AVOID BEING THE VICTIM OF FRAUD

OPTIVEST WEALTH MANAGEMENT

It is highly likely that in the past you may have been the victim of credit card fraud or some type of identity theft. Fraud is becoming so prevalent, the FBI is overwhelmed with investigations and once you have been scammed, the likelihood of recovering the stolen funds is increasingly less likely. So how can you avoid being the victim of fraud, to begin with?

To start, become aware of how criminals typically gain access to your personal data.

1.) Email hacking through phishing and social engineering

This can occur by allowing fraudulent access to sensitive information such as usernames, passwords, and bank or credit card details by individuals disguising themselves as a friend or trustworthy entity through emails and websites. An example of a potentially fraudulent contact could be something as simple as receiving an email that appears to be from the IRS or even Netflix that asks you to update your personal information. Perhaps you even had a delivery scheduled and are asked to "verify" your information by clicking on a displayed link. All of these could potentially be examples of fraudulent contact and should be reviewed closely before answering.

2.) Impersonation and Identity Theft

In these cases, a criminal uses your personal information to assume your identity for the purpose of committing fraud and other crimes. For example, this can include a criminal impersonating you in electronic or verbal means, or taking possession of your credit and ATM cards, financial statements, and your passwords. Criminals could have gained access to your information after you logged into an app on your phone using a non-secured Wi-Fi spot at the airport or a coffee shop.

Tips to prevent becoming a victim of fraud and cyber fraud:

Use only secured Wi-Fi connections and have strong AND unique and passwords on all sites and/or two-factor authentication when it is available.
Do not download programs or applications from unknown sources.
Run regular virus scans on your computers, laptops, and mobile devices.
Deploy spam filters on your emails.
Watch for spoof emails that seem very similar to your contact's email address such as dave1234@email.com vs daveI234@email.com; look for inconsistencies in language, spelling, punctuation, or even tone can also be frequent clues.
Never share your passwords or personal information in public venues or through open email.
Shred all printed materials which contain your personal information, account numbers and even signatures.
Review your bank and credit card statements regularly.
Change all your passwords regularly and keep them in a secure digital system such as LastPass.

If you do fall victim to fraud or cyber fraud, contact all of your financial institutions immediately (credit cards, investment advisors, bank accounts, etc.). Additionally, consider a credit freeze through the main credit reporting agencies: Equifax, Experian, TransUnion and Innovis. The most responsible action, though, is to remain vigilant and work with companies that take your security as seriously as you do.