Worry Prevention Quarterly

For members of the Nawrocki Center Worry Prevention Plan

Nawrocki Center For Elder Law, Special Needs & Disability Planning, PLLC

March, 2016

Identity Theft – It Happens to Real People!

My credit card company provides a service where they send me an e-mail whenever a charge is made on the card without the card being present. Normally I get these notices when I buy something online. But, about a month ago, I received a notice of a large purchase I didn't make. Sure enough, my credit card number was stolen, and a criminal was trying to use it!

I contacted the credit card company immediately and reported the fraudulent purchase. They contacted the company that the purchase was made from, who stopped the purchase from being shipped. The credit card company removed the fraudulent charge from my account, and issued a new card with a different number.

A few days later, I received a call from LifeLock. Someone tried to purchase a cell phone contract using the stolen number. LifeLock was able to stop the purchase before it was completed.

Yes, identity theft happens to real people; it happened to me! There are unscrupulous criminals out there who are coming up with new and increasingly devious means of defrauding ordinary people like us. In this e-newsletter, we have an article which discusses some of the newest scams, designed to prey on seniors and others. Read the article, and learn what you can do to avoid these scams.

If you don't have a service such as LifeLock, get it. Members of the Nawrocki Center Worry Prevention Plan receive LifeLock protection at no charge; if you are a member and opted out of LifeLock; contact the office if you wish to take advantage of it. If you are not a Worry Prevention Plan member, think seriously about signing up for such a service. The cost is small, compared to what it would cost you if a criminal was to steal from your bank accounts or credit cards.

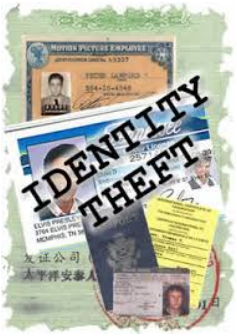
Most credit card companies offer fraud protection notifications by email or text message. Contact your credit card company to see how you can receive these notifications. And carefully review your monthly statement – or look at it online frequently – and immediately report any suspicious charges that you see.

Devious criminals keep trying to steal your identity and money through fraud and scams. The best thing you can do is to keep up-to-date with new scams, be vigilant in identifying and investigating potential attacks on your identity, and use all the tools available to you to help prevent identity theft and financial loss.

Nancy Nawrocki

New Identity Theft Scams Target Seniors

In its January-February 2016 issue, the AARP Bulletin has an article, titled The New Predators, which discusses several new scams that are targeting seniors. These scams happen on your phone, at your door, and online. Here are some scams to watch out for:



The Tech Support Scam: This is purported to be the biggest consumer scam in the U.S. right now. In this scam, you receive an unsolicited phone call from someone claiming to be with Microsoft or Windows tech support, claiming that viruses have been detected on your computer. In order to protect your data, you are told to immediately go to a certain website and follow its instructions. When you do so, malware is installed on your computer to steal your usernames and passwords, hold your data for ransom, and even use your webcam to spy on you. This scam is also perpetrated through unsolicited e-mails and pop-up ads in your browser.

If you get an unsolicited call like this, simply hang up. Neither Microsoft nor its partners make unsolicited calls. And don't click on links on unsolicited emails from Microsoft or Tech Support, and don't click on pop-up ads.

The silent call: The phone rings, you say "Hello," but there is no one on the line. This is a new type of robo-call, collecting your number to build a list of humans to target for theft.

To defend against this call, have your phone company to put caller ID on your land line, if you don't already have it. Then, if you don't recognize a caller's number, don't answer the

phone. If the caller wants to talk to you, they will leave a message and you can decide if and when to call back.

The IRS Impostor: You receive a phone call or a voice message from someone claiming to be from the IRS saying you owe back taxes and threatening that, unless funds are wired immediately, legal action will be taken or you will be arrested. In an alternate version, the caller says you have a refund waiting, but you need to verify personal information to receive it.

In fact, the IRS never uses phone calls to contact taxpayers, they only use letters mailed through the US Postal Service. So if you receive a call like this, simply ignore it. If you are ever in doubt about an IRS matter, call the agency directly at 800-829-1040.

The Cancer Rip-off: Groups ranging from organizations claiming to be large national Cancer organizations to individuals are soliciting donations for cancer research. This may be done via door-to-door solicitation, phone, unsolicited e-mail, postings on Facebook or Twitter, and on GoFundMe sites.

Before contributing to any charity, check out its rating on the website charitynavigator.org. Do not give cash to someone at your door or credit card information over the phone. Instead, ask for more information about the charity (brochures, websites) so you can investigate the card first. If the charity checks out, you can always make your contribution at a later time.

The Chip Card Scam: Banks and credit card companies are in the process if issuing customers new "chip" cards, which are more secure than the older magnetic-stripe cards and are almost impossible to counterfeit. The scam works when imposters shed genuine – appearing emails purportedly from the bank or credit card company requesting personal or financial information, or requesting that you click on a link before being issued a new card.

In fact, no credit card company will email or call you to verify personal information it already has on file before mailing a new card. At most, they will send a letter saying that your card will arrive soon. If you are unsure about the validity of an email from a bank or credit card, call the number on the back of your card (NOT the one in the email) and ask the company if it is trying to contact you.

Faith-based Dating: Con artists are now using faith-based dating sites such as BigChurch, Christian Mingle and JDate to target unsuspecting singles to steal money. People are more likely to fall for scams on sites like these because they can't believe that someone of their own faith is a con artist.

Before getting involved with anyone online, use Google or Spokeo.com to research the person, and view his or her address on Google Maps. "No results found" is a red flag. You can also do a Google Image search for a profile picture. People who are legitimately looking for love won't ask for money – unless they are your kids!

Medical Identity Theft: Unlike most credit cards, there is no protection against fraudulent medical insurance claims, and you can be required to cover the cost of health services you never received. These can include tests, prescription drugs and even operations.

To guard against this fraud, never give social Security, Medicare or health insurance numbers to anyone you don't know and trust. Be particularly wary of free health checks offered at shopping malls, fitness clubs and retirement homes. If they ask to photocopy your cards or sign a blank insurance form, don't do it – after all, it's supposed to be free. Also, carefully review all statements from your insurance provider. If there are charges you don't understand, call them immediately and ask about them. And when shopping online for prescription drugs or other health-related items, remember that if a price seems too good to be true, it probably is.

The Grieving Widow: Con artists know that we are most vulnerable when we lose a loved one. They review obituaries for prey, then pretend to be a bank official to trick them out of money.

When grieving, ask a trust family member to temporarily handle your financial responsibilities. Have that person follow up on any suspicious phone calls or emails. And be aware that while you are grieving, you may be more vulnerable to fraud tactics that play on your emotions.

The Gift Voucher Scam: You receive an unsolicited email from McDonalds, Subway or other popular restaurant or retailer offering a free gift card if you click a link to activate it. The pitch looks legit but it is designed to install malware on your computer or gather personal info by having you complete an online questionnaire.

Never click on a link in an unsolicited email, or divulge personal information. Do a Google search such as "McDonald's gift card scam" and see if any warnings come up. In most cases, they will.

Here are some things you can always do to avoid scams:

On the phone:

- Use your Caller ID to screen calls. If you don't recognize the caller, let the call go to voice mail or to your answering machine. If they really want to talk to you, they will leave a message.
- If you answer a call and it is a solicitation, hang up! You don't owe scammers any courtesy.
- Never give out your credit card or other information to an unsolicited caller. If you are interested in what they have, ask to have information mailed to you or ask for a call-back number. If the offer is legitimate, they will mail or email you information, or give you a number you can call them back on.

At the door:

- Never invite an unsolicited visitor into your house-keep the door closed or the storm door locked.

Recently in the Detroit area, there have been home invasions where a door has been opened to an unsolicited visitor.

- Never give cash to an unsolicited visitor. Ask for a brochure for their cause, and tell them you will decide later. Then investigate the cause before you contribute!

Online:

- Have a good anti-Malware program on your computer, and keep it current. Use Google to research effective anti-malware programs. There are good ones available at no charge with limited features, but a full-featured program might have an annual fee. It is well worth the fee if the program keeps your computer from being infected with malware. Most anti-malware programs will scan your computer and remove existing malware when they are installed.
- Set up your credit cards so you receive an email or text message alert when a purchase is made without a card being present. Contact your credit card company to help you to do this.
- Never click on a link in an unsolicited email or pop-up ad.
- Delete suspicious emails immediately!
- If you receive a suspicious email from a bank, credit card company, or online company, contact the company to see if it is fraudulent. Many scammers send legitimate-looking scam emails. Check the official website of the company to find out how to report suspicious emails; most have a special email address that you can use to notify them of the potential scam.
- If you are dealing with an online company that is not generally known, pay for purchases using PayPal. PayPal can allow you to pay without disclosing your personal credit card information to the online company.

To stay aware of new scams and frauds, you can use online resources such as the AARP Fraud Watch Network. Click on this link, or go to aarp.org/fraud.

Problems with Guardianship Abuse Leading to Calls for Reform

A growing problem with adult guardianship abuse is causing calls to reform the system. Vulnerable elderly can get caught in the guardianship system, being harmed and exploited by the very process that is supposed to protect them.

A guardian is someone appointed by a court to make decisions on behalf of an incapacitated individual ("ward"). The guardianship process usually starts when a family member or social worker notifies the court that someone can't take care of him- or herself. The court often appoints a family member as guardian. However, if the family can't agree on a guardian or there is no family to act as guardian, the court may appoint a public guardian. Public guardians are supposedly neutral individuals who are hired to act in the ward's best interest.

Unfortunately, in many states, the lack of court oversight combined with poorly trained guardians has led to reports of abuse. Once the court appoints a guardian, that guardian has complete control over the ward's property and finances. Guardians can block family visits, determine where the ward will live, and sell property. In addition, guardians charge fees for their services that are payable from the elderly person's bank account, which can cause corruption. When a senior gets caught up in the guardianship system, it can be very difficult to get out. There are many stories about seniors who are confused and overwhelmed after losing control of their lives to a guardian they don't know.

In response to complaints by advocacy groups about guardianship abuse, Florida passed a law in March 2016 instituting changes to its public guardian system. The law creates an Office of Public and Professional Guardians that is required to create standard practices and rules for public guardians. The office also has enforcement power to revoke a guardianship.

If you think a loved one needs a guardian, consult with a qualified elder law attorney to determine the best steps. There may be less restrictive alternatives to guardianship..

In addition, if your family can't agree on the best course of action for your elderly loved one, before fighting over guardianship in court, consider elder law mediation.

For more information about guardianships, go here:http://www.elderlawanswers.com/guardianship/conservatorship.

Make a Referral… Have Dinner on Us!

Do you know someone that we can help? We have a special offer for them, and for you.

For a limited time, you can refer someone to us for a FREE consultation on an Estate Planning or Elder Law legal issue. After they have had their consultation, we will send you a $50 gift certificate to a fine restaurant in the area.

Just fill in your name on the coupon on the back of this newsletter, and give it to a person who can use our services. They can call our office and make an appointment for their FREE consultation.

The FREE consultation offer expires June 30, 2016.

WORRY PREVENTION Quarterly
For members of the Nawrocki Center Worry Prevention Plan

NAWROCKI CENTER
For Elder Law, Special Needs & Disability Planning, PLLC
10299 Grand River, Suite N, Brighton, MI 48116