Protecting Your Identity

It's important to protect your identity and personal information because you don't want it getting in the wrong hands. Unfortunately, some individuals will use your information to falsely open up accounts in your name and ruin your credit. Sometimes, companies collect information that they really don't need to have. If there is ever a data breach, meaning a computer hacker has gained access to a company's computer system without their permission, your personal information becomes available. Thieves or online hackers can combine various pieces of information they have found and create a "profile." Once a profile is complete, they sell your information to individuals who try to impersonate you. This leads to identity theft, which is a growing problem and concern for everyone.

When you visit a website, are you ever asked to click and acknowledge that you are aware of the company's privacy policy? If so, have you ever read a company's privacy policy? Below is an excerpt from an actual company's privacy statement. It's somewhat disturbing the information they collect from you when you visit their website:

1. **Website Visits & Registration**

   We collect the following personal data when you visit the website or register to take surveys, whether you are a registered user of the website or not:

   - name
   - log in
   - password
   - IP address
   - website's usage (i.e. how you interact with our website)
   - information on your device (e.g. screen size)
   - (social) network user ID, if you use social network plug-ins (e.g. "Like" button)
   - location
   - public content you may have posted on, or through the website

It seems to be much harder to protect your information online since there are so many websites we visit each and every day. Here is a partial list of suggestions from experts. They recommend:

Source: Federal Trade Commission, Illinois Office of the Attorney General, and Practical Money Skills

- ✓ Don't carry your social security card in your wallet
- ✓ Don't share your personal information on an incoming call – even if the person says they are with your bank or a government agency.
- ✓ Safely dispose of computers, mobile phones, and other electronic devices that may have your personal information on them.
- ✓ Shred receipts, credit offers, credit applications, insurance forms, physician statements, checks, bank statements, expired charge cards, or documents you don't need any longer that has personal information on it, including old bank statements, credit cards, and insurance forms.
- ✓ Install antivirus software on your computer and keep it up-to-date.
- ✓ Avoid logging into financial accounts while using public wireless internet networks – especially at cafes or airports
- ✓ Set up passwords and regularly change them for your phone and computer
- ✓ Use different passwords for your online accounts
- ✓ Before sharing information at a business, workplace, school or doctor's office, ask why they need it, how they will safeguard it, and the consequences of not sharing it
- ✓ Consider signing up for the national or state "Do not Call Registry" so marketing companies are not able to contact you.

Source: Federal Trade Commission, Illinois Office of the Attorney General, and Practical Money Skills