TIP SHEET SERIES **NO. 3**

Basic Recommendations for Online Security

- **Keep Your Security Software Current.**

  The best defense against viruses or other malware is to have the latest security software, internet browsers and operating systems.

- **Automate Software Updates.**

  Many software programs automatically create defenses against unknown risks. If you have such an option, activate the automatic update option.

- **Protect All Your Connected Devices.**

  In addition to viruses and malwares, your computers, smartphones, gaming systems and other connected devices also need protection.

- **Plug and Scan.**

  USBs and other external devices may be infected by viruses or other malwares. Scan these devices through security software.

- **Be Sure that your Accounts are Secure.**

  Passwords are not enough to protect the accounts. Because of this, many email providers allow you additional ways to verify your identity.

- **Your passwords must be long and strong.**

  Create a strong password with numbers and symbols by collating uppercase and lowercase letters.

- **Create Separate Passwords for Each Account.**

  Creating separate passwords for each account keeps cyber criminals away from you.

- **Keep Passwords safe.**

  Everyone can forget your password. However, this problem can be solved with a list of passwords stored in a secure place away from your computer.

- **Check your online presence.**

  While online, check your customization and security settings to set your level of information sharing.

- **Delete if you have doubt.**

  Cybercriminals often steals personal information through links in e-mail, social media messages or online advertisements. Even if the source is known, when something seems suspicious, it should be removed immediately.

- **Be Careful About WIFIs**

  Any attacker can see what you can do while connected to a common network. In such environments, check the security settings of your machine and limit the types of jobs that

contain sensitive information such as credit card, password, customer data.

- **Connect with Care.**

  Make sure your site is safe while using Internet Banking and shopping online. Use websites that start with "https: //,". These sites take additional measures to protect your information. Sites starting with "http: //" are not secure.

- **Know the Internet well.**

  Keep up to date with new ways to stay safe online. Get information about this topic from trusted sources and share them with your family, colleagues and friends, making them well-informed individuals.

- **Think Before The Move.**

  Avoid people who are urging you to rush and who ask for your personal information. If you get good offers that can not be real, think again and be careful.

- **Back up Data.**

  An electronic copy of valuable work, music, photos and other digital information must be regularly created and safeguarded and protected.

- **You Are Safe, Everyone Is Safe.**

  Actions you do online have the potential to affect others. The good online habits benefit to the global digital world.

- **Help Authorities.**

  Inform the authorities about suspected cases of cybercrime