WHO ARE YOU?

We love new "Smart" devices, the ease of connecting, and the rapidity that today's technology allows us to conduct our affairs. The problem is we sometimes relax our guard against hackers and more importantly run the risk of **identity theft**. For example, a lady received a phone call from someone claiming to be from Microsoft who told her there was a problem with her computer. As her computer technician was on vacation just then, and believing there was a real problem, she was kept on the phone for 15 minutes and was told that if she paid €300.00 her computer problem would be fixed. She refused to pay and hung up, only to find that when she returned to the PC all her personal documents (photos, text, etc.) had completely vanished. Many functions could not be performed because a password was now required. So while on the phone with the alleged Microsoft person, her hard drive had been accessed and people on the other end had deleted her files and imposed a password that could only be removed by paying the €300.00. The end result was her computer technician later on managed to eliminate the password and recovered the hard drive to recapture her personal files: a time-consuming and costly price – and her e-mail passwords and security information changed; to date her credit cards appear not to have been affected.

Obtaining anyone's phone number is easy for those who want it; the danger lurks in their ability to access our **personal information**. Identity theft has grown exponentially in tandem with more people using social media, Wi-Fi connections, multiple mailings, and free-flowing information. We already know about numerous hacking cases from large companies whose databases have been compromised with a growing trend in medical identity theft where your

name and health insurance info is used to get consumer loans, drugs, care and file claims. Accept that we are vulnerable and follow these suggestions religiously:

- Keep your antivirus program up to date; if you have a free security system, upgrade it to a paid version for complete protection and keep it updated
- Use your credit card sparingly and only at well known and trusting vendors
- Monitor your bank accounts and credit cards **WEEKLY** for suspicious activities
- Mind how and where you connect wirelessly to the internet (public places like airports, cafés, bars, restaurants)
- Manage your email accounts by changing your passwords often and not opening mail from unknown sources – even from friends
- Maintain privacy in what you publish on social media sites –not everyone needs to know everything about you!
- Make these activities **HABITS**, not incidental actions.

YOU are the only person entitled to your identity. Keep it safe by using the internet smartly.