

Mid South Area

Computer Support Newsletter

Email all questions and comments to: MSA-HelpDesk@ars.usda.gov

Your Mailbox is Over Its Size Limit



Do you often get the dreaded message from “System Administrator” stating, “Your mailbox has exceeded one or more size limits set by your administrator. The mailbox size is limited to 100MB of message space. You will receive a warning when your mailbox reaches 87040 KB. You may not be able to send or receive new mail until you reduce your mailbox size.”

To make more space available, delete any items that you are no longer using or move them to your personal folder file (.pst). The folders migrated from GroupWise are examples of personal folder files.

Tips to Remember:

- Items in all of your mailbox folders including the Deleted Items and Sent Items folders count against your size limit.
- You must empty the Deleted Items folder after deleting items from other folders or the space will not be freed.
- If you create a folder under the Inbox, the contents of that folder will count against your size limit because the folder is in the Inbox.
- The MessageScreen Quarantine folder does Not count toward mailbox size.

- When sending email over the internet, total message size cannot exceed 10MB.
- Mail sent internally cannot exceed 50MB.
- 1MB = 1,000KB (approx.)
- When you attach a document to your email, Outlook shows the size of the attachment



Inside this issue:

Your Mailbox is Over Its Size Limit

MSA-HelpDesk

New ARSnet Password Policy

MSA IT Password Reset Policy

Useful Tips and News

Cyber Security Awareness

MSA-Helpdesk

Why do we ask for all IT requests to be sent to the MSA-Helpdesk?

Email sent to MSA-Helpdesk@ars.usda.gov is forwarded to all the staff in the Area IT Office. By sending IT requests to MSA-Helpdesk, your request will be answered quicker, especially in the event the Area IT employee you send your request to is out of the office.

How do I find MSA-Helpdesk in the address book?

- Click on the Address Book icon in Outlook
- In the “Type Name or Select from List” box, type MSA
- You will see MSA-Helpdesk on the list

Thank you for sending all IT requests to:

MSA-Helpdesk@ars.usda.gov



New ARSnet Password Policy

In December 2007, the USDA Chief Information Officer mandated a new USDA-wide password policy. To be in compliance, we are required to modify the ARS password policy. On June 30, 2008, the ARS/OCIO staff will begin implementing the new policy for ARSnet.

As of June 30, when you receive a notification to change your password, you must use at least 12 characters instead of the eight

now required.

Must use at least one of each of the following:

- Lower case alpha
- Upper case alpha
- Numeric
- Special character

The remaining eight characters can be any combination.

Example: Sum2@o8m3Rh0

Other changes:

- Passwords must be changed every 60 days
- After five failed login attempts, your account will be locked
- The system will not allow reuse of the previous 24 passwords you have created.

Remember ARSnet includes:

- Outlook
- SharePoint
- E-Forms
- REE Directory Updates

ARS-OCIO will send out additional password information to ease the transition. Users of ARSnet are expected to be in full compliance by September 30, 2008.

MSA IT Password Reset Policy

The Area It Office's policy for resetting NFC and FFIS/FDW passwords is that passwords are reset on Mondays and Thursdays only.

Why do I have to wait to have my password reset?

Among all of our other IT duties, we reset passwords for approximately 1000 ARSnet accounts and approximately 165 employees on 5 different NFC systems. This amounts to roughly 1,165 password resets.

How can I help?

The most important thing you can do is remember your passwords and change them before they expire.

Remember—

A password should be like a toothbrush. Use it every day; change it regularly; and DON'T share it with friends!



Useful Tips and News

Subway Anyone?

Have you ever needed a subway map for the United States or another country? Click [here](#) to check it out.

Training Resource

[AgLearn](#) has over 3,000 courses available from a variety of sources, such as SkillSoft, that

all USDA employees can use at no additional cost. Take advantage of this opportunity to improve your skills or learn something new. Log on to [AgLearn](#) and get started today.

While there, take a look at [The Enhanced AgLearn Tour](#) to see what all is new in AgLearn.

Keyboard Shortcut

When you leave your desktop you can lock your computer with a keystroke. (You must associate a password with your Windows user account to secure it from unauthorized access.)



(Flying Windows Key + L)

Password Reset Contact Points

ARSnet

(Outlook, SharePoint, eForms, REE Directory Updates)-
AD & Area Admin Office
(Stoneville)—[MSA-Helpdesk](#)
Stoneville—[Kathi Tullos](#)
Auburn—[Betty Shepherd](#)
Baton Rouge—[Gail Champagne](#)
Bowling Green—[Jason Simmons](#)
Lexington—[Gary Schaeffer](#)
Mississippi State—[Gary Burrell](#)
New Orleans—[Hans Wientjes](#)
Oxford—[Tyrone Swearngen](#)
Poplarville—[Susan Herrin](#)

ARIS—[Sandra Hanks](#) and
[Robin Jordan](#)

BRIO—[MSA-Helpdesk](#)

CATS—[Debra Magee](#)

All NFC Programs (except IAS)—
[MSA-Helpdesk](#)

IAS—[REE-IAS-](#)
Help@ars.usda.gov

PCMS/Discoverer—[Terry Jones](#)



Cyber Security Awareness

June 12, 2008

Avoiding Social Engineering and Phishing Attacks

Do not give sensitive information to anyone unless you are sure that they are indeed who they claim to be and that they should have access to the information.

What is a social engineering attack?

To launch a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

What is a Phishing attack?

Phishing is a form of social engineering. Phishing attacks use email or malicious web sites to solicit personal, often financial, information. Attackers may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

If you would like to know more about "phishing," some useful links are:

- Encyclopedia Entry on Phishing: <http://en.wikipedia.org/wiki/Phishing>
- OnGuardOnline Quick Facts on Phishing: <http://onguardonline.gov/phishing.html>
- FTC Consumer Alert: How Not to Get Hooked by a 'Phishing' Scam: <http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.pdf>
- Watch Out for "Phishing" Emails Attempting to Capture Your Personal Information: <http://www.privacyrights.org/ar/phishing.htm>

How do you avoid being a victim?

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.

- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Don't send sensitive information over the Internet before checking a web site's security.
- Pay attention to the URL of a web site. Malicious web sites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).

What do you do if you think you are a victim?

- If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.
- If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
- Consider reporting the attack to the police, and file a report with the Federal Trade Commission (<http://www.ftc.gov/>) or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261.
- If you are the victim of cyber crime, criminal complaints can be filed online with the Internet Crime Complaint Center (IC3) (<http://www.ic3.gov/>), which is a partnership between the [Federal Bureau of Investigation](#) (FBI), the [National White Collar Crime Center](#) (NW3C), and the [Bureau of Justice Assistance](#) (BJA).



Cyber Security Incident Management Team

Cyber Security Incident Hotline: 1-888-926-2373

PII Incident Hotline: 1-877-PII-2-YOU

Cyber Security Awareness Sponsored by:

Office of the Chief Information Officer
Farm Service Agency
Foreign Agricultural Service