Identity Theft Prevention:
There is Only One of You in the World!

Thieves will try to steal your identity through the massive retail security breaches occurring across the globe daily. Although the holiday shopping season is prime season for cyber thieves, be cautious at all times. Below are tips from the US Computer Emergency Readiness team, a division of the Department of Homeland Security.

Preventing and Responding to Identity Theft

Even those who never use a computer can be ID theft victims. Personal information (including credit card, phone and account numbers) can be accessed by database hacking, wallet theft, eavesdropping on phone calls and dumpster diving. A thief picking up a restaurant receipt can find an account number. Thieves can use stolen information to purchase items, open new accounts, or apply for loans.

Most companies and other institutions store client information in databases which can enable a hacking thief to access information about many people at once. The internet has also made it easier for thieves to sell or trade information, making it difficult for law enforcement to identify and apprehend the criminals.

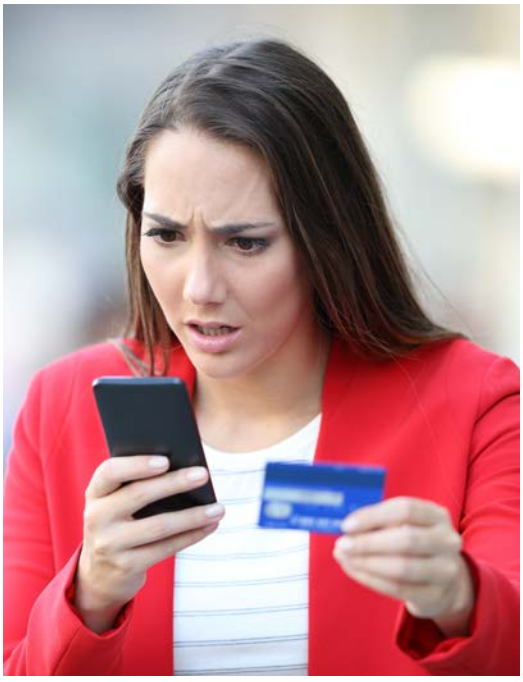
Identity theft is usually a crime of opportunity, so you may be victimized simply because your information is available. There is little you can do to guarantee that you won't ever be a victim of identity theft. However, use the following practices to keep your info as safe as possible:

- Before providing personal or financial information, make sure that you are interacting with a reputable, established company. Attackers often create malicious web sites that appear to be legit. Verify the legitimacy before supplying any information.
- Passwords and other security features add layers of protection if used appropriately. Choose passwords carefully to ensure they are difficult to crack.
- Take precautions when providing information, and make sure to check published privacy policies to see how a social website or company will use or distribute your information.
- Avoid posting personal data in public forums, particularly on social media sites.
- Use anti-virus software and a firewall to protect against viruses and Trojan horses that can steal or modify the data on your computer.
- Check account activity including statements and credit reports yearly.

Signs Your Identity Has Been Stolen

Companies have different policies for notifying customers after discovering a customer database breach. However, be aware of changes in your normal account activity. Here are examples that could indicate someone has accessed your information:

- unusual or unexplainable charges on your bills
- phone calls or bills for unknown accounts, products, or services
- failure to receive regular bills or mail
- new, strange accounts appearing on your credit report
- unexpected denial of your credit card



Steps to Take If You Think Your Identity Has Been Stolen

Recovering from identity theft can be a long, stressful, and potentially costly process. Many credit card companies have adopted policies to minimize the amount of money you are liable for. Yet, the implications can extend beyond your existing accounts and wreak havoc on your financial reputation for years. To minimize damage, take action as soon as possible:

- Inform the companies where you hold accounts to learn of any unauthorized transactions. Close accounts so that future charges are denied. Call the company and send a letter so there is a record of the problem.
- Contact the three credit reporting companies and check your credit report for any unexpected or unauthorized activities. Have a fraud alert placed on each credit report to prevent new accounts being opened without verification.
- File a report with the local police so there is an official record of the incident. You can also file a complaint with the Federal Trade Commission.
- Depending what information was stolen, you may need to contact other agencies; for example, if a thief has access to your Social Security number, contact the Social Security Administration. You should also contact the Department of Motor Vehicles if your driver's license or car registration have been stolen

The following sites offer additional information and guidance for recovering from identity theft:

Federal Trade Commission – http://www.ftc.gov/bcp/edu/microsites/idtheft/

United States Department of Justice – http://www.usdoj.gov/criminal/fraud/websites/idtheft.html

Social Security Administration – http://www.ssa.gov/pubs/idtheft.html