Nikki Hall
Independent Associate
Legal & Identity Theft Benefits Specialist
714-357-8851
www.bradandnikki.com

Identity Theft & Fraud Prevention Tips

Types of Identity Theft:

- Credit
- Social Security
- Driver's License
- Medical
- Criminal/Character
- Tax Return

How to protect your credit:

- Obtain free credit report each year at: www.annualcreditreport.com
- Use an aluminum or metal wallet to protect from credit card scanners
- Use credit card instead of debit card for online transactions
- Place a security freeze on your credit
- Sign up for account alerts on each of your accounts
- Use credit monitoring

Types of credit monitoring:

- Protection is offered for free on bank accounts & credit cards
- Monitoring fees charged for monthly monitoring reports
- Most only cover credit and some SS fraud
- Choose IDShield to provide restoration and includes SS, driver's license, medical ID, e-mail and more

Notes:

_____

_____

_____

_____

Ways to Protect your Medical ID, Social Security and Driver's License Information:

- Get copies of your medical records and add new information each time you get treatment
- Check your medical records at least once annually
- Read every explanation of benefits notice from your insurance company and report anything you don't recognize immediately
- When asked for your Social Security Number, ask why it is needed and see if only your last 4 digits can be used, if necessary
- If asked for your driver's license or government-issued ID, ask why it is needed and try not to allow it to be scanned or copied
- Guard your Medicare card (containing SS #) & medical insurance card. Don't carry your Social Security Card.
- If medical card is lost, request a new card #, if possible.
- Do not share medical, SS or driver's license information by phone, e-mail or over the computer, unless you are positive that you are dealing with your doctor or insurance co.
- Request Social Security statements annually and review for accuracy.

When Buying or Selling a Home – Protect Yourself from Wire & SS Fraud:

- Do not use unsecured e-mail to send or receive wire instructions or social security no.
- Call escrow company to verify wire instructions prior to wiring
- Call escrow company to confirm the wire instructions that they will use to wire your proceeds and verify that they will not change your wire instruction prior to closing

Phishing Calls & E-Mails – When you receive a call or e-mail demanding payment or verifying your personal information:

- Get the phone # and contact person's name to call them back
- Use the internet or your bank statement to get the correct phone # for the agency they are calling from to verify if the info is actually needed
- Hover your computer mouse over the link or e-mail address to see who the actual website or e-mail is going to.
- Watch for websites that look correct: vww.chase.com
- Don't use public wi-fi to access any account info

Notes:

_____

_____

_____

_____

_____

_____

Protecting Your Computer from Viruses & Hackers:

- You may get e-mails from people you know, however they contain a link with a virus or a link that will give them access to hack into your computer.
- Is there a subject on the subject that makes sense coming from that person?
- Does it contain a Google Doc, PDF or Word document? Do not click on a link, picture or download a document unless you know what it contains.
- Call or e-mail the person who sent it to ask what they are sending.
- Choose e-mail settings to not show pictures unless it is from a safe sender that you allow.
- Use virus and malware protection. Free: Microsoft Essentials – Preferred: IDShield Malware Protection (included with our service)

Social Media Safety Tips:

- Use privacy settings to not share your info with people who you are not friends with.
- Do not show your full birth date on Social Media. Do not show who your family members are. Do not show your phone #, address or e-mail contact info, whenever possible.
- Do not accept friend requests from people you don't know or from friends who you are already friends with (possible fraudulent accounts).
- Do not send money to friends who request it on Social Media accounts or by e-mail.

Password Safety Tips:

- Use passwords that are not easily guessed and contain at least 8 digits, with numbers, letters (capital and lower case) and special characters
- Don't use the same passwords for all accounts
- Keep passwords in a safe place or use a password protection service, like IDShield's Password Manager.
- Change passwords often
- Enable two factor authentication whenever possible, such as those used by Facebook, Amazon and Google, using both text and answers to questions to reset passwords or use a new computer to login.

Notes:

_____

_____

_____

_____

_____

_____

_____