Online Security Tips

Identity theft and online security are quickly emerging as modern day challenges for consumers, and also for businesses and governments around the globe. The topic is wide and complex. From the theft of Social Security and credit card numbers to the unauthorized accessing of the massive computer networks in an unregulated cyberspace, a final and comprehensive solution may never materialize. So, instead, the roadblocks are removed as they are encountered.

Consumers are utilizing the Internet at an increasing rate for all types of transactions, from on-line banking to making travel reservations to obtaining a home loan and beyond. OLP is preparing to make its revised online loan application available directly to UC loan applicants in the near future. As a result, the privacy of the online applicants and protecting their sensitive data is a top priority for the OLP team.

The following summary is a suggested list of measures by the security professionals in the field to battle the aforementioned roadblocks and more. The items listed are separate yet intertwined in nature and scope, and, if followed, may further help to protect the security and confidentiality of data stored on your computer or exchanged with others via electronic means.

CYBERSPACE SECURITY TIPS

1. Use protective "anti-virus Software" and keep it up to date.
2. Use protective "firewalls" to prevent intruders from taking control of your computer and stealing your valuable data.
3. Regularly update your browser by downloading the latest security updates, i.e. "patches".
4. If possible, avoid opening e-mail or visiting the web under your Administrator account - opt to create a user account with limited rights to engage in those activities.
5. Disconnect from the Internet when not in use any more.
6. Don't open e-mail or attachments from unknown sources. Learn about file sharing and don't engage in it if you don’t know how to protect yourself.
7. Use a mixture of numbers, upper and lower case letters, and characters (if allowed) in creating your passwords.
8. Regularly back up your computer data and your personal files.
9. When changing your clock for daylight savings time, re-evaluate your computer security measures.
10. Immediately inform those with infected computers of their vulnerabilities.

PERSONAL PRIVACY AND ID PROTECTION TIPS

1. Use care in sharing your personal information, such as your address, telephone number, social security number, bank account and credit card information, and PIN numbers. Know with whom you are sharing this information in advance.
2. Always shred unused convenience checks or papers with personal information before you throw them away.
3. Check your credit reports periodically. Check your bills as well for irregularities.
4. Decline to be on the marketing list of creditors or other marketing outlets.
5. Report any fraudulent activity to creditors, the credit bureaus and the police.
6. Change the password on your accounts from your social security number to a personal ID of your own choosing.

7. Notify the Postal Inspector if you don't receive your regular mail and suspect an unauthorized change of address.
8. Protect your Driver's license or DMV-issued IDs. Report to DMV immediately if stolen or lost.
9. Don't fall victim to your own lack of interest in managing and protecting your personal privacy. Keep current with the related events and remedies.
10. Remember, nothing is worth compromising your peace of mind. Be alert!