The Department of Homeland Security (DHS) plays a vital role in countering threats to our cyber network. DHS has created the National Cybersecurity and Communications Integration Center (NCCIC) operating 24/7 for the purpose of securing federal civilian networks, cyberspace and critical infrastructure considered essential to our lives and work. This center maintains a common operating picture for cyber and other communications across the entire communication spectrum which includes: federal, state and local government; intelligence and law enforcement communities and the private sector.

Stop. Think. Connect.  
Clheck out the DHS partner link, [Stop.Think.Connect](https://www.dhs.gov/about-stopthinkconnect)/www.stopthinkconnect.org. to find many valuable resources to help you make informed decisions when using the Internet and to help protect you and your family to stay cyber safe. Some resources available in the Stop.Think,Connect toolkit include: mobile security tip card, social media guide, cybersecurity while traveling; chatting with kids about being online and more plus the toolkit is tailored for different audiences.

Next Steps  
The following preventative steps are intended to help our partners to read emails safely. Email headers can be fraudulent attempting to deceive users into "clicking the link" or opening attachments to seemingly real websites:

* **Email headers/email body**. Delete emails if the sender’s address looks suspicious or your email address is not displaying correctly. Are there warning signs in the email body such as incorrect spelling or typos?
* **Never click on links within an email or text**. If unsure whether the email is legitimate, from a third party retailer or primary retailer, go to their website and log on directly. Whatever notification or service offering was announced in the email, it should be listed and available on their website.
* **Be suspicious of all attachments**. Remember, sometimes people you know may have their computer infected with malware. Always scan with anti-malware software. Retailers typically **will not** send emails with attachments. When in doubt, call the retailer and ask if they sent an email with the attachment.
* **Do not give out personal information in an email or over the phone** **(Vishing)** unless completely sure. Social engineering is a process of deceiving individuals into providing personal information to seemingly trusted agents who turn out to be malicious actors. If contacted over the phone by someone claiming to be a retailer or collection agency, **do** **not** give out your personal information. Instead, request their name, the agency’s name and telephone number. Then you call them back. Remember, just because they may have some of your information does not mean they are legitimate!

Other practical tips:

* **Set secure passwords and do not share with anyone.** Avoid using common words, phrases, or personal information and change your passwords on a regular basis.
* **Keep your operating system, browser, anti-virus and other critical software up to date.** Security updates and patches are available and free from major companies.
* **Pay close attention to website URLs**. Pay attention to the Uniform Resource Locator (URL) from websites you visit. Malicious websites will use a variation in common spelling or a different domain (such as .com instead of .net) to deceive unsuspecting computer users.
* **For e-Mail,** turn off the option to automatically download attachments.

Learn More

* www.[OnGuardOnline.gov](http://onguardonline.gov/)
* [www.stcguide.com](http://www.stcguide.com)
* [www.merit.edu/cyberrange](http://www.merit.edu/cyberrange)
* [www.uscert.com](http://www.uscert.com)
* http://clareco.net/emergency\_services

Tips

-Most people use passwords based on personal information which are easy to remember. However, this makes it easier for an attacker to guess or "crack" a password.

-Although intentionally misspelling a word ("daytt" instead of "date") may offer some protection against dictionary attacks, an even better method is to rely on a series of words and use memory techniques, or mnemonics, to help you remember how to decode it.

-For example, instead of the password "hoops," use "IlTpbb" for "[I] [l]ike [T]o [p]lay [b]asket[b]all." Using both lowercase and capital letters adds another layer of obscurity.  
- Your best defense may be to use a combination of numbers, special characters, and both lowercase and capital letters. Change the same example we used above to "Il!2pBb." and see how much more complicated it has become just by adding numbers and special characters.

*Remember cyber security is a shared responsibility so everyone plays a role in keeping the internet safe.*

