



## Alias/Vanity E-mail

When telephone lines were first introduced, many people were required to participate in a 'party line', which connected several individual telephones with a common line, and allowed all parties that shared that line to hear their neighbor's conversations. The evolution of telephone privacy has resulted in technologies such as caller I.D., unlisted telephone numbers, and the 'Do Not Call' list for telemarketing. E-mail privacy is still evolving, but one way to keep your personal e-mail secure from SPAM or unwanted communications is to establish an alias, or vanity, e-mail. We'll use the term 'alias e-mail' in this article.

To better understand what an alias e-mail is, let's compare it to a point of reference most everyone is familiar with, an e-mail address. A 'regular' e-mail address looks like this: [janedoe@hotmail.com](mailto:janedoe@hotmail.com). E-mail messages sent to [janedoe@hotmail.com](mailto:janedoe@hotmail.com) will arrive in Jane's personal e-mail account; the sender of a message knows that they are communicating directly with Jane.

An alias e-mail address, on the other hand, uses a generic name to define a person within another network. For example, if Jane Doe serves as the secretary at her church, and needs to be reached by e-mail, but does not wish to share her personal e-mail address, she could use an alias e-mail address, such as [churchsecretary@zionlutheran.com](mailto:churchsecretary@zionlutheran.com). E-mail messages sent to Jane's vanity e-mail ([churchsecretary@zionlutheran.com](mailto:churchsecretary@zionlutheran.com)) will be forwarded to Jane at her personal e-mail account ([janedoe@hotmail.com](mailto:janedoe@hotmail.com)). Therefore, in its simplest form, an alias e-mail address is a forwarding e-mail address.

Alias e-mail addresses are useful when a personal address is difficult to remember (such as [janedoe154835@yahoo.com](mailto:janedoe154835@yahoo.com)), when privacy is important, and when personal addresses

change often. These last two reasons are most pertinent to LWML and to your districts.

There is a balance between the need for interested parties to have access to district personnel and the need for identity protection. By using an alias e-mail address as a contact point, messages will still arrive in the appropriate person's e-mail inbox, but a personal e-mail address is not accessible to everyone who visits your district Web site.

Additionally, persons serving in LWML offices will not remain in that office indefinitely; that is, Jane Doe may be the District President right now, but someone else will be elected to take her place at the next District Convention. Therefore, using an alias e-mail address like [districtpresident@yahoo.com](mailto:districtpresident@yahoo.com) is much more practical than changing e-mail addresses every time a new person is elected to fill a position.

Acquiring an alias e-mail address is not difficult, but some options can be more costly. The best option is to go through your Internet Service Provider, who should be able to guide you through the appropriate steps for obtaining one on your current network. This option is oftentimes the most expensive.

Alternatively, many times the domain provider of your e-mail can establish an alias e-mail at less cost. Your domain provider is identified by the text following the '@' symbol in your current e-mail address. For example, if Jane's e-mail address is [JaneDoe@bresnan.net](mailto:JaneDoe@bresnan.net), then Bresnan is her domain provider.

In addition, webmail service providers, such as Google and Hotmail, have options for setting up alias e-mail addresses. Gmail, for example, provides a forwarding service that will allow you to establish a Gmail account ([districtpresident@gmail.com](mailto:districtpresident@gmail.com)),

### All About E-mail

The introduction of the World Wide Web, e-mail, and other Internet-based technologies has provided a convenient and economical way to communicate to a vast population. The benefits of these technologies are invaluable; unfortunately, while this technology has improved mass communication, it has also exposed individuals to inappropriate topical content, SPAM, identity theft, and threats to personal safety. It is foolish not to take advantage of the benefits, but it is also foolish to do so without taking precautions.

This edition of *Cyber Scoop* aims to help you identify ways that you can protect yourself and your fellow LWML sisters on the Internet and through e-mail. Much of the content is the result of inquiries from you!

and set it to forward to your actual e-mail account ([JaneDoe@bresnan.net](mailto:JaneDoe@bresnan.net)). With Gmail, the forwarding option can be found inside Settings, Forwarding, and POP/IMAP; once inside, we suggest selecting the option to forward incoming mail to your personal e-mail address and delete Gmail's copy. Hotmail also provides a forwarding service. Set up your Hotmail account, then select Options and Forward Mail to Another E-mail Account; Hotmail will automatically delete their copy of the e-mail. Hotmail requires you to sign into your e-mail account once every 120 days to keep the hotmail account active.

As committee members, you may wish to consider utilizing an alias e-mail as your primary contact, rather than your personal e-mail address.

*Information for this article obtained from <http://www.emailaddressmanager.com>, Wikipedia, WSTF member Wendy Greiner, Gmail and Hotmail.*

## Secure Passwords

In an attempt to limit the accessibility of particular Web sites or pages, webmasters often create a secure Web site that requires a user to register their personal information and select a password that will allow them entry to the site. The LWML Member Login is an example of a secured Web site that requires a password for entry. A problem arises when you have multiple secured sites that require passwords—it is very easy to forget your passwords! To help ourselves remember the password, we often choose words or dates that are easy to remember, such as a pet's name or a wedding anniversary, or we use the same password for every site. By doing so, we expose ourselves to hackers.

Here are some suggestions for choosing a secure password:

**1.** Never use personal information in your password, whether it be names or dates.

**2.** Don't use real words in your password. Hackers have technology that can run every word in the dictionary through your system to find the right one to access your account.

**3.** Use a variety of character types in your password, including upper- and lower-case letters, numbers, and symbols.

**4.** Use a *passphrase*, rather than a *password*. For example, you might choose "LWML conventions R the Gr8test!" as your passphrase.

In addition to following these suggestions, remember to use a different password for each secure site, and change your password every 30 to 60 days. If you have to write down your password so that you will remember it, keep your cheat sheet in a secure place, such as a locked drawer.

*Information for this article obtained from "Creating Secure Passwords, Tips For Creating Strong Passwords You Can Remember" By Tony Bradley, CISSP-ISSAP, About.com*

## Forwarding Your E-mail

Forwarding an e-mail is the process of sending an e-mail that you have received on to other e-mail addresses. Our e-mail inboxes are often filled with forwards containing jokes, sentiments, and news flashes. Forwards can be fun, but they can also expose you to viruses and junk mail. To avoid this exposure, follow these suggestions:

**1.** When you forward an e-mail, delete all of the other e-mail addresses that appear in the body of the message. These addresses are automatically included each time a message is sent on, so the more times the e-mail is forwarded, the more personal e-mails are added to the e-mail body. This process allows any recipient down the line to have access to your and all other recipients' e-mail addresses.

**2.** When you send an e-mail to more than one person, always use the 'BCC:' (blind carbon copy) field for listing all of the recipients' addresses. The 'BCC:' option will allow recipients to see only their own e-mail address in the forwarded message. If you don't see the 'BCC:' option when you forward an e-mail, click on 'TO:', and you should be able to highlight recipient addresses and choose 'BCC:'

*Note: Blind carbon copy is useful, but skillful spammers can still access e-mail addresses in the 'BCC:' field. When sending*

*e-mails to more than ten people, it is best to use a broadcast e-mail list (see the December 2007 issue of Cyber Scoop at <http://www.lwml.org/resources/webmasters/> for more information on broadcast e-mail lists).*

**3.** Remove 'FW:' in the subject line, or replace it with a new subject, if you wish.

**4.** When you receive a forward that requires you to open multiple messages before arriving at the actual forwarded message, always forward the message on from the last message box (the message containing the intended forward). This prevents other individuals' e-mail addresses from being sent on down the e-mail line.

**5.** Never put your e-mail address, home address, or name on an e-mail that asks you to participate in a petition. Petition e-mails with personally identifiable information are worth money to professional spammers. In fact, the best policy is to delete these messages, and stop them from circulating.

**6.** Delete e-mails that contain information that is not true. For example, if you receive an e-mail that warns about the dangers of eating bananas because they will make your ears turn yellow, go to [www.snopes.com](http://www.snopes.com), [www.truthorfiction.com](http://www.truthorfiction.com), or [www.factcheck.com](http://www.factcheck.com), to see if the claim is verifiable before you send it on to all your banana-eating friends.

## Securing Your Web Site

Certificate Authorities (CAs) issue and manage security credentials on a network to allow for information to be encrypted and deciphered. CAs are used to keep personally identifiable information secure. Any Web site that meets the following criteria should use a CA:

- you have an online store or accept online orders and credit cards
- you offer a login or sign in on your site
- you process sensitive data such as address, birth date, license, or ID numbers
- you need to comply with privacy and security requirements

An example of a CA is VeriSign®. VeriSign® issues Secure Socket Layer (SSL) Certificates, which encrypt sensitive data, authenticate information about the recipient of this sensitive data, and verify

the identity of recipients. In other words, an SSL Certificate ensures that personally identifiable information, such as a credit card number, is securely sent to the intended recipient for the intended purpose.

Shop LWML and the LWML Member Login utilize a VeriSign® SSL Certificate. If your district is considering adding a secure page to your Web site, be sure to purchase an SSL Certificate to protect those that will be accessing the page. SSL Certificates require a significant investment (VeriSign® certificates range from \$400 to \$1500 for one year, according to their Web site), but they provide invaluable security.

For more information on VeriSign® SSL Certificates, visit their Web site: [www.verisign.com](http://www.verisign.com)

*Information for this article obtained from Verisign.com and WhatIs.com*