Tips to Avoid Getting Scammed

1. Do not send money using a wire transfer, prepaid debit card, or a gift card. Do not send money to someone you have not met.

2. Be distrustful of links or attachments in unsolicited emails. Emails may look legitimate but may be fake. Scammers are good at making websites and emails look official.

3. Don't be pressured to make a decision or take action. Scammers try to pressure you and make you think that an action must be taken immediately.

4. Do not use a wire transfer, prepaid money card, gift card or any method to pay for goods, services, taxes or debts. These can't be traced and are like paying with cash.

5. Use secure websites. Make sure the website has "https" in the URL. The "s" stands for secure. Pay for purchases online using a credit card but check out the company to make sure it is a reputable business.

6. Be careful when using dating websites. Scammers reach potential targets using a variety of online sites. You may feel the individual you are communicating with is a friend or romantic partner. Unfortunately, this is not always the case.

7. Guard your personal information, such as Social Security Number, birthdate, and credit card information. Never give this information to anyone who contacts you unsolicited. Scammers attempt to obtain this information over the phone, by email, on social media, or by knocking on your door.

8. If you win a prize, a contest or the lottery, you will not be asked to send money to cover the cost of shipping or other expenses.

9. Do not accept and deposit a check at your bank and then agree to wire money to the caller. If the check you deposit turns out to be a fake, you are responsible for repaying the bank.

10. Be sure to use privacy settings on social media and online accounts. Be careful of what you share on social media. Scammers gain and use information about you from these accounts.

Sources: Better Business Bureau https://www.bbb.org/avoidscams/, Federal Trade Commission https://www.consumer.ftc.gov/articles/0060-10-things-you-can-do-avoid-fraud, and Consumer Federal Protection Bureau https://www.consumerfinance.gov/consumer-tools/fraud

How to Protect Yourself Against Identity Theft

1. Secure your Social Security Number (SSN). Don’t carry your Social Security card in your wallet or write your number on your checks. Only give out your SSN when absolutely necessary.

2. Don’t respond to unsolicited requests for personal information (your name, birthdate, Social Security Number, or bank account number) by phone, mail, or online.

3. Collect mail promptly. Place a hold on your mail when you are away from home for several days by contacting the US postal service at https://holdmail.usps.com/holdmail/

4. Pay attention to your billing cycles. If bills or financial statements are late, contact the sender.

5. Enable the security features on mobile devices, especially if you have contacts, banking websites and applications saved.

6. Update sharing and firewall settings when you’re on a public wi-fi network. Consider using a virtual private network, which can give you the privacy of a secured private network.

7. Review your credit card and bank account statements. Promptly compare receipts with account statements. Watch for unauthorized transactions.

8. Shred receipts, credit offers, account statements, and expired credit cards, to prevent “dumpster divers” from getting your personal information.

9. Store personal information in a safe place.

10. Install firewalls and virus-detection software on your home computer.

11. Create complex passwords that identity thieves cannot guess easily. Change your passwords if a company that you do business with has a breach of its databases. The Federal Trade Commission has helpful suggestions at https://www.consumer.ftc.gov/blog/2015/07/advanced-password-tips-and-tricks.

12. Review your credit report once a year to be certain that it doesn’t include accounts that you have not opened. You can order it for free from annualcreditreport.com.

13. Freeze your credit files with Equifax, Experian, Innovis, TransUnion, and the National Consumer Telecommunications and Utilities Exchange, for free. This prevents someone from using your personal information to open a credit account or get utility services.

Source: www.usa.gov/identity-theft