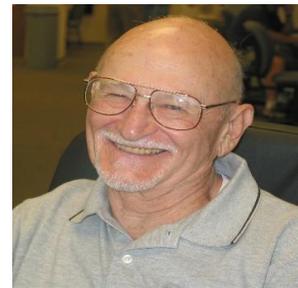


NOBODY ASKED ME BUT.....

By Matt Schwartz



The season of Ho, Ho, Ho and “Dreidle, Dreidle, Dreidle” is over. Visions of sugar plums and latkes are now replaced by credit card payments, checking bank balances and the dreaded I.R.S. Which means that the identity theft brigands are lying in wait to pounce on us to rob social security numbers, bank account numbers, credit card numbers, etc., etc. to hit and run thereby reaping a financial harvest at our expense. Identity theft is rampant and it is foolish and costly not to defend ourselves against it. What to do:

1. Check every email you receive from your financial institutions for authenticity. Phishing (fishing) uses phony emails to get as much personal information from you as possible, including those above. Some of these emails are almost exact duplicates of the legitimate ones.

2. When you receive an email from one of your financial institutions asking for personal information from you (usually “requesting verification”) DON’T GIVE IT. Contact the institution and question the legitimacy of the request.

3. Before you enter your computer name and password to log on be sure that the little padlock icon in the bottom right of your screen is CLOSED.

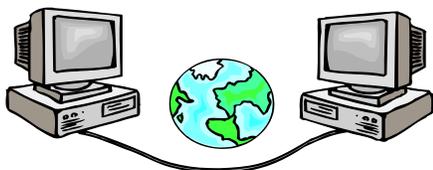
4. When you are finished with a transaction LOG OFF and CLOSE YOUR BROWSER. No one else can then get at your account.

5. Pick a password that has at least 7 characters and numbers. Why make it easy for the thieves?

6. Check your accounts REGULARLY. Call IMMEDIATELY on any discrepancies or strange activity.

7. I know you’ve heard this before but it’s your money and your security at stake. INSTALL AND KEEP UP TO DATE A GOOD ANTI-VIRUS PROGRAM. INSTALL A GOOD FIREWALL. INSTALL A GOOD SPYWARE PROGRAM. There are good ones out there that are both FREE and SIMPLE TO INSTALL.

Insurance is expensive and you probably have lots of coverage. All the foregoing costs you is a modicum of time. Become a victim and you have no one to blame but



Matt (mattinlw99@yahoo.com)