# **Avoid Online Money Scams**

### Why You Should Protect Your Information

It is important to not share your social security number because it is a key identifier used by many government agencies in the United States. It can be used to open financial accounts, file taxes, receive Social Security benefits, and more. Your social security number also serves as a precursor for identity theft; if someone obtains your SSN, they have access to a world of personal information about you.

The Social Security Administration advises that people never give out their SSN over the phone or internet unless they are sure of who they are giving it to and why. Additionally, individuals should never carry their SSN card in their wallets or purses; this could lead to the confidential information being stolen or lost if the wallet is misplaced. People should also be mindful of how much data they are sharing online; too much information can make it easier for identity thieves to steal an individual's identity.

Furthermore, people should regularly monitor their credit reports and bank statements for any suspicious activity. By taking these precautions, individuals can better protect themselves from identity theft and fraudulent activity associated with their social security numbers.

### **Examples Of Online Money Scams**

Online behavior that makes consumers vulnerable to privacy infringement, identity theft, and fraud includes activities like clicking on malicious links in emails or on websites, failing to secure wireless networks, carelessly disposing of devices containing personal information, participating in online scams such as phishing or giving away too much personal information online. E-mail and text-message scams are a particularly cunning method for tricking individuals into revealing their personal details.

Common examples include messages claiming to be from banks or other financial institutions asking customers to update their details in order to access services. By responding to these emails and supplying sensitive data, scammers can then use your information to falsely access accounts and commit fraud. Furthermore, telemarketers may also try to access private information by calling individuals and requesting details like bank account numbers or credit card details in order to offer services or products which are not genuine.

## Strategies To Reduce The Risk Of Financial Fraud

Given the proliferation of technology and internet usage around the world, it is now more important than ever for individuals to take precautionary steps when engaging with technology. It is essential that everyone takes responsibility for their own safety online; understanding how their data may be at risk and doing everything they can to protect themselves is key. Consumers should always be wary of unsolicited emails and calls, even if they appear legitimate; ensuring that anti-virus software is up-to-date will help identify any suspicious activity.

Furthermore, using strong passwords on websites where personal details are stored can help reduce the risks associated with online privacy infringement. Finally, it is also important for users not to share too much personal information publicly: although social media platforms provide an easy way for people to connect with one another, too much detail can leave them open to identity theft and other forms of fraud.

#### What If You Become An Identity Theft Victim

If you are a victim of identity theft, there are certain steps you should take immediately. First and foremost, contact all three major credit bureaus: Equifax, Experian, and TransUnion. Request that they place a fraud alert on your file and instruct them to notify you if anyone attempts to open up new accounts in your name. Additionally, you should order free copies of each bureau's credit report so that you can determine which accounts have been accessed or opened without your approval.

Next, contact the fraud departments at any financial institutions where fraudulent account activity has occurred. Notify them that you believe someone has stolen your identity and have them close or freeze the fraudulent accounts. Furthermore, inform these companies that it is illegal for anyone to use your identity for any purpose whatsoever and ask them to forward your complaint to the appropriate law enforcement agencies if necessary.

It is strongly recommended that victims of identity theft also contact their local police department and file a police report as soon as possible. Obtain a copy of the police report as it may be necessary when dealing with creditors or other agencies during the process of restoring your good name and credit history. Additionally, consider filing an official complaint with the Federal Trade Commission (FTC) by visiting their website or calling 1-877-438-4338 Monday–Friday 8am–8pm EST; they will provide additional guidance on how to address this type of crime moving forward.

**STANDARDS**: 6.12.11a, 6.12.11b, 6.12.11c, 6.12.11d