# SECURITY AWARENESS NEWSLETTER

DON'T CLICK THE "UNSUBSCRIBE" LINK AT THE BOTTOM OF UNSOLICITED EMAILS

Spam filters are catching most unwanted e-mail, but some might still reach you. Most spam is designed to get you to respond with your own email or to click a link to "unsubscribe." When you respond or click the "unsubscribe" link, the sender takes your email address and adds it to a SPAM database of active email addresses. You might then start to receive a large amount of SPAM in your inbox. Do not respond or click the "unsubscribe" links.

SAVE YOUR FILES TO A NETWORK SERVER

A computer user working on a critical project was saving the analysis document on his Windows desktop. Unfortunately, the Windows desktop was located on the local hard drive and local hard drives were not automatically being backed up. When his hard disk failed, he lost the file and had to work through nights and a weekend to make up for the lost time. If your company permits network backups or remote storage, be sure you back up your important files. PS. Important files don't include things like vacation pictures, which can overburden the backup system. Ask the help desk for advice on where such files should be saved.
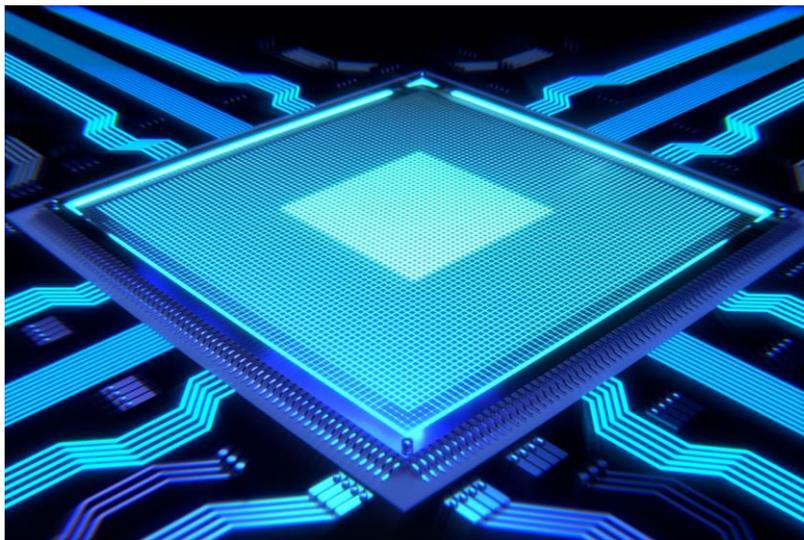
Three Tips for Safer Online Transactions

1. Make sure that the URL of the website begins with https (not http). Https ensures that your username, password, credit card number, expiration date and other information are sent from your computer to the site in encrypted form. Encryption helps to make your connection secure and reduces the risk that malicious people may intercept the information your enter and make illegal use of it.

2. A yellow icon that looks like a padlock at the lower right corner of your browser window confirms that you have a secure connection.

3. Some websites present a certificate of authenticity when you browse to them as a way to assure you that the site is legitimate. Check to make sure the certificate is valid and has not expired. If you are satisfied with the validity of the certificate, click on the link that takes you to the site itself. An invalid or expired certificate may indicate that the site neither authentic nor secure.

Letting Family or Friends Use Your Employer's Computers Can Be Bad for You

A candidate for Parliament in the UK received a lot of bad publicity when people took offense at a message her husband sent from her Council email account. She isn't the first person to get into trouble over a family member misusing their work email account or PC. Very few organizations let employees' families use their PCs. If you work from home on a corporate PC, then check your company policy and clarify boundaries with household members.
(http://news.bbc.co.uk/1/hi/uk_politics/6121646.stm?ls)

Review your credit reports routinely

The Fair Credit Reporting Act (FCRA) requires each of the nationwide consumer reporting companies — Equifax, Experian, and TransUnion— to provide you with a free copy of your credit report, at your request, once every 12 months.