NEWSLETTER Vol. 2 No.1

Identity THEFT

UCB United Community Bank

DEDICATED TO YOUR FINANCIAL SUCCESS
Milford • Okoboji • Hartley • Ocheyedan • Lake Park
www.unitedcommunitybank.com
Member FDIC

Fast Fact

Facebook apps can pose privacy risks.

One way your data can escape is through Facebook games and apps. Whenever you run one, it gets your public information, such as your name, gender, and profile photo, as well as your lists of friends even if you haven't made that list public. Unless you have chosen your privacy settings meticulously, a friend who runs an app could grant it access to your information without your knowledge.

TIPS to protect yourself on facebook.

1. **Protect basic information.**
   Set the audience for profile items, such as your town or employer. And remember: Sharing info with "friends of friends"could expose it to tens of thousands.
2. **Regularly check your exposure.**
   Each month, check out how your page looks to others. Review individual privacy settings if necessary.
3. **Think before you type.**
   Even if you delete an account (which takes Facebook about a month), some info can remain in Facebook's computers for up to 90 days.
4. **Know what you can't protect.**
   Your name and profile picture are public. To protect your identity, don't use a headshot photo since they can be used to create fake photo IDs. The best option is to use a photo that doesn't show your face.
5. **Block apps and sites that snoop.**
   Unless you intercede, friends can share.
6. **"Unpublic" your wall.**
   Set the audience for all previous wall posts to just friends.

Fast Fact

If you are monitoring medical statements from your insurer for benefits paid under your name but not received, remember, you have the right under federal law to receive a copy of your medical records from your health-care provider, though you will likely be charged a small fee. By law, the health-care provider has up to thirty days to respond to your request.

ID THEFT is growing.

Up From Last Year

Households in which someone experienced ID theft in the past 12 months.

15.9 million

Up From Last Year

Households that had charges placed on an existing credit card by an unauthorized person in the past 12 months.

7.4 million

Up From Last Year

Households in which someone submitted personal information to a phishing e-mail scam in the past 12 months.

9.1 million

Social Security Administration

IDENTITY THEFT AND YOUR SOCIAL SECURITY NUMBER

What if an identity thief is creating credit problems for you?

If someone has misused your Social Security number or other personal information to create credit or other problems for you, Social Security cannot resolve these problems. But there are several things you should do.

You should contact the Federal Trade Commission (FTC) at **www.ftc.gov/bcp/edu/microsites/idtheft.** Or, you can call **1-877-438-4338.**

Also, you should file an online complaint with the Internet Crime Complaint Center (IC3) at **www.ic3.gov.**

The IC3 gives victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. IC3 sends every complaint to one or more law enforcement or regulatory agencies that have jurisdiction over the matter.

IC3's mission is to receive, develop and refer criminal complaints regarding the rapidly expanding arena of cyber crime. For law enforcement and regulatory agencies at the federal, state, local and international level, IC3 provides a central referral mechanism for complaints involving Internet related crimes.

The IC3 reflects a partnership between the Federal Bureau of Investigation, the National White Collar Crime Center and the Bureau of Justice Assistance.

You also may want to contact the Internal Revenue Service. An identity thief might also use your Social Security number to file a tax return in order to receive a refund. If the thief files the tax return before you do, the IRS will believe you already filed and received your refund if eligible. If your Social Security number is stolen, another individual may use it to get a job. That person's employer would report income earned to the IRS using your Social Security number, making it appear that you did not report all of your income on your tax return. If you think you may have tax issues because someone has stolen your identity, contact the IRS Identity Protection Unit at **1-800-908-4490.**

GUARD AGAINST ID Theft

- Never provide personal financial information, including your Social Security number, account numbers or passwords, over the phone or the Internet if you did not initiate the contact.
- Remove mail promptly from your mailbox. Never use your mailbox for outgoing mail. Identity thieves raid mailboxes for credit card offers and financial statements.
- Do not be intimidated by an e-mail or caller who suggests dire consequences if you do not immediately provide or verify financial information.
- Limit the number of I.D. and credit cards that you carry. If they are stolen, you'll have fewer to replace.
- Never click on the link provided in an e-mail you believe is fraudulent. It may contain a virus that can contaminate your computer.
- If you believe the contact is legitimate, go to the company's website by typing in the site address directly or using a page you have previously bookmarked, instead of a link provided in the e-mail.
- If your Social Security number is used as your driver's license number or appears on another I.D. card, ask the issuer for a new card with a different account number. If your Social Security number is printed on your checks, reorder checks without it. Also, if your driver's license number is printed on your checks, consider removing it.
- Shred all important documents before putting them in the trash.

Experts say guard against identity theft by checking your credit once a year!

How to get your FREE credit report

ONLINE AT
www.AnnualCreditReport.com

TOLL FREE AT
877.322.8228

WHEN IT COMES TO PHISHING Timing Is Everything

Phishing attacks are "spoofed" emails and fraudulent websites designed to fool recipients into divulging personal financial data. Trusteer Associates, a research firm, studied the time-to-infection of e-mail phishing attacks. They found 50% of phishing victims' credentials are harvested by cyber criminals within the first 60 minutes of phishing e-mails being received.

Given that a typical phishing campaign takes at least one hour to be identified by IT security vendors, which does not include the time required to take down the phishing website, Trusteer has dubbed the first 60 minutes of a phishing site's existence the "Golden Hour." The company said the fact that so many Internet users visit a phishing website within such a short period of time means that blocking the site – which sometimes is a cracked legitimate site – within this golden hour has become "absolutely critical."

During the "Golden Hour," Trusteer's research shows:

- **more than 50% of stolen credentials are harvested.**
- **within five hours, more than 80% are collated and become usable by cybercriminals.**
- **the first 10 hours produce more than 90% of the total credentials that will be stolen by any given phishing site.**

IT security companies and industry experts working with key government agencies are trying to establish really quick feeds into browsers and other security tools, so that phishing filters can be updated much more quickly than they are today.