3 Ways to Enhance Cyber Security

In order to help deter would-be thieves or hackers we need to take certain precautions. Let's face it. The end user is the weakest link in all security measures.

Use "strong" passwords	
Phrases are key	12 Characters or more Passwords are easy to hack. Pass-Phrases create the most strength
Mix up characters	Combine Uppercase – Lowercase – Numbers – Symbols ***Ex:*** S0met!mesUFeelLIke@Nut
Every 90 Days	Change the password every 90 days. Update your phone's email access each time.
After 3 attempts	Make the password lock out after 3 attempts (for 15 minutes).
Change it each time	Don't keep using the same password over and over. If you have to write it down, you can jot down the note that would trigger your phrase. Store the list separately.
Make it memorable	**The time to create memorable passwords is much less than the time spent attempting to recover lost data.** These tips can help you remember passwords – of course using a mix of characters as noted above: 1. Use lines from your favorite movies, TV, shows, songs, or jingles 2. Think of a phrase, then use the first letters of each word and the numbers in the phrase (Ex: MFhW16mFh!8 ---My first house was 16 miles from Hwy 18) 3. Choose a base phrase, and add part of that website name to it 4. Purposely misspell words – remember, no one will know! 5. Develop your own code (Ex: instead of the letter J, use 10 since it's the 10th letter in the alphabet) 6. Assign associations to people or objects instead of using names (**Ex:** Instead of typing Aaron Rodgers, we could type "BeSt25b@ck2Da!" 7. Think of vivid imagery that makes you smile, cringe, giggle, etc.
Keep it a secret	Never share your password with another user (Unless your manager requires it)

Be alert and aware	
Don't let your guard down Like at the airport – report suspicious activity	If it is computer related: • Don't click on anything. Just hold the power button on the computer until it shuts down. • Call IT immediately - notify your manager If it's not computer-related, report it to your manager immediately
Work and personal should not mix	Don't use your work computer for personal things. Keep that at home where it belongs. Don't store work information on your home computer.
Save to a network	Everything should be saved to a network drive for security and backup reasons. Don't store work information on your local system.
Be wary of flash drives	Don't bring in flash drives or other outside media without prior approval.
Your computer needs sleep too	At no time should a computer be logged in overnight. If you are going on vacation, it should be shutdown.
The daily restart	All computers should be restarted every morning, in order to get the latest network updates and security.

Email and internet surfing	
Know the Sender	If you don't recognize the email, delete it.
Question links and attachments	It's easy to spoof (duplicate) and email address so it looks like it's coming from someone you know. Don't click on links or attachments within emails without knowing 100% if it's a good link or attachment. If you were not expecting the email, give them a call to make sure they sent it.
Going to click on an ad? Hover over the link to confirm it will take you to a valid website.	Common websites (MSN – Yahoo – Star Tribune etc.) are not checking their paid advertisements, so they are often infected with malware. Often web links are bad and can be hijacked so they point to an infected site. Remember, once you click on a link or attachment, you automatically install whatever is there. You don't get to "undo" that click.