



Minnesota Crime Prevention Association's Crime Prevention Tips

The MCPA strives to bring current information regarding prevention topics to its members. Please use these prevention tips to promote safety to the citizens of your community. These tips are great for brochures, newsletters, e-mails, etc.

Topic: **Cyberspace – The Electronic Workplace**

Enterprising criminals can gather enough information about a business through everyday PC compliance, electronic transactions, dumpster diving debris and/ or pretend to be an: employee, vendor of the company and/ or agency, etc. Once this happens a business can be accessed in the world of electronic cyberspace.

It is suggested that a business draft or have in place the following policies as it relates to the responsible use of business property and proprietary information.

- ✓ Computers, Hand device (Blackberry/ Palm pilots/ Cell Phones), electronic resources are the property of the business and are to be used solely for business practices.
 - Employees should treat the Internet, e-mail, and voicemail systems as other written business communications with care, professionalism, confidentiality and a company representative.
 - Ensure that the use of Internet connections and portals are respected with regards to copyright issues: software, information and noted authors.
- ✓ Fraudulent, harassing, threatening, discriminatory, sexually explicit or inappropriate message should not be transmitted, printed, requested or saved.
 - Personal information should not be sent over the Internet, through e-mail, or over cellular phones as it is company property.
 - Use and access may be monitored, accessed, and tracked by the business at any time with or without notice. Items, which appear to be deleted, can be recovered from IT/ IS settings.
- ✓ Passwords that are obvious should not be used — names (friends, relatives, or pets), birth date, even street addresses. The best passwords mix numbers with upper and lowercase letters and include numbers or symbols. A password that is not found in the dictionary is even better because there are programs that will try every word in an effort to crack a code.
 - Avoid break-ins by changing your password regularly and memorizing it. If you have several set up for a system do not write the passwords down especially in a common area to ensure that compromising does not take place.
- ✓ In order to maintain and assure business access to data, no employee should be permitted to use devices, which may encrypt company data without written authorization or documented approval.
 - Ensure that employees are using the business provided anti-virus software.
 - Ensure that any server room/ computer lab has the appropriate security devices: CCTV, alarms, pass card access as defined by the business and/ or SOX compliance.

- ✓ Destroy any printed confidential information. Tear, shred and/ or utilize a document destruction company, which will shred on-site and ensure that the destruction of the document(s) are confined.