

The Computer Support Newsletter

June 2004

<http://msa.ars.usda.gov/computerhelp>

email news: sntucker@msa-stoneville.ars.usda.gov

Computer Support Newsletter Audience

A note to our many readers.....

This newsletter is published mainly to inform MSA employees of Information Technology (IT) news and happenings. Much of the newsletter will relate to the local user base. If you are NOT at Stoneville, some of the contained items may not be relevant to you.

INSIDE THIS ISSUE

- [Spam](#)
- [Phishing](#)
- [Spyware / Adware](#)
- [Tips / Tricks](#)
- [Agency News](#)

Due to the continue outbreak of new security vulnerabilities, this issue is also being dedicated to desktop security. The need to convey good security practices throughout the MSA can not be emphasized enough. Computer systems and the information they store are valuable resources that need to be protected. Increasingly sophisticated threats can exploit a variety of weaknesses in computer systems and cause significant damage. The key is to understand the security-related problems that you need to think about and solve. If you missed the last issue dedicated to the importance of virus protection, Windows updates and password security, [click here](#) to review.

Spam

What is spam?

Spam is the electronic version of "junk mail." The term refers to unsolicited, often unwanted, email messages. Spam does not necessarily contain viruses, valid messages from legitimate sources could fall into this category.

The Stoneville mail server processes on average about 10,000 messages daily. A significant portion of the messages processed are spam. Over the past eight months we have implemented a spam filtering system which reads all e-mails coming in from the Internet and assigns a score to each one based on various criteria. When a message is flagged as spam it is archived for human inspection later. About once per day, the messages are inspected and the ones which were incorrectly flagged as spam are resubmitted. Spam is a common, and often frustrating, side effect to having an email account.

How can you reduce the amount of spam?

Although you will probably never be able to eliminate spam, there are ways to reduce it.

- Don't give your email address out arbitrarily. Email addresses have become so common that a space for them is often included on any form that asks for your address. It seems harmless, so many people write them in the space provided without

realizing what could happen to that information. Often, these email addresses are sold to or shared with other companies, and suddenly you are receiving emails that you didn't request.

- Check privacy policies. Before submitting your email address online, look for a privacy policy. You should read this policy before submitting your email address or any other personal information so that you know what the owners of the site plan to do with the information.
- Be aware of options selected by default. When you sign up for some online accounts or services, there may be a section that provides you with the option to receive email about other products and services. Sometimes there are options selected by default, so if you do not deselect them, you could begin to receive email from those lists as well.
- Don't follow links in spam messages. Some spam relies on generators that try variations of email addresses at certain domains. If you click a link within an email message or reply to a certain address, you are just confirming that your email address is valid.

The Computer Support Newsletter

June 2004

<http://msa.ars.usda.gov/computerhelp>

email news: sntucker@msa-stoneville.ars.usda.gov

- Consider opening an additional email account for personal at home use. Many domains offer free email accounts. If you frequently submit your email address (for online shopping, signing up for services, or including it on something like a comment card), you should have a personal email account. For security reasons, use of these email accounts on an MSA network is prohibited. Be aware of the [ARS policy](#) that pertains to email use.
- Don't spam other people. Be a responsible and considerate user. Some people consider email forwards a type of spam, so be selective with the messages you redistribute. Don't forward every message to everyone in your address book, and if someone asks that you not forward messages to them, respect their request.

Phishing

What is phishing?

Phishing is an Internet scam where official-looking emails attempt to fool users into disclosing online passwords, user names and other personal information. Victims are usually persuaded to click on a link in an email that directs them to a doctored version of an organization's Web site. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers

are able to convince up to 5% of recipients to respond to them.

How to avoid the "phish" hook

As good as phishing attacks are getting, you can take some relatively easy steps to evade them:

- Be suspicious of any email with urgent requests for personal or professional financial information. They typically ask for information such as usernames, passwords, credit card numbers, social security numbers, etc.
- Don't use the links in an email to get to any web page. Try to log onto the website directly by typing the Web address into your browser.
- Avoid filling out forms in email messages that ask for professional or personal financial information. You should only communicate information such as credit card numbers or account information via a secure website or the telephone. To make sure you're on a secure Web server, check the beginning of the Web address in your browsers address bar - it should be "**https://**" rather than just "http://"
- Ensure that your browser is up to date and security patches are applied, otherwise you

may be fooled.

As phishing attacks become more skillful, consumers have to be more vigilant as well. A little thought before acting on a threatening e-mail can go a long way. For more info on phishing, visit <http://www.antiphishing.org>.

Spyware and Adware

As if spam, viruses, and worms aren't bad enough. Adware and spyware are here to sap the remaining life out of your productivity and privacy.

What is Spyware/Adware?

Spyware is software that sends your personal information to a third party without your permission or knowledge. This can include information about Web sites you visit or something more sensitive like your user name and password.

Adware is software that displays advertisements on your computer. These are ads that inexplicably pop up on your display screen, even if you're not browsing the Internet.

The main problem that most people notice with either kind of program is that they cause performance issues with their computers. For example, Internet Explorer might not work

The Computer Support Newsletter

June 2004

<http://msa.ars.usda.gov/computerhelp>

email news: sntucker@msa-stoneville.ars.usda.gov

properly any more, your computer might hang more frequently, or your computer might slow down significantly.

Unauthorized adware and spyware usually installs on your computer covertly by using one of two methods:

- Tricking you into clicking a link that installs it. Links to spyware can be deceptive. For example, a Web site that's trying to push spyware onto your computer might open a window that looks like a Windows dialog box, and then trick you by installing when you click a Cancel button to close the dialog box.
- Installing freeware that includes it. For example, you might install a free file-sharing program that surreptitiously installs spyware on your computer. File-sharing programs can be a major conveyor of adware.

Once installed, spyware can transmit your personal information and download advertisements 24 hours a day. It can also hijack your browser settings, such as your home page or search page.

How to avoid installing spyware/adware

Companies pushing adware and spyware are relying on two things: your desire for free software and your gullibility. Here's how to

avoid infecting your computer with deceptive software:

- Make sure the programs you install don't contain adware. Many freeware programs do include adware. It's how the publishers make their money. If you're not sure, read the license agreement carefully. If you're still not sure, search Google Groups for the name of the program and the keywords adware or spyware. If you don't find any postings about it, then you're probably OK.
- Don't unwittingly install adware or software. If you do click what seems like an innocent link, and then you see a dialog box asking if you want to install a program, don't click the Yes button to install the software.
- Adjust your Internet Explorer 6 (Web browser) security settings. You can adjust your Web browser's security settings to determine how much or how little information you are willing to accept from a Web site. The higher the security level, the lower the risk. The downside: using the highest security levels may make Web sites less usable. [Click here](#) to learn how to adjust IE security settings.
- Keep Critical Windows Updates current. This step can not be emphasized enough.

Just remember we've all heard the cliché, "There's no such thing as a free lunch." This is as true on the Internet as anywhere else. Whether it's through advertising, or through the use of your personal information, you're going to have to pay somehow.

Tips and Tricks

Windows XP - Check for Disk Errors

The ScanDisk utility is not available in Windows XP, however, you can use the Error-Checking tool in Windows XP to check the integrity of your hard disk. For steps, [click here](#).

Groupwise 6.02 Stoneville Server Users— Having Trouble Receiving Emails? Large fonts, lots of links, tables and heavy formatting are all characteristic of most spam. Spam filters often times incorrectly tag these messages as spam. If you know you are not receiving valid emails, have the sender send a new message in plain text formatting and it will breeze right past the spam filter. If you prefer to NOT have any spam blocked, send request to devans@msa-stoneville.ars.usda.gov

Microsoft Word – Saving a File for Use in Another Program Word allows you to save a document in a file format other than the Word document format. This could be useful to those who want to begin using Word now, but share

The Computer Support Newsletter

June 2004

<http://msa.ars.usda.gov/computerhelp>

email news: sntucker@msa-stoneville.ars.usda.gov

files with someone who is still using WordPerfect. For steps, [click here](#).

Agency News

Groupwise Announcement

Due to security reasons, password caching has been turned off in Groupwise. All non-netware users (users not using Novell netware) will be required to enter Groupwise password before accessing their email accounts daily and the remember password option has been disabled.

- ARS has set August 1, 2004 as the new implementation date for Microsoft Word and Adobe Acrobat as the Agency word processing standards. After this date, please insure that all email attachments sent within ARS are in Word format for editable documents and in Adobe Acrobat 6.0 for non editable documents.
- All MSA Secretaries, Office Automation Clerks, Administrative Assistants and Administrative Support personnel in the Mid South Area should plan to have a pc running Microsoft XP Professional Operating System by October 1, 2004. Employees who use LOTS, and NFC-PC-PRCH transmit/receipts should keep a WIN98SE PC available (secondary) for such applications.

- When purchasing a new PC, remember to order Microsoft XP Professional Operating System (not HOME version). Microsoft XP Professional Operating System is the Agency standard at present.
- For quotes on recommended systems, [click here](#).

Rumor Mill

Here's an update on some of the latest ARS initiatives:

- Web Migration – During the next few months the MSA Web site will be merged in to the main ARS website. All MSA webeditors have been assigned credentials to begin using ARS SitePublisher software. A training class will be held here at Stoneville for webeditors in the local area on June 9, 2004. An official website launch date has not been announced yet.
- Word / Adobe Training – Users have begun to receive notification of purchased training modules. The training is provided through the GoLearn system and is strictly for job enhancement. There is not a deadline to complete it, but access is valid for 1 year. **IT IS HIGHLY RECOMMENDED THAT THE TRAINING ROOM BE USED FOR ADOBE AND WORD TRAINING. A**

CALENDAR WILL BE POSTED ON THE TRAINING ROOM DOOR FOR AVAILABLE TRAINING TIMES. A FACILITATOR WILL BE AVAILABLE FOR EACH TRAINING SESSION.

- Informs Replacement – ARS has selected FormSofts Group's FormFinder for the Web as the replacement for Informs. FormFinder for the Web is a Web form and data repository solution that provides easy end-user access to forms and records and powerful centralized data storage, as well as basic routing of forms. The end-user will complete forms using Adobe Acrobat Reader software. Due to budget shortfalls this year, and pending waiver approval, ARS does not plan to pursue this project in FY 04, but will request funding for FY 05. In the meantime, you can download forms to fill out by hand from: <http://www.afm.ars.usda.gov/forms/new-formlst.htm> .
- MS Exchange migration – Still, there is no information on how or when this will take place. More info to come when provided from headquarters.

Comments and Contacts:

Comments: email your comments to: sntucker@msa-stoneville.ars.usda.gov