

In this issue;

- Protecting Your Identity
- Phishing Trips and Other IRS Scams
- New Mileage Deduction Rates

DWORKEN, HILLMAN, LAMORTE & STERCZALA, P.C.

Being GREEN = Emailing future issues!
Please send your current email address to Lynn at lynnb@dhls.com
(Addresses of colleagues & friends are also welcome.)



Your Identity – It's Yours to Lose

by Michael F. Ganino, CPA

Whether its children who write their names on a box of crayons and tuck them in the back of their school desk, teenagers who place their belongings in school lockers or adults who click a button to set a house or car alarm, we instinctively understand that in order to protect things of value, we must be proactive. Aside from non-material items, most people would agree that there are few things of greater value than their identity; however, it's surprising how little most individuals do to effectively protect it.

You fall victim to identity theft when someone steals and uses your personal information, such as a social security number or credit card, without your permission. So widespread has identify theft become, that The Federal Trade Commission (FTC) has estimated over 9 million Americans will fall victim to this crime every year, making this the fastest growing offense in the United States.

With the quantity of personal information available and ease at which technology makes it available, you may think you're fighting a losing battle, however a quick internet search will reveal countless resources that could be used to your advantage. In this article, we present some of the most effective ways to protect your personal information, along with practical yet simple steps to reduce the risk of you falling victim to identity theft.

1. Protect identifying numbers such as your social security number

- Be cautious when asked to give your social security number and before complying, inquire as to the reason it's needed and how it will be protected
- Never carry your social security card or a copy of it in your wallet, purse or vehicle

2. Dispose of sensitive items properly

- Destroy bank statements, medical records, paid bills, credit card statements and other documents that contain sensitive personal information
- Professionally remove information from hard drives of computers being donated to charity or sold

3. Treat outgoing and incoming mail carefully

- Limit placing outgoing mail in unsecured mail boxes such as your home mailbox
- Retrieve incoming mail as soon as possible and if you are out of town, arrange for your post office to hold all mail and deliver it upon your return

4. Use caution when using the internet

- Avoid entering personal information on websites you do not feel comfortable with
- Utilize internet security systems and place your computer security settings to the highest level practical
- Make use of features such as the "last login date noted" and assure this information is consistent with your prior usage

5. Select passwords with the appropriate security level

- Steer clear of over simplified passwords, such as birthdates, maiden or children's names
- Secure the passwords appropriately and change them on a regular basis

6. Beware of unsolicited requests for information

- Never respond to unsolicited emails that request personal information
- Be cautious when using unsecured links (for example, links that do not have "https" as part of the address)
- Note that government agencies will only correspond using the United States Postal Service. Emails from agencies such as the IRS should be treated as an attempt to gain access to your personal information. ■

DHL&S Family News & Events

- **Congratulations** to Mark Pires, who has been promoted to Senior Accountant. A warm welcome to our new staff accountants Emily Joy, Robert Vieira and James Norton. And double congratulations to Katie and Anthony Regan on Katie's promotion to Supervisor and on the birth of their son, Jack.



If You Teach a Man to Phish... Watch Out for IRS Imitators

by Walter R. Fulton, CPA, MST

Identity thieves constantly try to prey upon people's unease about dealing with the Internal Revenue Service as a tool in their attempts to gain access to sensitive information. More and more, they are using e-mail to accomplish this.

The IRS has repeatedly stated its policy that it NEVER initiates taxpayer communications through e-mail, only through the U.S. Postal Service. So, if you receive an email purporting to be from the IRS, be on the alert that you may be a victim of a "phishing" expedition.

What is phishing?

Phishing is a scam typically carried out by unsolicited e-mail and/or websites that pose as legitimate sites and lure unsuspecting victims to provide personal and financial information.

According to the IRS ALL unsolicited e-mail claiming to be from either the IRS or any other IRS-related components should be reported to phishing@irs.gov.

If you receive an e-mail claiming to be from the IRS that contains a request for personal information:

1. Do not reply.
2. Do not open any attachments. Attachments may contain malicious codes that will infect your computer.
3. Do not click on any links
4. Forward the e-mail as-is, to the IRS at phishing@irs.gov.
5. Then delete the original email

Further information on identity theft issues relating to the IRS is available on their website at www.irs.gov. ■

IRS Increases Mileage Rate to 55.5 Cents per Mile

The Internal Revenue Service recently announced an increase in the optional standard mileage rates for the final six months of 2011 in recognition of recent gasoline price increases. You may use the optional standard rates to calculate the deductible costs of operating an automobile for business and other purposes in lieu of tracking actual costs.

You always have the option of calculating the actual costs of using your vehicle rather than using the standard mileage rates – just make sure you have receipts to back up your claim.

Mileage Rate Changes from 7/1/11-12/31/11

Business from .51 to 55.5

Medical/Moving from .19 to 23.5

Charitable stays at .14

For more information on how we at DHL&S can help with these and other tax planning and financial opportunities, please contact your tax specialist at 203-929-3535, or visit our website at www.dhls.com.



More IRS Scams To Be on The Lookout For

by Walter R. Fulton, CPA, MST

The Internal Revenue Service has recently noted an increase in tax-return-related scams, frequently involving unsuspecting taxpayers who are led to believe they should file a return with the IRS for tax credits, refunds or rebates for which they are not really entitled.

Unscrupulous promoters and unlicensed tax return preparers deceive people into paying for advice on how to file false claims charging unreasonable amounts for preparing illegitimate returns. In other situations, identity theft is involved.

According to the IRS, taxpayers should be wary of any of the following:

- Fictitious claims for refunds or rebates based on excess or withheld Social Security benefits.
- Claims that Treasury Form 1080 can be used to transfer funds from the Social Security Administration to the IRS enabling a payout from the IRS.
- Unfamiliar for-profit tax services teaming up with local churches.
- Home-made flyers and brochures implying credits or refunds are available without proof of eligibility.
- Offers of free money with no documentation required.
- Promises of refunds for "Low Income – No Documents Tax Returns."
- Claims for the expired Economic Recovery Credit Program or Recovery Rebate Credit.
- Advice on claiming the Earned Income Tax Credit based on exaggerated reports of self-employment income.

Remember the old adage: if it sounds too good to be true, it probably is.

Our experienced tax staff can help you avoid these situations and provide you with quality expert tax planning advice designed to minimize your taxes legitimately. Please contact us immediately if you receive any of these unsolicited propositions at 203-929-3535. ■