Small Business Aide

Mary Passino, JD

10 things you should know about identity theft

1 Scams are everywhere. Identity theft has become a major problem. Strictly speaking, identity theft occurs when someone literally steals your identity. They set up bank accounts, take out credit cards, file tax returns, and borrow money in your name. Related scams include someone using your credit card number illegally or stealing your PIN and looting your bank account.

2 Bogus e-mails designed to steal your identity, also known as phishing, are becoming a major problem. While they can take many different forms, most scams are designed to trick you into revealing personal information such as your social security number or online account password. Through clever use of logos and familiar-looking web addresses, these e-mails often appear to be an urgent message from your bank, mortgage lender, or e-mail provider.

3 Thieves are especially eager to gain access to your web e-mail account. Why? Once a scammer has access to your e-mails, he or she can often figure out where you bank and detect clues to passwords you might use.

So what can you do to protect yourself? Take a moment and think before you click. Never respond to an e-mail asking for your social security number or birth date. You can almost bet that it is a scam. If an e-mail contains a website link that you are not familiar with, do not click on it. Instead, either go directly to the company's trusted website, or contact them by phone.

4 Be alert to scams if you're job hunting. Crooks can find your resume online and, posing as recruiters, e-mail you asking for personal information to do "a background check."

5 E-mail scams become more prevalent following a significant public event, such as a natural disaster or sudden stock market drop. Thieves will prey on your sympathies or fears during these times, so be extra careful when responding to appeals for charity. Also, be leery of e-mails with demanding language or incorrect grammar – both are potential signs of a counterfeit e-mail.

For preventive measures, try to use a different password for every online account, and change your passwords regularly. Make your passwords stronger by using combinations of letters, symbols, and numbers. Also, keep your computer anti-virus software up to date.

6 Providing too many details about yourself on a social networking site can also lead to problems. Giving your birth date, family information, and other facts could enable a scam artist to put together enough information to impersonate you.

7 The IRS is warning taxpayers not to respond to e-mails and phone calls they may receive which claim to come from the IRS or another federal agency. Such contacts are likely to be scams whose purpose is to obtain personal and financial information from taxpayers – information that is then used by the scammers to commit identity theft.

Typically, the scam e-mail or phone call states that the IRS needs certain information to process a tax return or refund. The e-mail contains links or attachments to what appears to be the IRS website or an IRS form. Though they appear genuine, these phonies are designed to get from taxpayers the information scammers need to steal identities. The links can even download malicious software onto the taxpayer's computer if clicked.

8 In an especially aggressive phone scam, the caller claims to be from the IRS and tells the intended victims they owe taxes which must be paid immediately with a pre-paid debit card or wire transfer. Individuals who don't pay up are threatened with arrest or loss of their business or driver's license. Watch for these signs that the call is a scam:

- Use of fake IRS badge numbers.
- Caller knows the last four digits of your social security number.
- Caller ID appears as if IRS is calling.
- Bogus IRS e-mail is sent as follow-up.
- Second call claims to be from police or DMV, again supported by fraudulent caller ID.

9 Scam artists constantly think of creative new ways to steal your personal data. Scams to watch for –

- Bogus tax forms that appear to come from the IRS requesting personal data.
- Fake letters from your bank asking for "account update" information.
- Bogus e-mails from retailers or Internet service providers asking you to update credit and account details.
- Phone calls or e-mails referring to fraud problems on your account and asking you to "confirm" personal data.
- Bogus applications for low interest credit cards asking for your credit and personal details.

10 Identity theft is no longer a novel occurrence, and it's easy to become bored and let down your guard. Take identity theft seriously, or you could become the next victim. Remember, it's not just the potential financial loss that can occur when your identity is stolen; it's the months (and even years) of your life that may be lost to sorting out the problem and regaining your identity. Don't make the mistake of thinking identity theft is mainly an online problem. There are very real offline ways to fall victim to identity theft. In fact, you may be in greater danger from con artists rummaging through your trash or stealing your mail than from online scams.

For assistance in identifying and implementing the fraud prevention strategies best suited to your situation, please contact us.

Small Business Aide
Mary Passino, JD

166 Winthrop Ave. • Revere, MA 02151
(781) 286-8474 • FAX (617) 895-0239
mary@smallbusinessaide.com
www.smallbusinessaide.com