TAKE A BITE OUT OF CYBER CRIME

www.bytecrime.org

CYBER SAFETY CHECKLIST

For the Home User

□ **Install anti-virus software:** Digital bugs are still the most common and damaging threat to most computers, and they require a solid defense.

□ **Get a spam blocker:** Spam doesn't just mean annoying ads anymore—it introduces all kinds of new threats, such as phishing scams.

□ **Guard against spyware:** Obtain reliable anti-spyware software. Crooks want to know what you're doing online and they'll use that information in harmful ways.

□ **Build a firewall:** Don't worry, it isn't hard to do. A firewall is just a digital barrier that keeps hackers out. They exist on most operating systems, so make sure yours is turned on. If you don't have a firewall, you can download one.

□ **Create penetration alerts:** Set all of the above defense software to notify you when suspicious activity is occurring.

□ **Setup effective encryption keys on your wireless home networks:** Always use long, automatically-created network encryption keys and rotate them regularly. You can also find wireless protection software that can walk you through this process.

□ **Install security patches:** New vulnerabilities are regularly exploited in many software platforms. You should check for and install updates on all software you use.

□ **Backup important files:** No amount of protection is a guarantee, so take preventative steps to save your data before it can be damaged.

□ **Always watch for Internet scams:** Online criminals always think of clever new ways to rob you. Don't get lured in by emails telling sad stories, making unsolicited job offers or promising free money.

□ **Take care when shopping online:** Look for indicators that the site is secure, like a small lock icon on your browser's status bar, a trusted seal like those from VeriSign or TRUSTe and a website URL that begins "https" (that "s" stands for "secure").

□ **Don't open unknown email:** If you have no idea where an email comes from, take the safe course and delete it before opening it.

□ **Treat IM seriously:** Attacks can come through instant messaging programs as easily as they can through other channels.

□ **Treat it just as you would email and stay on guard from nasty files.**

□ **Beware of file sharing:** Make sure you scan shared files for viruses. Also, set up the file sharing software carefully and take the time to read the software's User Agreement to be clear about any side effects that may be built in.

□ **Create smart passwords:** Your online and computer passwords should be at least 8 characters long and incorporate letters, numbers and symbols. Use different passwords for different accounts, change them every 90 days and never share them with anyone.

NATIONAL CRIME PREVENTION COUNCIL CMO COUNCIL FAME Forum to Advance the Mobile Experience comcast intel McAfee VeriSign Walmart.com