Consumer Watch

A Monthly Newsletter from the Connecticut Department of Consumer Protection

William M. Rubenstein, Commissioner *Dannel P. Malloy, Governor*

www.ct.gov/dcp Vol. 3, No. 4 April 2014

In This Issue

Suggested Links

www.ct.gov/dcp
Our website offers the latest and most comprehensive information that we have on dozens of consumer-related topics!

www.smartconsumer.ct.gov
Basic information to protect yourself and avoid scams!

https:www.elicense.ct.gov
To verify a license, permit or registration, or to run a roster of licensees. Also, the place for online renewal!

Contact Us

www.ct.gov/dcp

dcp.communications@ct.gov

Find us on facebook

SmartConsumer Contest Winners Announced

They reviewed, they authored, and they won! Students from across the state accepted our challenge during Consumer Protection Week, March 2nd through March 8th. The Department's SmartConsumer contest for youngsters aged 12 to 18 required participants to score 100% on the Department's online quiz and then write and submit an essay about some of the important consumer protection strategies that they learned about.

The three winners, who will receive their prize of an **Apple I-pad Mini**, and **Apple I-pod Touch**, or a **Kindle Fire** at a recognition event later this month, include:

- Erin Special, Norwich, age 12
- Makaila Cerrone, E. Hampton, age 16
- Brian Liao, Glastonbury, age 12

The winning essays are printed in this issue, starting on this page and continuing on page 2.

Congratulations to the winners for their excellent work!

Phone Scamming *by Erin Special*

"Phone scamming" is a term I just learned on smartconsumer.ct.gov, but my family has had experience with it. Phone scammers are people you do not know who call or email you and try to trick you into giving them money. They are very smart and clever. They know the people to target, and they know what they're doing. Everyone must educate themselves about phone scammers to protect themselves.

Phone scammers might pretend to be a friend or family member and say that they are in trouble in a different state or country. If they are young, they will probably ask you not to tell their parents. Scammers might also pretend to be a business and claim that your account is overdue.

More, page 2

From the Commissioner

As tomorrow's leaders, today's youth must prepare to be savvy consumers, and we're pleased to name the winners and share the winning essays from our Smart Consumer contest. Kudos to everyone who participated! Another milestone has been reached in the creation of a program that will soon offer some of the state's very ill patients a palliative treatment option, and like most stakeholders, we are eager now to witness the evolution of this new patient-care industry. Tax season brings scammers to the forefront, so spend a minute on page 3 to refresh your memory on common tactics these scams utilize. Two events that might be of interest to many are on the schedule for this spring -- the last Small Claims Court workshop till the fall (page 4) and on page 2, news about a food recall seminar appropriate for anyone involved in Connecticut's food industry, co-sponsored by the Connecticut Association of Food Protection.

Enjoy the long-awaited spring!

William Rubenstein

SmartConsumer Contest Winners, *continued from page 1*

Phone Scamming *…continued from page 1*

They will tell you that you need to give them your credit card number right away to avoid closing your account or damaging your credit. When they call, they will rush you so you will give them what they want without even having time to think.

Phone scammers can go after anyone, so we all have to be aware and prepared. When my phone rings, I look at the Caller ID. If I don't recognize the name or number, I won't answer it. My mom won't let me have my own email address, so I don't have to worry about that yet. She is careful about scammers and spam in her email.

People have tried to scam my grandma over the phone. One day, her phone rang and she answered it. The person on the phone pretended to be my cousin. He said he was arrested for drugs but they weren't his. He said they belonged to a friend of his but the police didn't believe him. He asked her to send money right away to get him out of jail, but please don't tell his parents. My grandma believed it was my cousin at first. She said it sort of sounded like him but he sounded far away. She told him that she had to hang up to make the arrangements.

She was rattled by the call, but something about it didn't sound right to her. She called my cousin's cell phone and he answered it. He told her he was fine and he was not in any trouble. My grandma called the police. The police said they had received several calls from grand-parents with similar stories, but they couldn't do anything about it because no money was sent. If my grandma sent the money, they could find the people. My grandma didn't want to do that.

Grandma and I will never fall for a phone scam because we are aware that scammers are out there, and we know to be careful. I am going to tell my friends about phone scamming so they will know how to protect themselves and their families. They and their parents will know what to do, and they will all stay safe.

Internet Safety: Teens Might Not be as Safe as They Think *by Makaila Cerrone*

The most important new subject I learned about on this website was how vulnerable I am online and what I can do to protect myself. This section was very applicable to my life because as a teenage girl always wanting to be in touch with my friends, it's no surprise that I have a Twitter, Instagram, Facebook and Tumblr and use them both on my mobile device and regular computer. I always thought I was pretty safe on the internet since I never use online chats, never add people on my social networks that I don't know, and don't post personal information such as my phone number or address. I never realized how much I am still at risk.

The first section that alarmed me was the dangers that smartphone apps bring. I have over 30 apps on my cell phone and have never once actually read the privacy policy because I never thought it was necessary. I didn't realize how much personal information could be spread just by simply pressing the download button.

I learned to read the apps policies before blindly clicking accept and to do a little bit of research about an app before deciding to download it. Five minutes of research and reading could be the difference between whether or not my phone becomes infected with malware or my personal information becomes shared with hundreds of people.

Another aspect of online safety that concerned me was public Wi-Fi. I only have a certain amount of data on my smart phone so I join public Wi-Fi networks wherever I can without thinking twice about it. I didn't realize other people using the same Wi-Fi network could log into my accounts and steal all of my information. I learned that I'm not truly safe using a Wi-Fi network unless the network asks me for WPA or WPA2 password.

more, page 4

Things I Learned *by Brian Liao*

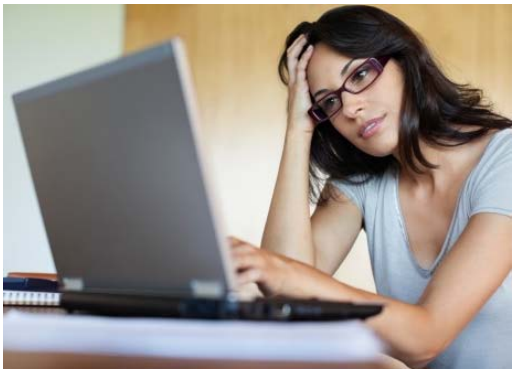
There is a variety of things I've learned from the Smart Consumer web site. One is the pre-paid card. I've learned that unlike many other forms of getting money, pre-paid cards do not require photo identification to spend the money on one. They are especially hard to trace and the transactions on the cards are quick. Worst of all, if the card or the all-important serial number falls into the hands of a scammer, the money on the card (millions of dollars can be stored on one card) will be added to the scammer's card to spend on their wants. This relatively new way for scammers to steal your money, with its benefits to scammers, is why they use them.

The second thing I learned about was computer protection. I learned that most free Wi-Fi hotspots are not secure, meaning they do not include encryption. Encryption is the state where a picture or a document on a computer is scrambled and put into a code when sent from a secure Wi-Fi hotspot or a secure website, and re-arranged back into the document when it is received at the receiving end. With encryption, scammers have a hard time deciphering the scrambled document, lowering your chance of being a victim. A secure Wi-Fi network will ask for a WPA or WPA2 password, and only then can you tell that the network includes encryption. If the web address begins in "https", that would mean that the site is secure ("s" stands for secure). No matter what, never send personal info such as credit card numbers and social security numbers through E-mail, even though you have encryption. This information can be used by scammers to gain access to money or other private documents. These precautions can help stop scammers from stealing personal documents. Scammers have another tool they can use- malware. Malware is bad software that sneaks its way into your computer if its security software, web browser or operating system is not up-to-date. By fixing these problems, you can get rid of bad software and spyware which can affect you in more ways than one.

The final subject that I found new was phone fraud. Scammers try to extract money or other info that can help them obtain even more of it, all from the victim. Scammers try to do so in many different ways- saying you won the lottery, but need to pay a fee in order to claim the prize, a family member or friend needing money because they're in trouble, or threats of shutting off a service if you do not pay your supposedly "overdue" bill (pretending to be a phone or other service company). Though these excuses seem real, they are really scammers trying to get your money or information. Some ways you can sniff out fraud are by listening for the immediate demand for money. Another is to call the family member and ask if they called you, or another family member and check to see if they're all right. Remember that prizes don't need to be paid for - ever. If an inheritance is mentioned, ask for the opinion of someone you trust. Personal info such as credit card numbers and social security numbers must not be shared.

From the extremely helpful and interesting SmartConsumer web site, I have learned about prepaid cards, computer safety, and phone fraud. After reading through the site, these are the three topics that stood out to me.

How to Recognize an Online Tax Scam



Another tax season is wrapping up, and criminals are pushing their tax scams. Because recent major data breaches exposed sensitive consumer information on a large scale, be even more watchful and vigilant now against ID theft and other online crimes.

Signs of an Online Tax Scam
Beware of any "official" emails that:

- Ask for personal and/or financial information such as name, SSN, or credit card numbers or security-related information, such as your mother's maiden name. The requests might be in the email itself or on another site to which you are directed;
- Include paid offers to grab your interest, such as promising a tax refund or offering to pay you to participate in an "IRS" survey;
- Threaten a consequence for not responding to the email, such as additional taxes or blocking access to your funds;
- Have incorrect spelling, incorrect grammar or odd phrasing;
- Include a downloadable document (usually in PDF format) that will supposedly explain changes to the tax laws. (The documents probably contain malware.)

Avoid Becoming a Victim if you prepare your tax return and/or file electronically:

- Secure your computer by installing the latest security updates. Check that your anti-virus and anti-spyware software are running properly and are receiving automatic updates. If you haven't already done so, install and enable a firewall.
- Carefully choose sites you visit. Be cautious when you search for tax forms or seek advice on deductibles, tax preparers, and similar topics. Do not visit a site by clicking on a link sent in an email, found on a blog, or in an advertisement. The website you land on may look just like the real site, but could be fake.
- Be wary of Wi-Fi. Wi-Fi hotspots are intended to provide convenient public access to the Internet and are not always secure against hackers. *Don't use Wi-Fi to file your taxes*.
- Never send sensitive information in an email. It may be intercepted by thieves.
- Keep an eye out for scams. Common scams promise tax rebates or offer deals on tax preparation or free tax calculation tools. Emails claiming to be from the IRS are definitely fake -- the IRS will not contact you via email, text messaging or social network, nor will it advertise online. Do not respond to an email that appears to be from your employer, bank or broker claiming there is an issue with your tax information and asking you to verify something; it might be a scam. Contact the person or business by phone or in person.
- Use strong passwords. Scammers now have software to guess passwords. Don't use dates that might be publicly available in some document or database. Passwords should have a minimum of nine upper case and lower case letters, numbers and symbols. Use different passwords for your work and personal accounts. Change them all a few times each year; keep them written down and stored in a safe place.

Medical Marijuana Program Selects First Dispensary Facilities

On April 3rd, Connecticut's first medical marijuana dispensary facilities were named and are now preparing to begin operations later this year. The dispensary facilities and the four growing operations named in January will serve Connecticut residents who have been certified to receive medical marijuana for palliative treatment of one of eleven serious illnesses. *(Consumer Watch, February 2014)*

"With the selection of dispensary facilities, all necessary pieces of the medical marijuana program are in place and we are poised to provide patients with a safe and secure source of needed medicine," Commissioner Rubenstein said. "As retail points from which products are dispensed and educational materials are provided to patients, the dispensary facilities will be the public face of Connecticut's medical marijuana program, and therefore, careful thought and deliberation went into selection of the most qualified applicants."

The six dispensary facilities are:

Arrow Alternative Care, Inc.	92 Weston Street Hartford, CT
Bluepoint Apothecary, LLC	469 East Main Street Branford, CT
D & B Wellness, LLC	2181 Main Street Bridgeport, CT
Prime Wellness of Connecticut, LLC	75 John Fitch Boulevard South Windsor, CT
Thames Valley Apothecary, LLC	1100 Norwich-New London Tpke (Rte 32) Uncasville, CT
The Healing Corner, Inc.	159 East Main Street Bristol, CT

More, page 4

Tax Scammers Now Try Dialing for Dollars

"Your driver's license has been suspended. You will be arrested. You will be deported. We're on our way to your home right now." These are a few of the threats that scammers made to hundreds of Virginia residents in recent weeks. The scammers used fake names and IRS badge numbers, and were described as aggressive, insistent, and easily angered when victims didn't immediately agree to their demands for payment of "overdue tax balances" by pre-paid card. Do not give in to these threats if you get such a call; hang up and notify local police instead!

True or False?

Our April newsletter reported that the top consumer complaint received by the Department changes from year to year and is always different from one year to the next. ***True or False?*** *Answer, page 4*

Internet Safety, ***cont. from page 2***

I also learned that to really protect myself I can send my information through a secure website and look for web addresses that begin with https in order to insure that my information is safe. In addition, I learned to change up some of my passwords and usernames since I virtually have the same one for every website I visit.

Overall as a teenager in the digital age, staying safe online is the information that pertained most to my life and what I take most from the smart consumer website. Myself, and undoubtedly many other teens, don't realize how much danger we put ourselves in every single day just by down-loading an app or connecting to a Wi-Fi network. I believe teenagers can take countless amounts of useful tips from this website as I have, and hopefully become a more concerned group when it comes to protecting ourselves online.

Food Recall "Train-the-Trainer" *Seminar Scheduled for May 27th*

The Connecticut Department of Consumer Protection and its program sponsor, the Connecticut Association for Food Protection (CAFP), are pleased to invite food manufacturers, growers, food industry representatives, retailers, distributors, State public health and agriculture employees and officials, and members of the University of Connecticut extension program for this important seminar on:

Tuesday, May 27, 2014
8 am-4 pm
at the
Holiday Inn Hartford East,
100 East River Drive, Hartford

When registering at the link below, please take the time to answer the 10 survey questions about your knowledge of food recalls, recall strategy and planning. We will use this information to capture industry knowledge and identify gaps within the state in recall readiness and preparedness.

Register here!

A $20 fee is requested to register for the event. **Please make checks payable to CAFP** and send at your earliest convenience (by May 22nd) to:

Frank Greene, DCP Food & Standards
165 Capitol Avenue, Hartford, Connecticut 06106

If you have questions about the seminar, please email **Lisa.Fluker@ct.gov**

Medical Marijuana, *continued from page 3*

Like the producers earlier this year, the facilities were chosen through a competitive process, from 27 applicants that submitted proposals in November 2013.

The selected dispensary facilities will be eligible to receive their licenses upon payment of the $5,000 license fee and submission of certain final documentation, which must occur within 30 days. Upon receiving their State license, the dispensary facilities will begin construction efforts as needed, hire and train staff, develop educational programs and materials, and create appropriate, Department-approved advertising and signage. All are expected to be ready to open and serve patients by the time marijuana products are available from licensed producers sometime this summer.

Connecticut's is the first state medical marijuana program based on the pharmaceutical/ medical model -- from physician certification, to production facilities operating as pharmaceutical manufacturers, to dispensing to patients by licensed pharmacists.

The Department's role is now oversight of producers and dispensary facilities as they gear up and begin full operation later this year. Department inspectors and agents will ensure full compliance with State law and regulations.

It appears that the work continues for everyone involved in the formation of this new patient-care industry in Connecticut.

Last Small Claims Court Workshop Until Autumn!

This brief evening program will provide you with a free introduction to Small Claims Court. You'll learn how to file a case and represent yourself. UCONN Law School students are offering this program for the public. Sign up today to attend the workshop on:

Tuesday April 15 from 6:00 to 7:00 pm
Reading Room, Starr Hall
UCONN Law School, 45 Elizabeth St., Hartford

Register at this link or email Andrew.glass@uconn.edu.

True or False? *Answer*

The answer is False. We reported that for the first time in at least a decade, home improvement complaints ranked second only to fuel-related complaints in 2013, partly due to the sudden closure of a home heating company during the year. The number of home improvement complaints was actually slightly higher than that of 2012.

Complaints about home improvement contractors and new home builders typically involve issues such as unfinished work, improper contracts, damage to home or property, shoddy materials, and non-return of deposit. Working with a contractor who is properly registered with the Department of Consumer Protection is crucial, as is getting numerous, excellent references and a detailed, written, signed and dated contract that includes a start date, end date, and all aspects of the work to be done, including the quality of materials to be used. The contract must also state that you have three business days to cancel!