Module 2 Article

# Protecting Your Money

## 5 Types Of Identify & Cyber Theft

Identity theft is a serious crime that involves the exploitation of personal data to commit fraud. Identity thieves have various methods they can use to obtain this information, such as stealing wallets or breaking into computers. Some of the most common tactics they employ include phishing emails, skimming credit and debit cards, dumpster diving, and exploiting public Wi-Fi networks.

Phishing emails are one of the most popular methods used by identity thieves. These emails appear to be sent from a legitimate source, such as a bank or online service provider, but are actually sent by criminals intending to steal personal information. The emails often contain malicious links or requests for confidential information which will be used for fraudulent activity.

Skimming is another method employed by identity thieves in order to gain access to personal information. This technique involves capturing data from the magnetic strip of debit and credit cards when they are swiped through a card reader or ATM machine. The stolen information can then be used for purchases made over the phone or online without permission from the cardholder.

Dumpster diving is another way criminals attempt to gain access to confidential information about an individual's identity. They rummage through trash cans looking for discarded documents with sensitive information such as utility bills, financial statements, medical forms, and more. The discarded paperwork may contain passwords, account numbers, Social Security numbers, credit scores and other personal details that could be used in criminal activities.

Finally, identity thieves can exploit weaknesses in public Wi-Fi networks in order to obtain personal data. Most public Wi-Fi networks do not require authentication before users connect which makes them easy targets for hackers hoping to intercept any data being transmitted on them (such as passwords). It's important that individuals take precautions when using public Wi-Fi connections and avoid sharing their usernames and passwords while connected.

## 10 Ways To Protect Your Personal Information

1. Change passwords regularly and use a mix of letters, numbers, and symbols to make them more secure. Ensure that passwords are not shared across multiple accounts, such as social media sites or online banking websites, as this could give hackers access to all of your information.

2. Avoid giving out too much personal information online and be aware of what you are sharing publicly on social media and other websites. Ensure that any profiles contain limited info about yourself that cannot be used to identify you.

3. Make sure your computer is protected by installing firewall software, anti-virus software, and other security measures to hinder potential cyberattacks from malicious software or hackers. Additionally, keep these programs up-to-date with the most recent versions so they can best protect your data from the latest threats.

4. Use two-factor authentication whenever possible for additional security for your accounts when signing in remotely or making purchases online. Two-factor authentication requires both something you know (like a password) as well as something you have (like a code sent to your mobile device).

5. Be aware of suspicious emails or phone calls asking for personal details or credit card numbers; do not respond or click on any links contained in these messages. Legitimate businesses will never ask for sensitive information via email or over the phone without prior authorization from the customer first.

6. Check your bank and credit card statements regularly so that you can catch any fraudulent activity early on before it becomes a larger issue; contact the institution immediately if there are unauthorized charges or suspicious transactions occurring in your account(s).

7. Shred documents containing personal identification information before discarding them in order to prevent people from accessing this data if it is thrown away recklessly in an unsecured trash container; invest in a good quality shredder that cuts paper into small pieces so it cannot be reconstructed again later on easily by criminals intent on identity theft activities.

8. Utilize financial institutions' features like alerts via text message, email notification or notifications through their mobile app when important changes occur related to your accounts; with these types of services enabled you can monitor activity happening within your accounts more quickly and easily than ever before while remaining secure at all times in the process.

### How To Safely Manage Finances With Mobile Apps

One of the most important steps people can take to safely manage their finances using mobile technology is to ensure that they are using secure, up-to-date apps. This means downloading the latest version of a mobile application from the official app store or website. To double-check its legitimacy, users should make sure the app is offered by a trusted source, such as a well-known financial institution or software provider. Additionally, users should be aware of any additional security measures provided by the app itself and update their passwords frequently.

Another key step in managing finances with mobile technology is to set up two-factor authentication (2FA). **2FA** adds an extra layer of protection when logging in and requires users to enter a security code after entering their username and password. This code can be sent via text message, email, or through a one-time use application like Google Authenticator. Using this type of verification can help protect accounts from unauthorized access by hackers and malicious individuals.

Finally, when it comes to storing sensitive information online, it’s highly recommended that users encrypt their data with a strong encryption tool like **AES 256**-**bit** encryption or another similar product. This helps prevent anyone from intercepting personal financial information stored on mobile devices and prevents hackers from cracking login credentials or other confidential details. Additionally, many modern encryption tools also work across multiple platforms, allowing for greater flexibility when it comes to accessing data from different systems.

**STANDARDS**: 8.7a, 8.7b, 8.7c