

# THE KEY

MARCH 2010



## UNLOCKING YOUR FINANCIAL OPPORTUNITIES



**Farmers**  
**STATE BANK**

Cedar Falls • Waterloo • Jesup  
Raymond • Dunkerton • Gilbertville

MEMBER FDIC

## THE IDENTITY THEFT EDITION

### IN THIS ISSUE:

PICTURE PERFECT SECURITY,  
PHISHING SCAMS, &  
ONLINE BANKING SECURITY

### CD RATES:

9-13 Mo. - 1.75%<sup>APY\*</sup>

15-17 Mo. - 2.00%<sup>APY\*</sup>

25-30 Mo. - 2.27%<sup>APY\*</sup>

60-67 Mo. - 3.27%<sup>APY\*</sup>

### IRA CD RATES:

26-32 Mo. - 3.00%<sup>APY\*</sup>

\*APY = Annual Percentage Yield. IRA = Individual Retirement Account. Qualified funds only. Substantial penalty for early withdrawal, \$1,000 minimum opening deposit for 15-17 month, 25-30 month, 26-32 month and 60-67 month terms. \$2,000 minimum opening deposit for 9-13 month term. 9-13 month CD interest rate 1.74%, 15-17 month CD interest rate 1.99%, 25-30 month CD interest rate 2.26%, 26-32 month IRA interest rate 2.98%, 60-67 month CD interest rate 3.24%. Interest compounds semi-annually for 15-17 month, 26-32 months & 60-67 month CD's and every 3 months for 9-13 month CD. Effective 2/10/2010.

### SIMPLE STEPS TO SAFEGUARD YOUR IDENTITY

Up to 500,000 individuals each year are victims of identity theft, a fast-growing form of fraud.

“Identity theft” or “account takeover fraud” involves criminals stealing a person’s personal information. The crooks assume a person’s identity, apply for credit in his or her name, run up huge bills, stiff creditors and generally wreck the victim’s credit record.

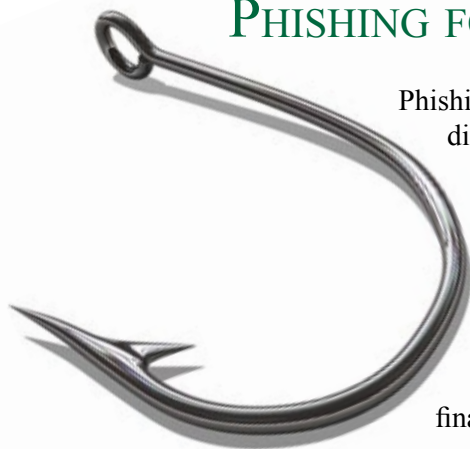
At Farmers State Bank, we put a combination of safeguards in place to protect customers, including: employee training, rigorous security standards, data encryption and fraud detection.

Fortunately, a few simple steps can help you avoid becoming a victim:

- Don't give your Social Security or account numbers to anyone over the phone unless you initiated the call.
- Review your bank and credit card statements as soon as you receive them to check for unauthorized transactions.

- Shred receipts, old bank statements and unused credit card offers before throwing them away. Criminals could steal information from your trash and use it to get credit in your name.
- Protect your Personal Identification Number (PIN) and computer passwords; use a combination of both letters and numbers and change them often. Never carry this information with you!
- Order copies of your credit report once a year to ensure accuracy. Visit [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) to download your free credit report once a year from Equifax, Experian and Trans Union.
- Report any suspected fraud to your bank and credit card issuers immediately so they can start to close accounts and clear your name right away.

# PHISHING FOR YOUR PERSONAL INFORMATION



Phishing attacks use ‘spoofed’ e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, Social Security numbers, etc. By hi-jacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince recipients to respond to them.

Restoring your identity can be a tremendous inconvenience. It’s worth your while to exercise a little preventive maintenance. Protect yourself against this terrible crime. If you ever have concerns, please call the bank for more information, and for more personal finance tips, visit our web site at [www.FSB1879.com](http://www.FSB1879.com).

## CONSUMER TIPS:

Never give out your personal financial information in response to an unsolicited phone call, fax, or email, no matter how official it may seem.

**Tip #1** - Do not respond to emails that may warn of dire consequences if you do not validate your information immediately. Contact the company to confirm the e-mail’s validity using a telephone number or web address you know to be genuine. Check your credit card and bank account statements regularly and look for unauthorized transactions, even small ones. Some thieves hope small transactions will go unnoticed. Report discrepancies immediately.

**Tip #2** - When submitting financial information or making purchases on a website, look for the padlock or key icon at the top or bottom of your browser, and make sure the Internet address begins with “https”. This signals that your information is secure during transmission.

**Tip #3** - Report suspicious activity to the Internet Crime Complaint Center at [www.ic3.gov](http://www.ic3.gov), a partnership between the FBI and the National White Collar Crime Center.

**Tip #4** - If you have responded to an email that you believe is fraudulent, contact the bank immediately so they can protect your account and your identity.

.....

## STEPS TO TAKE IF YOU ARE A VICTIM

If you suspect misuse of your personal information to commit fraud, take action immediately. Keep a record of all conversations and correspondence when you take the following suggested steps:

**Step #1** - Contact your bank(s) & credit card issuers immediately so access to your accounts can be protected.

**Step #2** - File a police report with your local police department.

**Step #3** - Contact the three major credit bureaus and request a copy of your credit report. The major credit bureaus and their phone numbers are: Trans Union (800) 680-7289, Experian (888) 397-3742 and Equifax (800) 525-6285.

**Step #4** - Be aware of when monthly statements and bills are received in the mail. Missing mail can indicate that someone has requested an unauthorized address change.

**Step #5** - Maintain a written chronology of what happened, what was lost and the steps you took to report the incident to the various agencies, banks, and firms impacted.



## PICTURE PERFECT SECURITY

Gain additional fraud protection with our [FREE Photo Check Card](#). It features your picture on the front to offer you a new level of protection against fraud and theft. Using your Photo Check Card avoids the inconvenience of writing checks. It is accepted at any merchant that displays the VISA, Shazam, or Cirrus logo. Most PIN-based merchants will allow you to take up to \$100.00 in cash on top of your purchase without generating any charge or fee to you. To find a listing of all non-FSB, surcharge free, ATM's visit [www.shazam.net/privileged.htm](http://www.shazam.net/privileged.htm) and look for this logo on any ATM machines.



## STRENGTHENING ONLINE BANKING SECURITY

It is our commitment to you that access to your financial information is secure. We have taken enhanced measures to secure our Online Banking site with Multi-Factor Authentication. This requires you to complete a one-time security update that activates your account. It is intended to provide you with the best security possible. Multi-Factor Authentication consists of validation and authentication of a customer using more than one method of verification. Generally, this is accomplished by verifying three things:

**Item #1** - You will need to create three question and answer pairs. This allows us to verify that you are in fact, you, by presenting a question that only YOU know the answer. If you don't answer the question correctly, you will not gain access to your accounts.

**Item #2** - You will also need to create a "Security Key". This allows you to verify that you have reached our Online Banking site, and not some other fictitious site. Every time you log into your accounts, you will see a graphical representation of your Security Key on every page. If you do not see that Security Key, or it is not the one you created, then you know that you are NOT at OUR site. If this happens, please contact us immediately at 1-877-FSB-1879.

**Item #3** - This is one that you already know - your password.

## WHY ALL THIS ATTENTION TO SECURITY?

Every bank was required to use Multi-Factor Authentication by December 31, 2006. Federal agencies, including the Office of the Comptroller of the Currency (OCC), have mandated that all providers of Internet Banking services increase log-in security from Single-Factor Authentication (such as a password) to Multi-Factor Authentication. Therefore, all are required to implement this level of security.

## TECH TIPS


- PROTECT YOUR PINs AND COMPUTER PASSWORDS; USE A COMBINATION OF LETTERS, NUMBERS AND SYMBOLS AND CHANGE THEM OFTEN
- WHEN CONDUCTING BUSINESS ONLINE, MAKE SURE YOUR BROWSER'S PADLOCK OR KEY ICON IS ACTIVE
- DON'T OPEN E-MAIL FROM UNKNOWN SOURCES
- BACKUP YOUR IMPORTANT FILES TO AN EXTERNAL HARD-DRIVE OR BURN TO DVD'S
- USE VIRUS DETECTION SOFTWARE




## CLICK




Apply for an Auto Loan



Apply for a Mortgage Loan



Apply for an Account

AT

[www.FSB1879.com](http://www.FSB1879.com)

### BRANCH & ATM LOCATIONS:

- |  |   |
|--|---|
| <b><u>Cedar Falls</u></b><br>1710 1 <sup>st</sup> St Ste A<br>(319) 268-1879 | <b><u>Waterloo</u></b><br>1009 Peoples Sq<br>(319) 287-3961             |
| <b><u>Jesup</u></b><br>1310 6 <sup>th</sup> St<br>(319) 827-1050             | <b><u>Raymond</u></b><br>300 South 3 <sup>rd</sup> St<br>(319) 232-3070 |
| <b><u>Dunkerton</u></b><br>905 Jon Rd<br>(319) 822-2521                      | <b><u>Gilbertville</u></b><br>1222 5 <sup>th</sup> St<br>(319) 296-1410 |

### OTHER ATM LOCATIONS:

- Cedar Falls**  
**Prime Mart** - 2827 Center St  
**Tobacco & Liquor** - 2328 College St  
**Prime Mart** - 2323 Main St
- Waterloo**  
**Supervisors Club** - 3265 DeWitt Rd  
**Omega Cabinets** - 1205 Peters Dr  
**Court House** - 316 E 5<sup>th</sup>  
**Prime Mart** - 1008 LaPorte Rd  
**Prime Mart** - 3535 Marigold Dr
- Gilbertville**  
**Mini Mart** - 115 25th Ave
- Independence**  
**Starlight Cinema** - 2401 Swan Lake Blvd

## FIND YOUR KEYS

U O R E I S E T R N S I S I  
 N I A Y N M E A O T N O D K  
 N O I T A C I T N E H T U A  
 S Y I I E T A N L G T N A D  
 H H L T S I O C I N P E R A  
 E A R N C A R D N I P O F P  
 H T E E O E A D E H W Y T I  
 R D R D D O T I T S T T L H  
 D E B I T O I O S I E C E T  
 N F T C O I D A R H R E Y L  
 N U G H O F P U O P P Y D O  
 U C I T S D C H T R C I P G  
 H F W H K E Y I T E K O C L  
 H N R A S K O O R C O I D D

### KEY WORDS

- AUTHENTICATION
- CARD
- CREDIT
- CROOKS
- DEBIT
- EMAIL
- FRAUD
- IDENTITY
- KEY
- ONLINE
- PASSWORD
- PHISHING
- PIN
- PROTECTION
- SECURITY
- SHRED

### **\$250,000 FDIC DEPOSIT INSURANCE COVERAGE THROUGH 2013**

To help reassure depositors about the safety of their money during the economic crisis, Congress temporarily increased the basic limit on federal insurance coverage from \$100,000 to \$250,000 per depositor through December 31, 2009.

That temporary increase in deposit insurance has been extended by law through December 31, 2013.

This means that if you have a total of \$250,000 or less in all of your deposit accounts at the same insured bank, you don't need to worry about your insurance coverage – your deposits are fully insured through at least 2013. And as always, you may qualify for more than the basic insurance coverage at one insured bank because the FDIC provides separate insurance coverage for deposits held in different “ownership categories,” such as single accounts and joint accounts. Under current law, certain retirement accounts, including IRA deposits, will continue being protected up to \$250,000 even after 2013 because that is the permanent coverage limit previously set by Congress for these accounts in 2006.

For more information and to calculate your FDIC insurance coverage, start at [www.myfdicinsurance.gov](http://www.myfdicinsurance.gov) or call toll-free 1-877-ASK-FDIC (1-877-275-3342).

