CYBER SAFETY CHECKLIST

TAKE A BITE OUT OF CYBER CRIME

www.bytecrime.org

For Business User

- [ ] **Install anti-virus & spyware software:** Digital bugs and spies are the most common and damaging threat to business computers, and they require solid defenses. Set the software to update virus/spyware definitions regularly and automatically.

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

- [ ] **Build a firewall:** The digital barrier keeps hackers out and luckily it exists on most operating systems. Make sure yours is turned on. If you don't have a firewall, you can download one.

- [ ] **Tight E-Commerce:** If your company provides online buying, be 100% sure there aren't flaws on your website that hackers can exploit to steal your customers' data. An Internet infrastructure services company like VeriSign can help with this.

- [ ] **Setup effective encryption network access keys:** Always use long, automatically-created network encryption keys and rotate them regularly.

- [ ] **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.

- [ ] **Safeguard your brands and logos:** Stay vigilant to make certain that your company's trademarks or image are not being used in a "Phishing" or "Pharming" scam, where others hijack your customer's trust and manipulate it for their gain.

- [ ] **Act quickly if infected:** Even if you only suspect your computer has been infected with malicious code, contact your IT personnel immediately – if that's one of the hats you wear, then unplug your computer from the Internet and run a virus scan right away.

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

- [ ] **Take care when purchasing 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, the safest course is to delete it before opening.

- [ ] **Treat IM seriously:** If your business uses instant messaging treat it just as you would email and stay on guard from dangerous software.

- [ ] **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.

- [ ] **Teach your employees & colleagues:** Form an army against computer criminals by passing on this tip sheet... and Take a Byte Out of Cyber Crime.