuthentication Service enables USDA customers to confidently share data and conduct official business transactions with USDA electronically via the Internet.

Q. What are the criteria and rules governing passwords within the eAuthentication system?

A. Please create a password that you will remember. Your password is case sensitive.

All passwords in eAuthentication must adhere to the following criteria:

- 9 to 12 characters long
- Have one uppercase letter
- Have one lowercase letter
- At least 1 of the following characters:
0 1 2 3 4 5 6 7 8 9
! # \$ % = + : ; , ? ~ * -

Do Not Use:

- Dictionary Words
- Profile Information such as mother's maiden name, date of birth, PIN, your name, address, phone number, email, etc.

Your password will expire after 180 days



Microsoft Office 2007 and AgLearn

Many of the MSA locations have already begun implementing MS Office 2007.

There are four new features in MS Office 2007:

1. The Office Button replaces the File menu.
2. The Ribbon contains all the commands logically grouped under Tabs.
3. Galleries offer live preview features
4. Quick Access contains frequently used commands

To prepare for MS Office 2007, [AgLearn](#) is offering several courses. **Microsoft Office 2007: New Features** is an excellent course to begin with. You can self assign the curriculum to your learning plan. Simply log on the

AgLearn using your eAuthentication credentials, type “**Microsoft Office 2007: New Features**” in the search box and click on Go. You will then click on the “Self Assign Curriculum” button to add the course to your learning plan.

There are also advanced courses available for Word, Access, Excel and Outlook 2007.

Outlook and Large File Attachments

Unlike our GroupWise system, when the server was local, sending large file attachments to email distribution groups through Outlook causes the email system and network resources to be unavailable to intended users.

If you are sending email that is posted on a website, please reference the URL (<http://....>) in the message of the email and DO NOT attach the file to your email.

Large email attachments sent to a few email users do not present a network resource problem unless the file is sent during peak hours and exceeds 5MB.

File attachments that are considered emergency releases are not restricted; but if the attachment is greater than 2 MB and is sent to ARS-MSA-ALL, delivery will be delayed based on network availability.

When you attach a file you will

see the size of the file displayed.

Points to Remember:

- An email attachment greater than 1MB sent to ARS-MSA-ALL can cause a Denial of Service attack which cripples our network resources, including email, FFIS, ARIS, BV-Admin, as well as other applications
- Email attachments greater than 2MB sent to various email groups can stall our
- Email attachments greater than 5MB sent to various email groups can stall our network more than 2 hours
- Depending on the time of day the email is sent, an email attachment greater than 5 MB can stall our network resources (email, FFIS, ARIS, BV-Admin, etc.) for 5 hours or more

From OCIO Cyber Security Staff

Cyber Security for Electronic Devices

When you think about cyber security, remember that electronics such as cell phones and PDAs may also be vulnerable to attack. To find out more, [click here](#).

Debunking Some Common Myths

There are some common myths that may influence your online security practices. Knowing the truth will allow you to make better decisions about how to protect yourself. [Click here](#) to read more.

Preventing and Responding to Identity Theft

Identity theft is a crime that can have substantial financial and emotional consequences. Take precautions with personal information; and if you become a victim, act immediately to minimize the damage. You can be a victim of identity theft even if you never use a computer.

[Click here](#) for more information.



Flash Drive Removal

Are you a frequent flash drive user? These days most of us are. After all, flash drives are simple to use and inexpensive.

If you want to make sure your flash drive has a long and useful life, you must take steps to protect it.

To keep your flash drive working, it is important to properly remove it from your computer. Most of us just

pull them out of the USB port and go on about our business.

If a flash drive is repeatedly pulled out of the USB port without properly ejecting or stopping the hardware, over time the drive can become damaged.

One of the recommended methods of removal is to:

- Double click on the Safely Remove Hardware icon located in the bottom system tray.
- Highlight USB Mass Storage Device
- Click on Stop
- Highlight the drive
- Click OK
- You will see a pop up window telling you it is safe to remove the hardware.



Safely Remove Hardware Icon



Microsoft Outlook Tips

Adding Holidays to Your Calendar

Follow these steps to add holidays to your Outlook calendar:

- On the menu bar click **TOOLS**
- Select **OPTIONS**
- Under Calendar area, click the “**Calendar Options**” button
- Under Calendar options area, click the “**Add Holidays....**” button
- Click **OK**

Do you need to resend a message?

- Click the **SENT ITEMS** folder
- Navigate to the message you want to resend
- Double click on the message
- On the menu bar, click **ACTIONS**
- Click **Resend this Message**
- You can change the recipient or edit the text before sending.
- Click **SEND**

How do I recall a message?

Have you ever sent a message and forgot to include the attachment? Follow these instructions for recalling messages:

- Click on the **SENT ITEMS** folder
- Navigate to the message you want to recall
- Double click the message
- On the menu bar, click **ACTIONS**
- Click Recall this Message
- Choose from the options shown
- Click on OK



Recall This Message only works on messages that have not been read by recipients.

More Tips and Tricks

Where did the menus go in Internet Explorer 7?

Have you recently started using IE 7 and cannot find your menus for File, Edit, View, Favorites, Tools and Help? To get them back temporarily, just hit the **ALT** key on your keyboard and the menus will appear. If you want them to stay, click on the **TOOLS** button and choose **Menu Bar**. This will keep the menus for good.

Alt + Tab

For an easy way to scroll through the programs open and running on your computer use the **Alt + Tab** key combination. When you press **Alt + Tab** together at one time and hold them down, it will bring up a box that has all of your open programs listed. Keep the **Alt** key down and press the **Tab** key to scroll through the programs. When you find the one you want, release the **Alt** key to pull that program up.

MSA-Helpdesk

Remember to continue sending requests for assistance to MSA-Helpdesk@ars.usda.gov. Messages sent here are automatically delivered to the Area IT staff.

Past issues of the MSA Computer Support Newsletter can be found on the [MSA Computer Support Website](#).



Internet Explorer 7 (IE7) menus

FY09 Annual Security Awareness Training

The Federal Information Security management Act (FISMA) and the Office of Management and Budget (OMB) Circular A-130 require Federal agencies to provide annual security awareness and privacy basics

training to all employees, contractors, and students.

The course “USDA Information Systems Security Awareness FY09” has been placed in all ARS employees’ AgLearn learning plans.

Unlike last year when there were two security courses to complete, this year there is only one.

All ARS-MSA employees, contractors, and students are to complete this training by December 15, 2008.



Cyber Security Highlight

Celebrating National Cyber Security Awareness Month

Highlights Personal, Business Preparedness During National Cyber Security Awareness Month

October is the National Cyber Security Awareness Month designed to educate the public on the shared responsibility of protecting cyberspace. It is important that all employees and contractors become aware of ways in which we can better safeguard our network communications infrastructure.

There is no single entity which owns the Internet; USDA needs the cooperation of both employees and contractors to protect against a range of cyber incidents that occurs daily. USDA encounters approximately 200,000 attacks monthly to the Network. If you are not familiar with how you can protect and get involved, please contact your Agency Security Officer. Some examples are:

- Employ virus detection software and updates as necessary,
- Use strong passwords and change them frequently,
- Back up important files, and
- Ignore suspicious e-mails and avoid suspicious websites

Report Suspicious Cyber Incidents

- **Unauthorized Changes or Additions**
Has anyone made unauthorized changes or additions to your system's hardware, firmware, or software characteristics without your IT System Security Officer's knowledge, instruction, or consent?
- **Unauthorized Use**
Are unauthorized parties using your system for the processing or storage of data? Are former employees, customers, suppliers, or partners still using your system?

“Protect It Like Your Own”

**Cyber Security Incident Management Team Hotline: 1-888-926-2373
PII Incident Hotline: 1-877-PII-2-YOU**

