Identity THEFT

Keeping You Informed

Prudential Savings Bank
215-755-1500
www.prudentialsavingsbank.com
Member FDIC

Identity Theft NEWSLETTER

Vol. 12, No. 2

Don't become the next victim...

Protect your computer, smartphone and other mobile devices.

- Be suspicious of unprompted popup windows that appear without clicking on a hyperlink.
- Deploy browser security tools and set security settings to disallow popups and certain scripts from running.
- Always log out of online banking and other sensitive online applications and accounts before going to other websites, so that the sessions do not remain active.

A Victim's True Story

Joan T. and her husband just finished applying for their mortgage. They left their bank feeling a real sense of accomplishment.

Three days after the bank appointment, Joan received a call from a man who identified himself, by name, as someone working in the mortgage department of the bank calling to verify all of her information to expedite the application process.

After answering simple questions about her address and phone number, the caller asked Joan for her account number and social security number. Joan became suspicious and told the caller that the bank already has this information.

The "so-called" bank employee stated, quite confidently, that this was part of a verification process to avoid errors that would delay the mortgage approval process.

Joan did not give out the critical information and when she called her bank, she learned there was no such employee or a formal process of verification.

Remember, your bank or credit union will never contact you by phone, text message or email for confidential information concerning your account.

HOW THE IDENTITY SCAM WORKS

Scammers, posing as legitimate businessmen, contact all three major credit reporting agencies and purchase credit information reports. Certain reports list all individuals who are applying for a mortgage and the name of the bank or credit union that is processing the application.

The criminals, then merely work the list to try and get critical information from their unsuspecting victims.

ID THEFT IS GROWING

Up From Last Year
15.9 million
Households in which someone experienced ID theft in the past 12 months.

Up From Last Year
7.4 million
Households that had charges placed on an existing credit card by an unauthorized person in the past 12 months.

Up From Last Year
9.1 million
Households in which someone submitted personal information to a phishing e-mail scam in the past 12 months.

(Source: eMarketer)

Fast Fact

Secure Your Devices

Make sure your smart phone, iPad, other mobile devices, and portable flash drives containing personal data have security applications and encryption in case they're lost or stolen.

Beware of the Latest Scam

Are you protecting your most valuable personal property - your banking information?

The Federal Bureau of Investigation warns account holders of a new spam email scheme that involves a type of malware called "Gameover." The scheme involves fake emails from the National Automated Clearing House Association, the Federal Reserve or a financial regulatory agency. After tricking recipients into clicking on a link to resolve some type of issue with their accounts or a recent ACH transaction, the Gameover takes over your computer, and thieves can steal usernames, passwords and your money.

The FBI also warns that thieves' hacking capabilities can navigate around common user authentication methods financial institutions use to verify your identity. What is traditionally thought of as extra security, often personal questions, birth dates or other pieces of private information, are easily exposed and dangerous in the wrong hands. With the advent of mobile banking, we're reminded that a phone is virtually another computer that has a greater exposure to the internet, thus allowing for greater exposure to having your information compromised.

Here are a few crucial steps to take to avoid falling victim to this type of Internet crime.

- Keep your computer and mobile device updated with the newest versions of ant-virus software.
- If you have any doubts about an email sender's authenticity, do not click on any embedded links.
- Remember, banks or credit unions never request any personal information via email.
- Be vigilant about checking your account balances. The sooner you notice and report any type of fraudulent activity, the more likely you'll be able to be reimbursed for any missing funds.

Fast Fact

Beware of Text Message Identity Rip-off

A scammer offers a free $1,000 Walmart gift card through a link in a text message. When you click it, a website comes up requesting personal information that can be used to steal your identity.

What To Do If You Are A Victim

1. Contact your credit card company and your financial institution and close your accounts. The FBI suggests that you put passwords (not your mother's maiden name) on any new accounts you open.
2. Contact the fraud departments of each of the three major credit bureaus.
   - **Equifax** 1-800-525-6285
   - **Experian** 1-888-397-3742
   - **TransUnion** 1-800-680-7289

Tell them that you're an identity theft victim. Request that a "fraud alert" be placed in your file, as well as a "victim's statement" asking that the creditors call you before opening any new accounts or changing your existing accounts. This can help prevent an identity thief from opening additional accounts in your name.

3. Call the Social Security Fraud Hotline: 800-269-0271.
4. Contact the Federal Trade Commission (FTC) theft hotline: 877-438-4338 / www.ftc.gov/idtheft
5. You should not only file a report with the police, but also get a copy of the report in case you need proof of the crime later for credit card companies, etc.

Fast Fact

One way criminals steal your name is by taking preapproved credit offers from your mailbox to open an account. They can then watch your mailbox to lift the new card you didn't know was coming. You can stop credit bureaus from selling your name to lenders by going to www.optoutprescreen.com or calling 888-567-8688. Opting out should stop most offers, and it's free.

ID THEFT Q&A

Q: What Is Phishing?

A: Here's How Phishing Works

In a typical case, you will receive an e-mail that appears to come from a reputable company that you recognize and do business with, such as your financial institution. In some cases, the e-mail may appear to come from a government agency, including one of the federal financial institution regulatory agencies.

The e-mail will probably warn you of a serious problem that requires your immediate attention. It may use phrases, such as *"Immediate attention required"* or *"Please contact us immediately about your account."* The e-mail will then encourage you to click on a button to go to the institution's website.

In a phishing scam, you could be redirected to a phony website that may look exactly like the real thing. Sometimes, in fact, it may be the company's actual website. In those cases, a pop-up window will quickly apear for the purpose of harvesting your financial information.