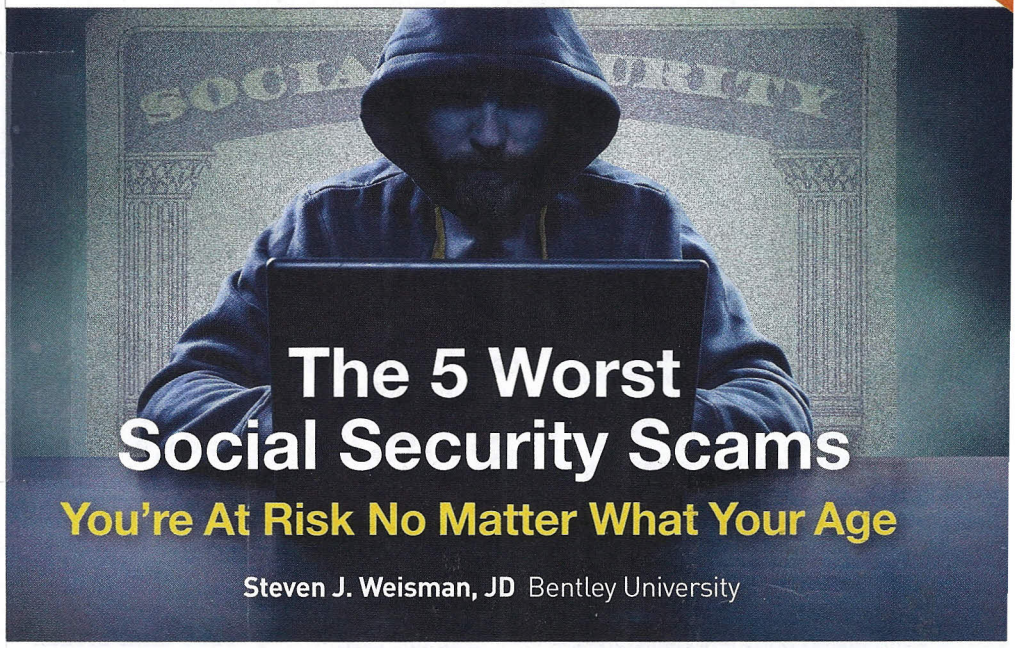
36 YEARS / INSIDE INFORMATION FROM THE WORLD'S BEST EXPERTS

BottomLine PERSONAL

VOLUME 37
NUMBER 8
APRIL 15, 2016 / $5

Surprising causes of back pain
Page 5



The 5 Worst Social Security Scams

You're At Risk No Matter What Your Age

Steven J. Weisman, JD Bentley University

Your Social Security account is a tempting target for scammers whether you are already collecting benefits or will be in the future. Few people understand all the ins and outs of this complex government program, and the bad guys have developed ways to exploit this confusion. Watch out for these five scams…

SCAMS THAT APPLY TO EVERYONE

Online account hijacking. The Social Security Administration is encouraging beneficiaries and future beneficiaries to set up "My Social Security" accounts on its website, SSA.gov. If you set up an account, you can check on the size of future Social Security benefits or make changes to your account, such as altering your mailing address or bank information, without visiting an office or waiting on hold for a phone rep. Unfortunately, this system is proving convenient for scammers, too. They have been setting up accounts in the names of benefit recipients (and people who are eligible to receive benefits but have not yet done so)…and then routing benefits to the scammers' bank accounts or debit cards.

Scammers can do this only if they know a victim's Social Security number, date of birth and other personal information, but thanks to recent data breaches, that information often is easily accessible. If a scammer hijacks your benefits, Social Security will reimburse you, but it could take months to sort this out, during which time you could have financial trouble if you depend >>

Bottom Line Personal interviewed Steven J. Weisman, JD, senior lecturer in the department of law, tax and financial planning at Bentley University in Waltham, Massachusetts. He is founder of the scam-information website Scamicide.com.

>> on your benefits.

What to do: Set up an account at SSA.gov/myaccount before a scammer sets up a bogus account in your name—the sooner, the better. You can set up an account even if you have not yet reached retirement age and/or do not yet wish to start receiving your benefits (accounts may be set up only for people who are at least 18 years old). When you set up your account, click "Yes" under the "Add Extra Security" heading on the online form. That way, a new security code will be texted to your cell phone each time you try to log onto your account. Access to the account will be allowed only if you enter this code, making it extremely unlikely that a hacker would be able to hijack your account.

Fake data-breach scam. There have been so many data breaches in recent years that it would hardly come as a surprise if the Social Security Administration's database were hacked. Scammers use this fear of data breaches to their advantage.

It works like this: The scammer contacts a victim, claims to work for the Social Security Administration and says that its computers have been breached. The scammer says that in order to find out which accounts have been hacked and altered, he/she must check whether he has the correct bank and account number for the beneficiary. He gives account information that he knows does not pertain to the victim. When victims say the account mentioned is not theirs, they are asked to provide the correct bank information and perhaps other information as well. In reality, victims who provide the requested information might have their bank accounts robbed and their benefits and/or identity stolen as well.

What to do: Always ignore calls and e-mail messages about Social Security data breaches—the Social Security Administration never initiates contact with recipients via phone or e-mail. If you receive a letter claiming you must take action because of a data breach, this, too, could be a scam—call the Social Security Administration at 800-772-1213 (not at a number provided in the letter) to ask whether the letter is legitimate. Be extremely wary if someone who contacts you about a Social Security data breach asks you to provide sensitive information, such as bank account details—the real Social Security Administration would never ask for this.

SCAMS THAT APPLY ONLY TO CURRENT BENEFICIARIES

Cost-of-living adjustment scam. Social Security benefits increase in most years to keep pace with inflation. This year was an exception—falling energy prices kept inflation down last year, so there was no 2016 cost-of-living adjustment. To scammers, this exceptional situation represents an opportunity.

Victims receive an e-mail, text, letter or phone call explaining that the Social Security Administration has noticed that they did not apply for their cost-of-living increase this year. Apply soon, these victims are warned, or this benefit boost will be forfeited. An application form might be provided or possibly a link to a website. In reality, victims who supply the requested information will have their identities and/or Social Security benefits stolen.

What to do: Ignore any notices or calls suggesting that you must apply for a Social Security cost-of-living adjustment. These adjustments are made automatically in years when they occur. And never assume that a phone call is legitimate because your phone's caller ID says that it is coming from the Social Security Administration—scammers have ways to fool caller-ID systems.

Social Security card scam. It seems perfectly reasonable that the old paper Social Security cards might be due for an upgrade—after all, the latest credit cards contain computer chips. In fact, Social Security card modernization is a scam.

Scammers contact benefits recipients, claim to work for the Social Security Administration and say that no further benefits can be issued until the beneficiary's old, out-of-date paper card is replaced with a modern, chip-enabled card. These scammers offer to expedite replacement-card requests if the beneficiary provides some identification details. If this information is provided, the victim's benefits and/or identity will be stolen.

What to do: Ignore anyone who says you need a new, high-tech Social Security card. There is no such thing.

Fake-scam scam. Scammers have come up with a way to steal Social Security benefits by exploiting people's fear of being scammed. The scammer contacts victims, claims to work for the Social Security Administration, and says the Administration's scam-spotting software noticed a suspicious change to the victim's account—did the victim recently reroute his benefits to a bank account in a different state? When the victim says no, the helpful Social Security "employee" warns that a scammer must have hijacked the victim's account. The scammer says that he will help the victim fix the problem, but the person must act fast. As part of the process, this fake government employee will request information such as Social Security number and bank account details that will allow him to steal the victim's benefits and/or identity.

What to do: Never provide any information to anyone who contacts you with a warning that you might be the victim of a Social Security benefits scam. Instead, contact the real Social Security Administration at 800-772-1213, describe the warning you received and ask if your account is truly at risk. BLP