Avoid receiving spam

Spam has increasingly become a problem on the Internet and on our Mail systems. While every Internet user receives some spam, email addresses posted to websites or in newsgroups and chat rooms attract the most spam.

Following the methods described below will help reduce the amount of spam you receive:

Don't reply to spam

If you reply to spam, the spammer or the automated program on the other end will then know that your address is connected to a live person, and the spammer will then bombard you with even more spam, and circulate your address to other spammers. It is critical that you pause and think before replying to any spam. Consider the following guidelines:

- Setting up your email account to generate automatic responses while you are away can have the unfortunate side-effect of verifying your email address to every spammer that sends you spam.
- If the message appears to come from a legitimate company, the company may have obtained your email address from some transaction between you and the company. In fact, you may have inadvertently provided your email address (e.g., if you didn't check a box marked don’t send me product updates). In these cases, it is usually safe to reply and ask to be removed from the mailing list.
- If it is not a company you recognize, use your judgment. To be safe, copy and paste the link to the company's site into the browser rather than clicking it in the email message.
- If you don't see a decent privacy policy listed on a company's site, we recommends that you do not reply or conduct any business with them.
- If the spam is clearly from a disreputable source, never respond. Do not follow the link (probably bogus) unsubscribe directions. In most cases, if you never reply, the network of spammers will eventually decide your email address is a dud, and will stop using it as often.

Be careful releasing your email address, and know how it will be used

Every time you communicate on the Internet or browse a website, there are opportunities for spammers to intercept your communications to obtain your email address and other personal information.

Otherwise reputable companies may sell or exchange your email address with other companies, and this information may eventually find its way to a spammer. At worst, spammers will use automated programs to bombard these lists of email addresses with spam. Consider the following guidelines:

- Subscribe only to essential discussion lists, and ensure that they are moderated.
- Think twice before offering your email address to a website. You may wish to check the site's privacy policy first to be sure it uses secure technology, and that the company does not share your email address with others.
- If you need to list email addresses on your website, present the addresses in a way that makes them less vulnerable to collection and abuse by spammers.
- Every time you are asked for your email address verbally or on paper, think carefully about whether or not you want to receive any information from that company or organization. It is usually best to decline to provide your email address.
- Whenever possible, advocate that organizations you are involved in or do business with default to the opt-in model. This requires you to specifically request to be added to their email lists, rather than the opt-out model, where they add you to email lists automatically, and then give you the option of asking to be removed.

Use a secondary email account

If you have your email address listed on a web page, you should also consider opening a free account. You should also consider opening a free account for performing potentially spam-inducing activities such as posting to Usenet newsgroups, bulletin boards, or unmoderated mailing lists, spending time in chat rooms, or using an online service that displays your address.

You should also consider using a disposable email address service such as spamex or mailshell. For a fee, these services allow you to create a new disposable email address discreetly linked to your real address whenever you need to supply one. If spam starts coming to one of the disposable addresses, you can simply turn the address off. Because you can give out a different disposable address on every occasion, you can easily determine who supplied your address to spammers.

Account recovery scams

Attackers are compromising mail accounts with just text messages, social engineering and look alike websites. Always contact your Districts Technology Department before inputting any account information on a web page. More often than not will they ask you to input any account and password information!

Donna ISD Technology Department

956-464-1660

Be proactive

Adjusting the security settings in your web browser is a good preventive measure. For a higher level of security, have your browser disallow:

- Accepting cookies
- Listing your name and other personal information in your browser profile
- Filling in form fields for you

This will help reduce the amount of personal information transmitted to sites at the expense of full functionality, since many legitimate websites require you to accept cookies.

Do not contribute to the spam problem by producing any of it yourself! In particular, learn about chain mail and do not forward chain mail to others. Also, if you receive an email message that appears to warn of some horrible thing happening (a virus that reportedly deletes all your files, for example) or is a touching sob story (about helping to save a poor sick girl or boy, for example), be suspicious.

Nearly every instance of chain mail is a hoax. The message may even come from someone you know and respect who is simply not aware that it's a hoax. Learn about hoaxes and the sites available to verify hoaxes, and do not forward them to others.