6 Steps for better cyber security:

By: State Farm Insurance (https://www.statefarm.com/simple-insights/smart-ideas/6-tips-for-cyber-safety?cmpid=enews-dec17)

More than 41 million people have been the victims of identity theft,[1] but there are steps you can take to be proactive in helping keep your information secure. Along with creating strong, varied passwords for every online account, consider these cyber security tips.

1. **Keep software up to date**
   Tech companies are constantly monitoring their software for weak spots or security breaches and often release updates to help fix those issues. Set up your devices for automatic updates.

2. **Install antivirus software and a firewall**
   Both are a great baseline in the battle against cybercrime; antivirus software detects malicious infections, while a firewall fends off outside access. Although a variety of free options exist, you may want to invest in a paid version that offers more updates.

3. **Check web addresses**
   Anytime you're providing financial information, such as credit card numbers, double-check the web address: It should begin with "https" and display a padlock sign, meaning you are securely transmitting information. And remember, if you're using a public network, your information is more vulnerable.

4. **Never click on suspicious links**
   Cyberthieves are masters at creating emails that imitate trusted vendors and sites. If an email is asking to verify personal information, demanding money or promising a refund, visit the website directly or call its customer service line to check its legitimacy. If you hover over a hyperlink in an email, a phishing scam will often reveal an unusual URL or one with a slight misspelling.

5. **Rely on two-factor authentication**
   Another powerful tool that adds an extra layer of security to log-ins and helps discourage cybercrime is two-factor authentication. It requires a username and password for the first factor and another piece of personal information, such as a security question or a onetime code sent to your phone, as the second factor.

6. **Don't send personally identifying information in email**
   Never email your credit card information, Social Security number, driver's license number or other financial or identifying information — especially if your email is unencrypted. Email is an easy way for hackers to snatch sensitive information.

[1]http://www.bankrate.com/finance/consumer-index/money-pulse-1016.aspx