

Mid South Area

Computer Support Newsletter

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

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

The Best Defense Against E-mail Attacks

E-mail has become one of the most common ways for hackers and crooks to infect or try to take control of PCs. Their newest trick is adding links to emails that either take you to an infected website or a “Pharmed” website (see article below).

It is said that curiosity kills the cat, and sometimes it tricks us into launching viruses, installing browser-disabling add-ons, or even forking over credit card numbers and passwords. Maybe we are inspired by the false belief that firewalls, antivirus software, and anti-spyware programs protect us

from all viruses, worms, and intrusive programs. But even the best of these shields cannot always protect you from the biggest security threat of all: YOURSELF.

Do not be someone who clicks first and asks questions later. Everyone should consider the following:

- Do not respond to unsolicited (spam) e-mail
- Be skeptical of individuals representing themselves as officials soliciting personal information via e-mail

- Do not click on links contained within an unsolicited e-mail
- Only open attachments from known senders
- Validate the legitimacy of the organization by directly accessing the organization’s website rather than following an alleged link to the site
- Do not provide personal or financial information to anyone who solicits the information via e-mail

Pharming: Is Your Trusted Web Site a Clever Fake?

Inside this issue:

The Best Defense Against E-Mail Attacks
Pharming: Is Your Trusted Web Site a Clever Fake?
Microsoft Windows Update
From OCIO Cybersecurity Staff
Microsoft Outlook Help
MSA News
Helpful Websites

What is Pharming?

“Pharming” is when criminal hackers redirect internet traffic from one web site to a different, identical-looking site in order to trick you into entering your user name and password into the database on the fake site. Banking or similar financial sites are often the target of these attacks, in which criminals try to acquire your personal information in order to access your bank account, steal your identity, or commit other kinds of fraud in your name.

Can't I tell that a web site is false simply by moving the pointer over the links and seeing if the code goes to an apparently random address off the site?

Not necessarily. The false web sites used in pharming scams usually “spoof” their links so they look exactly like the ones you expect to see, even in the code that appears when you move your mouse over them. Also, web sites may change the code in their own links from time to time for various

internal reasons, such as when they are upgrading their software, server platform, and customer traffic analysis method.

If you notice something suspicious about a trusted web site, report it —by telephone if possible —to the business or site owner. It may be a normal glitch or a new update, or it may be a mistake a criminal has made when trying to duplicate a web site.

Microsoft Windows Update

Microsoft Corporation releases security fixes for its products the second Tuesday of every month. Microsoft recently released 11 software updates to plug holes in Windows, Office, Internet Explorer and other products.

Check your Windows Update settings to make sure you are receiving and installing these critical updates. Microsoft Windows Automatic Updates are not always automatic. You must manually install the latest ver-

sion of Microsoft Genuine Advantage software; otherwise Microsoft Automatic Updates will silently stop working.

It is recommended you perform manual checks on a monthly basis to check for any updates. It is also recommended to reboot your computer after applying updates. Some of the updates will not be fully installed until the computer has been shut down and restarted.

To manually check for Windows Updates:

- Open Internet Explorer
- In the toolbar select TOOLS
- In the dropdown menu select WINDOWS UPDATE
- Select EXPRESS to get High Priority Updates (Recommended) or CUSTOM to manually

select which updates to apply

- Click on INSTALL UPDATES
- Follow the prompts to complete the download and installation
- You may be required to reboot your PC to finalize the updates



From OCIO Cybersecurity Staff

Bluetooth Technology

Many electronic devices are now incorporating Bluetooth technology to allow wireless communication with other Bluetooth devices. Before using Bluetooth, it is important to understand what it is, what security risks it presents, and how to protect yourself. [Read more....](#)

How Anonymous are You?

You may think that you are anonymous as you browse web sites, but pieces of information about you are always left behind. You can reduce the amount of information revealed about you by visiting legitimate sites, checking privacy policies, and minimizing the amount of personal information you provide.

[Read more....](#)

Microsoft Word Tip

If you want to quickly zoom in and out within your document, hold down the CTRL key and roll the scroll wheel on your mouse to zoom in and out. This will work in Outlook as long as MS Word is your e-mail editor.



Mouse with Scroll Wheel

Microsoft Outlook Help

Do you ever wonder where you can find quick answers to questions concerning Outlook such as:

- Personalizing Outlook
- Out of office assistant
- Signatures
- Sharing a Calendar
- and many more categories

In the Outlook toolbar, click on  to open Outlook Help. You can then enter your search item or browse Outlook Help. Outlook Help provides links to training demonstrations, step-by-step instructions and general information on selected topics.

This help feature is also available in other Microsoft applications such as Publisher, Word and PowerPoint.

Give it a try the next time you have a question about how to complete a task in Outlook, Publisher, Word or PowerPoint.



Microsoft Outlook Help



MSA News

Vista

There is still a moratorium in place on the purchase of Vista PCs. Do not purchase or use any Vista PCs until the moratorium has been lifted.

Apple iPhone

There are still numerous concerns over the security of iPhones within an enterprise environment. Until further notice, the iPhone is not authorized for use in USDA.

Office Professional 2007

The MSA Admin Office will begin implementing Office Pro 2007 at the beginning of FY09. CDs have been distributed to computer contacts at each location.



Password Resets

The [May/June MSA Computer Support Newsletter](#) included a list of password reset contact points. Please print the list and post it near your desk for quick reference.

MSA-Helpdesk

Remember to send all requests for IT help to MSA-Helpdesk@ars.usda.gov. 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.

FY09 Computer Security Training and Privacy Basics

The AgLearn staff is currently testing a combined course for Computer Security Training and Privacy Basics. It promises to be more “user friendly” than courses in the past. The course should be available in October.

TIP: The key to successfully completing AgLearn Courses is to
FOLLOW
THE
DIRECTIONS!

Helpful Websites

[Mid South Area SharePoint Site](#)-Log in using the same ID and password used for accessing your Outlook e-mail.

[How to Change My Password for ARS Employees](#)-To change your ARSnet password. Used for Outlook, eForms, SharePoint and REE Updaters.

[MSA Computer Support Website](#)-Repository for computer related issues, current and past issues of *The Computer Support Newsletter*, and help for USDA software.

[Outlook Web Access](#)-Used for accessing e-mail when away from your desk. Use the same ID and password used to access e-mail from your desktop setup.

[USDA-ARS-Mid South Area Web Site](#)-Links to all locations in the MSA and information pertaining to the Mid South Area.

