Top 10 Online Safety Precautions
(from Brendan McHugh with the District Attorney's CATCH Team)

1. Use unique, complex passwords for every online account and computing device. A complex password consists of 8 or more characters which includes capital letters, lower case letters, numbers and special characters.
2. Keep operating systems, applications and anti-virus programs up to date. Virtually all programs and applications have some vulnerability that the publishers find and fix, if you don't keep them up to date, you are exposing your devices to known vulnerabilities.
3. Setup local administrator accounts on your computing devices to ensure that only an administrator can download programs and applications. In most operating systems, one can setup a user account, for instance in Windows that can be done through the Control Panel. By setting an administrator account with a unique, complex password, and user accounts that do not have administrator privileges, you can control what is downloaded onto your computer.
4. Only download programs from trusted sources. Freeware and Shareware is notoriously ridden with viruses. If you have any question about the legitimacy of a site, don't download programs from that site.
5. Understand the privacy settings and access settings on mobile applications. Be cautious about downloading applications for mobile computing devices and be aware of what data they access on your device as a condition of your using the application. Look at the comments other users post about these applications before loading them to your device.
6. Secure your home wireless network. The minimum level of encryption is WPA2 and if your wireless router is not capable of running WPA2, replace it. The router should be password protected with a unique, complex password and WPA2 encryption should be turned on.
7. Limit the personal identifying information you post on social media sites and limit the number of people who can see it. There are privacy settings in virtually every social network site, use them to limit the number of people who can see your profile. Despite your best efforts to limit the number of people who can see your profile, understand that there will be some unintentional leak, so don't post personal identifying information that you are not comfortable with the world knowing.
8. Beware of phishing websites, text and phone calls. If you receive a telephone call, email or text message from a financial institution asking you to provide them information so they can change your password, you are communicating with a criminal. Don't respond to these messages by clicking embedded links or calling numbers they provide. Contact your financial institution directly at the number on the back of your card or account statement, or the login you routinely use.
9. Only conduct financial business and transactions online through websites that are encrypted. When you login to a website to conduct financial transactions, look to ensure that the website is https or shttp encrypted. An unencrypted website will appear as http, and should not be entrusted with sensitive financial information or payment card numbers.
10. Check credit reports and account statements regularly. Consumers are entitled to one free credit report a year, request yours and ensure that there is no irregularity that needs to be addressed. Similarly, check account statements on a regular basis and report any irregularity or transactions you did not approve.

Websites for further information include: Catchteam.org, FTC.gov, Onguardonline.gov, IC3.gov, Getnetwise.org, Idtheftcenter.org, Securingourecity.org