



Having a safe community goes beyond safe streets – When you are protected online, you can enjoy the benefits of the digital society.

Keep Your Computer Safe

- Keep your security software updated. At a minimum, your computer should have anti-virus and anti-spyware software
- Never install software from an untrusted source. Be cautious about opening attachments and downloading files from emails, regardless of who sent them. These files can contain viruses or other malware that can weaken your computer's security. These programs can cause your device to crash and can be used to monitor and control your online activity. Criminals use malware to steal personal information, send spam, and commit fraud.
- Back up your files: Copy important files onto a removable storage (CDs/DVDs or flash drives/USB stick) or an external hard drive, and store it in a safe place so you have a backup copy if needed.

Protect Your Personal Information

- Use long and strong passwords - The longer the password, the tougher it is to crack. Combine capital and lowercase letters with numbers and symbols to create a more secure password.
- Don't share your account passwords and don't use same passwords for different online accounts
- It's ok to write down your passwords - Just make sure you put your written reminder in a safe place and away from your computer.

Beware of Scams

- Scammers use email, online ads, popups, and search results to trick you into sending them money and personal information. This is called "Phishing" and criminals use the information to commit identity theft.
- Scammers impersonate legitimate businesses, and even friends and family to trick you. If you weren't expecting it, check it out before responding. Legitimate businesses don't ask you to send sensitive information through insecure channels.
- If an offer looks too good to be true, it probably is.

Continued...

Connect with Care

- Look for web addresses with “https://”. The “s” stands for secure which means the site takes extra measures to keep your information secure.
- Secure home wireless network with a password and encryption
- Use your browser’s privacy and security settings, such as pop-up blockers
- Watch your links:
 - If you have a question about a link on a website, put your mouse over the link without clicking. Your browser should show you the actual address of the web page where the link will take you. If everything looks ok, you can then click on the link.
 - Is it the official site? Example:
 - service@paypal.com = good
 - service@paypal.com.clickz.com = bad

Talk with your Kids

- These safety and security tips apply to computer and Internet users of all ages. Make sure your kids know not to share passwords and personal information and to beware of scams or malware advertised as “free” stuff.
- Look for teachable moments — if you hear about a scam or get a phishing message, use it as an example with your kids.

Help Your Community

- Share cyber safety tips with your friends, family and neighbors
- Report cybercrime: Complaints are an essential resource for local, state, and federal law enforcement officials. Law enforcers review consumer complaints to spot trends and build cases against hackers, identity thieves, scam artists, and other fraudsters
- File cybercrime reports with the Minneapolis Police Department so that cases in Minneapolis can be addressed and documented. Reports can also be submitted to www.ic3.gov (Internet Crime Complaint Center) and the Federal Trade Commission www.ftccomplaintassistant.gov

More: Explore resources at www.onguardonline.gov and www.stopthinkconnect.org for additional tips on Internet safety tips and protecting yourself online.

