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. 1, No. 8 January 2012

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!

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

Unsubscribe

To unsubscribe to Consumer Watch, control-click here and press "send"

Are You Gambling with Your Winnings?

The Department of Consumer Protection's Gaming Division works to ensure the highest degree of integrity in all forms of legalized gaming in Connecticut, and at the two state's two federally-recognized tribal casinos. This involves regulating casino games, lottery drawings, scratch-off tickets, pari-mutuel betting, bingo, and sealed tickets, among others.

While our efforts ensure fairness in the games we regulate, there are many situations that consumers need to watch for in order to protect themselves. Wherever money is involved, recognize that someone could be using unfair and even illegal means to pocket it for themselves. Smart consumers stay alert and take responsibility for themselves when participating in any form of gaming.

Keep an Eye on Your Lottery Tickets

While the Connecticut Lottery is safe to play, and the vast majority of lottery retailers are truthful and reliable, it doesn't hurt to take a few precautions, as some people may try to take advantage of a winning ticket. So, always watch the checking process, and when possible, check tickets yourself using the "ticket checker." If a clerk tells you that you don't have any winning tickets, ask him or her for all of your tickets back. Always check your tickets a second time before tearing them up and throwing them out. Whenever you turn in a winning ticket, be sure to verify the value of the ticket on the customer display. Once you receive your payment, lottery agents are instructed to tear the ticket in half and discard it.

In a scam active now in California and Texas, con artists work in pairs or groups. One con artist approaches the victim outside a store or business, and says that he has a winning ticket but cannot collect the prize for some reason – he is in the country illegally, isn't 21, cannot pay the taxes, or just wants an honest person like the victim to help verify the numbers.

A second con artist appears, joins the conversation, and as their enthusiasm builds, the first scammer offers to sell the winning lottery ticket to the victim for a "bargain" price – much lower than the "winnings" to be collected. Sometimes the con artist even escorts the victim to the bank to get money or valuables. When the victim then turns in the "winning" ticket, he discovers that it is not valid.

more, page 2

From Commissioner Rubenstein

The past year has certainly been dynamic for the Department of Consumer Protection and its staff as we met the challenge to consolidate with another state agency and integrate staff and functions into our new Gaming Division, which oversees legal gaming in the state including the Lottery, off-track betting, certain casino operations and charitable bingo, bazaars and raffles. Given our months-long internal focus on gaming issues, we've chosen in this issue of Consumer Watch to shed light on gaming problems that consumers can prevent and avoid, such as keeping an eye on lottery tickets and sidestepping illegal, fraudulent or improperly-run games.

The start of a new year is also a perfect time to do a thorough cleaning of your computer and update your security measures, so I hope you'll find our articles related to malware on Page 3 helpful.

Here's to a happy and healthy new year!

William M. Rubenstein

Commissioner Rubenstein was appointed by Governor Malloy and approved by the Legislature in 2011.

Changes Coming to Sealed-Ticket Sales

Since 1987, the State of Connecticut has been the sole source for the purchase of sealed-ticket game products by permittees in the state, but that's about to change.

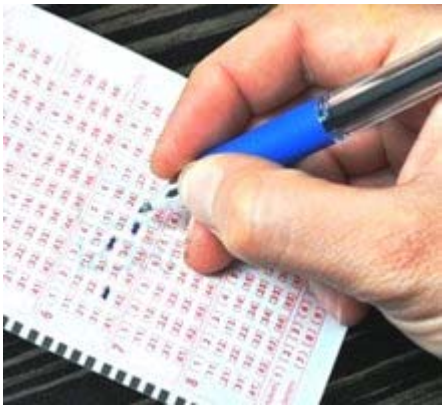
A recently-enacted law will eventually transfer responsibility for the sale of sealed-ticket game products from the Department of Consumer Protection's Gaming Division to authorized, privately-owned, sealed-ticket distributors.

In order to implement this change, sealed-ticket game product manufacturers and distributors will need to register with the Department of Consumer Protection for authorization to manufacture, sell or distribute tickets in Connecticut. The Gaming Division will maintain regulatory oversight of all sealed-ticket activity and continue to permit nonprofit organizations to sell sealed-ticket game products as fundraising items.

We expect several manufacturers and distributors to be registered early this year, making available a greater variety of sealed-ticket products for purchase by non-profit organizations. Once the transition is complete, sealed-ticket permittees will buy only from any of the registered distributors, rather than from the State.

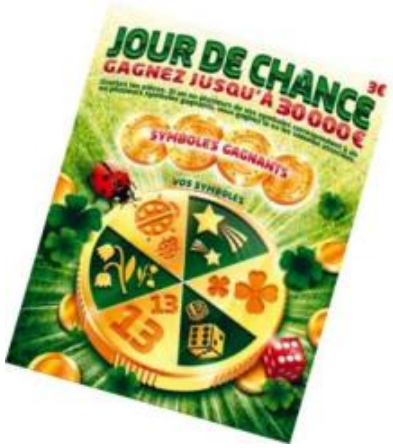
The Department is working to ensure a smooth transition for sealed-ticket permittees, manufacturers, and distributors. It will soon adopt updated regulations governing the sale and distribution of sealed-tickets; meanwhile, it continues to sell off its existing sealed-tickets. For more information, you may call the Gaming Division at 860-594-5480.

Winnings, *from page 1*



What's the Word on Foreign Lotteries?
A lottery is simply a promotional device by which items of value are awarded to members of the public by chance, but some form of payment is required to participate – such as buying a ticket. Legitimate foreign lotteries do exist -- *but only for people located in those countries*. It is illegal for a U.S. citizen to use a telephone, internet or mail to play a foreign lottery from within the United States, just as it is illegal for most foreign citizens residing in another country to play a U.S. lottery unless they are visiting in the United States. Lotteries in the United States and most developed countries are illegal unless conducted by a governmental entity or specific, exempt licensed charitable organization.

Nevertheless, scam operators use telephone, email and direct mail to entice consumers around the world to buy chances or collect their winnings from high-stakes foreign lotteries – because sadly, this scam still works. Lottery scammers acquire names, addresses, phone numbers and email addresses of potential victims via spyware and other tools, and through various trade journals, business directories, magazine and newspaper advertisements, Chambers of Commerce -- anywhere that information appears on the Internet or in print.



Lottery scams typically notify their "victims" they have won a prize, which can be claimed only after the victim pays some transfer fees or taxes, and/or provides some proof of identity and/or details of bank accounts or credit cards. Some scammers even send a real-looking check as part of the winnings, which the victim is told to deposit and return some amount to cover the associated fees and taxes. Of course, no legitimate lottery will EVER send a portion of winnings and ask someone to send part of it back in fees. Victims who take the bait send money from their own account to the scammers; the "check" eventually proves to be a fake; their money and their "prize" are lost forever. Steer clear if you see any of the following signs of this scam:

- You're informed that you have won a lottery prize - but you did not buy a ticket.
- A "winning letter" is personally addressed to you but it has been posted using bulk mail - thousands of others around the world are receiving the exact same notification.
- You're informed that you have won a lottery prize and are asked for money up-front to release your "winnings."
- You're informed that you have won a lottery prize and are asked for bank account, credit card, or other confidential information.
- You're informed that you have won a lottery prize and are told you must comply with the terms immediately or the money will be given to someone else.
- You're offered an opportunity to buy shares in a fund that buys foreign lottery tickets.

Again, playing any foreign lottery from within the U.S. is against federal law, and anyone inviting you to do so is already showing criminal intent. There are no secret systems for winning foreign lotteries; your chances are slim to none. Buying even one foreign lottery ticket will lead to more bogus offers. A legitimate lottery does not require you to pay fees to collect your prize, and taxes are due AFTER you receive the winnings. If you're lucky enough to be holding a winning ticket, it's you who notifies the lottery -- they do not notify you.

If you receive a notice from what seems to be an illegal lottery, you may forward a copy to your local Post Office to possibly help prevent others from receiving the same scam. Otherwise, just ignore and recycle!

Reduce your chances of downloading more malware!

- Don't click on a link in an email or open an attachment unless you know who sent it and what it is. Links in email can send you to sites that will automatically download malware to your machine.

Opening attachments — even those that appear to come from a friend or co-worker — also can install malware on your computer.

- Download and install software only from websites you know and trust.

Downloading free games, file-sharing programs, and custom toolbars may sound appealing, but free software can come with malware.

- Talk to your family about safe computing. Make sure everyone understands that online activity can put a computer at risk and out of service. This includes clicking on pop-ups, downloading free games or programs, or posting personal information.

- Routinely monitor your computer for unusual behavior. If you suspect your machine has been exposed to malware, take action right away.

- Report problems with malware to your Internet Service Provider so that it can try to prevent similar problems and alert other subscribers.

Minimizing the Effects of Malware on Your Computer

Malware, a term applied to a host of software types that infect personal computers by copying and transmitting themselves to other users, by monitoring and logging user keystrokes to gather personal data, or by covertly hijacking computer processors for other purposes, is an under-recognized threat to personal security, according to State information technology experts.

"We've gotten security reports indicating that some personal computers used by residents to log in to State online services are compromised with malware," Consumer Protection Commissioner William M. Rubenstein said. "Although their transactions with the State are secure, we believe that hidden keystroke loggers or other malware on residents' personal computers definitely pose a threat to the security of their information."

The Department is reminding computer users that strong computer security measures include a combination of **firewall**, **anti-virus** software, **anti-spy** software, and **anti-malware** software. While many one-stop solutions exist, a combination of strategies is most effective, according to agency IT personnel.

The Federal Bureau of Investigation announced in November 2011 that it had busted a pack of Eastern cyber-thieves known as the Rove group. This group had hijacked at least four million computers in over 100 countries, including at least half a million in the U.S., making off with $14 million in "illegitimate income" before being caught. The malware allegedly used in the massive and sophisticated scheme targeted websites for major institutions like iTunes, Netflix and the IRS -- forcing users who tried to get to those sites to different websites entirely. The hackers rerouted internet traffic illegally, using the infected computers to reap profits from internet advertisement deals.

Closer to home, the Department of Consumer Protection learned that some of the personal computers interacting with the State's various online business systems show signs of being compromised by malware. These compromised computers belong to Connecticut residents who are using the machines to access online State services.

State information analysts are notifying affected computer users if indications point to their computer being infected. They also recommend that owners take immediate steps, such as alerting credit companies and banks in order to protect personal information, and pursuing corrective IT services to eradicate the malware from their computer.

Telltale signs that a computer may be infected with malware include:

- The computer works more slowly, frequently malfunctions, or displays repeated error messages.
- The computer won't shut down or restart as normal.
- The computer displays a lot of pop-up ads, or pop-up ads appear when not surfing the web.
- The computer displays web pages or programs not launched by the user, or sends emails that the user didn't write.

If you suspect malware has infected your computer, **STOP** online shopping, banking, or other activities that involve user names, passwords, or other sensitive information. The malware could be collecting and sending your personal information to identity thieves.

continued, page 4

Sweepstakes: Don't Pay to Play!

Who doesn't ***love*** the idea of winning something for nothing? Nearly half of all American adults enter sweepstakes each year, mostly contests run by reputable marketers and non-profit organizations to promote their products and services. Capitalizing on the popularity of these offers, some con artists devise schemes that look like legitimate sweepstakes, and every day, U.S. consumers lose thousands of dollars to these unscrupulous promoters.

A sweepstakes is a promotion in which prizes are awarded to participating consumers by **chance**, with no purchase or entry fee required to win, and no fees or taxes to be paid before receiving the prize. Two common types of sweepstakes scams are:

- A "winning" notification is sent from a real business, but the prize is either fake, or actually an offer for a multi-level marketing scheme, timeshare, travel club, or something similar.
- A notice is sent by a scammer who is **unaffiliated with any** real organization. Claiming to represent a legitimate organization such as a national bank or the non-existent "National Sweepstakes Bureau," they offer assurances that the sweepstakes is safe and legitimate. In truth, there are no prizes, it's just a ploy to get your money.

Both scams require consumers to send or provide funds to claim a prize they've won. But, as many have learned the hard way, "free" prizes never materialize. If you're tempted by a letter, email or telephone call telling you that you've been chosen to receive a great prize, remember:

- ✓ **Don't pay to collect:** Legitimate sweepstakes don't require you to pay or buy something to enter or improve your chances of winning, or to pay "taxes," "insurance" or "shipping and handling charges" to get your prize.
- ✓ **Confirm authenticity:** Sponsors of legitimate contests identify themselves prominently; fraudulent promoters are more likely to downplay their identities.
- ✓ **Read the fine print:** Bona fide offers clearly disclose the terms and conditions of the promotion in plain English, including rules, entry procedures, and usually, the odds of winning.
- ✓ **Skip the sales pitch:** Agreeing to attend a sales meeting just to win an "expensive" prize is likely to subject you to a high-pressure sales pitch.
- ✓ **Expect more spam:** Signing up for a sweepstakes might subject you to more promotion tactics.
- ✓ **Don't provide personal information.** Disclosing your checking account or credit card account number in response to some promotion or contest is a sure-fire way to get scammed.

Malware, *continued from page 3*

Next, **ALERT** your credit companies and banks in order to protect your personal information. Finally, **CONFIRM** that your security software is active and up to date. Every home or laptop computer should have anti-virus and anti-spyware software, a firewall and one or more anti-malware programs. You can buy each item as a stand-alone, or they can be packaged into a security suite. Most importantly, you must keep these programs **current** by downloading security updates frequently.

Once your computer is thoroughly clean, remain alert in order to avoid new malware downloads to your machine. Some scammers actually distribute their malware disguised as anti-spyware! So, don't fall for software ads that appear in pop-up messages or emails, especially those that claim to have scanned your computer and detected malware. That unfair tactic has already attracted the attention of the Federal Trade Commission and various law enforcement agencies, and is under investigation.

OnGuardOnline.gov, which is maintained by the Federal Trade Commission, is a useful consumer website with more tips on securing your computers, protecting personal information, and guarding against Internet fraud. Make it a point to practice safe computing -- always!

There IS Help for Problem Gambling

For most people, gambling is a social or recreational activity, fun and entertaining. But for others, gambling causes problems, becomes uncontrollable and is no longer a choice. Problem gambling includes all gambling behaviors that compromise, disrupt or damage personal, family or vocational pursuits to **any** degree. Someone who is becoming a problem gambler may experience:

- an increased preoccupation with gambling;
- a need to bet more money more frequently;
- restlessness or irritability when trying to stop;
- an impulse to "chase" losses; and
- a loss of control manifested by continuation of the gambling behavior in spite of mounting, serious, negative consequences.

Help is available across Connecticut. Visit **www.ct.gov/dcp** and look for "Problem Gambling Resources" on our home page.