

Subject: DHR Best Practices - How to reduce Spam and Viruses

Spam

Most users have probably received an unsolicited (spam) email at one time or another trying to sell a product or service, soliciting personal information, or simply advertising other Web sites (most of which are offensive in nature). Some steps to help minimize the amount of spam you might receive are as follows:

1. **Do not reply to an unsolicited (spam) email - even to "unsubscribe"**. Any response you provide will typically be used to confirm your email address and send you more spam in the future. This would include being careful about the use of "auto reply" rules that you have configured in GroupWise.
2. **Be very careful about where you use your DHR email address on the Internet**. Most spammers search the Internet with software designed to pick up email addresses from unsecured Web sites, online mailing lists, discussion forums, and website registrations.

Viruses

Unlike spam, viruses and worms are typically designed to cause physical problems to your computer or data. Once again, there are a few helpful points users can follow to avoid suffering from computer viruses.

1. **Be VERY careful of any suspicious or unsolicited email you receive - especially those with files attached**. When in doubt, it is safer to delete a suspicious message than to open it and risk having computer problems.
2. **Pay close attention to strangely worded or garbled subject lines and messages - even if the sender is a person you know**. Viruses now have the ability to get names from address books and insert innocent user names in the "From" field when spreading themselves.
3. **Be VERY careful about unidentified messages instructing you to perform an action on your computer – such as loading a software patch or warning other users of a virus**. It is becoming more common that viruses hide themselves in email messages titled "security patch – install immediately" or "Virus alert – warn your friends". DHR's Office of Information Technology (OIT) or Communications Office will issue official computer security alerts and will include "DHR" somewhere in the subject line to help assure users the message is valid.
4. **Never access Internet-based email accounts (such as Hotmail, Yahoo, Netscape, or web-based email accounts from your home Internet provider) from a DHR computer**. This is one of the leading causes of virus infections since personal or free web email accounts do not get scanned by DHR's antivirus software.

If you are ever in doubt about a suspicious message or one that is requesting action but doesn't look like an "official" DHR communications, contact the Help Desk at 1-877-482-3233 for assistance. You can also view the following DHR OIT website for information on viruses and spam.

<http://gw.dhr.state.ga.us/news/virusnews.html#spam>