Guidelines for Personal and Financial Security Online

DO NOT give out any personal or financial information over the Internet unless it is required by a transaction that you have initiated.

DO NOT broadcast details about your personal or financial life over the Internet unless needed for a transaction that you have initiated. This includes social security information, birthday, home address, names and birthdates of family members, as well as account and password information.

DO use secure websites, marked with an “https” at the front of the URL and with a gold lock on the site, for all business transactions.

DO create strong passwords. These should be 15 characters in length, if possible, and include an interweaving of letters, numbers, and symbols.

DO change your passwords frequently. The minimum recommendation is once every 6 months.

DO be conservative when using social media sites, and do not share information with strangers.

DO use control settings on social media sites to limit your engagement to those you know.

A hacker is one who attempts to gain access to computers illicitly. Protect against hacking by keeping your operating system and security systems up to date, and turning your computer off when not in use.

A phisher is one who attempts to get personal information by sending email or text messages that appear to be from legitimate individuals or institutions. Protect yourself against phishing by never responding to unsolicited emails and never opening attachments or links in these emails. Block the sender or mark it as SPAM. Report the sender to the email service provider if possible.

Identity theft consists of one person using another person’s personal identifying information without permission and in order to commit fraud or other crimes.

http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/

Protect against identity theft by following the recommendations given for protecting personal and financial information. In addition, make sure you change your passwords frequently. Finally, monitor all your accounts and report any unauthorized transactions or activity immediately.