Student Tips to Prevent ID Theft

Being online and sharing information has become a part of our everyday lives. Technology is changing the way we interact, and while it makes communication more efficient, it also increases the risk of identity theft. Here are some tips to minimize the threats of identity theft while online.

Don't reply to text, email, or pop-up messages that ask for personal or financial information.

1. **Be careful with the information you share on social networks.** Whether you use Instagram, Snapchat, X "Twitter" or Facebook be cautious of the information you share. Limit the personal information you post such as your full name, age, photos, home and email address, phone number, or school name. Once you post, you can't take it back. Assume that everything you put on a social networking site is permanent. Consider what a post reveals, who might see it and how it could be perceived now and in the future. Choose your social networking site carefully and understand the privacy policy. Most social networking sites have privacy settings. Find out how to turn these settings on and use them.
2. **Think before you click.** Don't click on links from unknown senders. If you receive unexpected or questionable messages, even from friends, don't open any attachments, including photos, songs or videos. Check with the sender to ensure the message comes from a trusted source. Use caution when downloading software, games, music or any other content as destructive viruses can be hidden in websites, downloaded apps or email attachments. If something looks suspicious, it is best to delete it.
3. **Use secure file sharing networks.** Peer-to-peer file sharing allows you to easily share music and games with friends, but these informal networks are prone to malware. Safeguard your personal information by checking the default security setting when you install the file sharing software to ensure that nothing private is shared. Run security scans on all shared files. Talk to your parents about the security risks involved with file sharing.

4. **Beware of imposters.** Hackers can break into accounts to access personal information and send messages that look like they are from your friends, a business or your school, but they are not! If you suspect that a message is fraudulent, use an alternate method to contact your friend to find out if they actually sent it. Ask yourself: do you know and trust who you are dealing with? Limit your online friends to people you actually know so you don't share information that could be used against you with strangers.
5. **Don't get hooked by phishing scams.** Be cautious of scam artists throwing deceptive bait to see if you will bite and give up your personal information. Don't reply to text, email, or pop-up messages that ask for personal or financial information, and don't follow any links in the message. Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them. Unexpected files may contain malware.
6. **Be smart about smartphones.** Lock your phone with a passcode and don't share it with anyone. Most smartphones have GPS technology that

allows you to find out where your friends are and allows them to find you. Adjust your location settings so that only people you know can see your location, and turn them off when not in use. Don't respond to text messages from unknown senders requesting personal information. Contact your mobile service provider about blocking unwanted text messages. If you like to download apps, you may be sharing a lot of personal information about yourself with the app developer. Check your privacy settings before downloading a new app, and check the information the app collects.

7. **Use secure Wi-Fi networks.** When using an at home network, run security software, keep your browser and operating systems up to date and pay attention to security warnings. When surfing the web on your smartphone, using your own 4G or 5G network is the most secure option. If you will be on a public Wi-Fi network, it is best to use a password secured network. If you plan to use an unsecured public network, refrain from accessing any personal information while online. Stick to encrypted websites - look for websites that begin with "https" (the "s" stands for secure).

8. **Create strong passwords.** Passwords are the first line of defense in protecting yourself from cyber criminals. Choose strong passwords for all of your accounts. A mix of upper case and lower case letters, numbers and symbols is the best combination. Make sure to change your passwords regularly and never share them with anyone. Use two-step authentication if offered and always log out of your accounts before you shut down your computer.

9. **Place a security freeze on your credit report.** Parents and legal guardians can place a security freeze on the credit report of a child or other protected individual. A security freeze will prohibit the release of any information on the credit report without express authorization. A security freeze is designed to prevent an extension of credit from being approved without consent, which makes it more difficult for identity thieves to open new accounts in your name.

10. **Ask someone.** Before you give out personal information, click on a link or visit a new website, consult with someone you know and trust. Discuss the sites you visit with your parents and review privacy policies together.

For more information or to file a complaint, visit our website or contact:

Wisconsin Department of Agriculture,
Trade and Consumer Protection
Bureau of Consumer Protection
2811 Agriculture Drive, PO Box 8911
Madison, WI 53718-8911

Email: DATCPHotline@wi.gov
Website: datcp.wi.gov
PHONE: (800) 422-7128 TTY: (608) 224-5058

StudentTipsPreventIDTheft668 (rev 10/23)