

# ***SOUTHEAST AREA EXTENSION SAYS***

By: Kaye Kasza, CSU Extension Agent

Contact: [Kaye.kasza@colostate.edu](mailto:Kaye.kasza@colostate.edu) or 719-456-0764

FOR IMMEDIATE RELEASE – March 26, 2010

## **Online Banking: Ways to Protect Your Money**

SOUTHEAST AREA---Online banking, bill paying and shopping are convenient, and most of the time completed quickly and without a glitch. However, just as with other transactions, in a small percentage of cases something goes wrong. That's why you need to take precautions against theft and errors.

In particular, even as banks and merchants tighten up security, Internet thieves devise new, sophisticated ways to trick consumers into sending money or into revealing information that can be used to commit fraud. "Today's Internet threats wear many different disguises, from fake Web sites to fraudulent text messages on cell phones," warned Michael Benardo, Chief of the FDIC's Cyber-Fraud and Financial Crimes Section. "That's why online consumers need to be aware that they may be targeted and they should always be on guard."

David Nelson, an FDIC fraud specialist, added: "Online fraud is an ongoing game of cat and mouse. Crooks continuously hunt for security holes, banks and merchants plug those holes, and then the criminals find new ones to slink through." Steps you can take to protect your identity and possessions follow.

1. If you bank online, frequently check your deposit accounts and lines of credit to spot and report errors or fraudulent transactions, just as you should with traditional banking. The sooner you detect a problem with a transaction, the easier it should be to fix.

Check your accounts online once or twice a week. Many banks are making it easier for their customers to keep an eye on their accounts electronically. For example, many banks offer e-mail or text message alerts when your balance falls below a certain level or when there is a transaction over a certain amount. Federal laws generally limit your liability for unauthorized electronic funds transfers, especially if you report the problem to your financial institution within specified time periods, which will vary depending on the circumstances. A good rule of thumb is to check your statements promptly and report unauthorized transactions to your bank as soon as possible.



**Southeast Area  
Extension**

### **County Extension Offices**

#### **Baca County**

772 Colorado St.  
Springfield, CO 81073  
719-523-6971

#### **Bent County**

1499 Amb. Thompson Blvd.  
Las Animas, CO 81054  
719-456-0764

#### **Cheyenne County**

425 S. 7<sup>th</sup> W.  
P. O. Box 395  
Cheyenne Wells, CO 80810  
719-767-5716

#### **Crowley County**

603 North Main St.  
Courthouse Annex  
Ordway, CO 81063  
719-267-4444, ext. 7

#### **Kiowa County**

1305 Goff  
P. O. Box 97  
Eads, CO 81036  
719-438-5321

#### **Otero County**

411 N. 10<sup>th</sup>  
P. O. Box 190  
Rocky Ford, CO 81067  
7190-254-7608

#### **Prowers County**

1001 S. Main  
Lamar, CO 81052  
719-336-7734

2. Never give your Social Security number, credit or debit card numbers, personal identification numbers (PINs) or any other confidential information in response to an unsolicited e-mail, text message or phone call, no matter who the source supposedly is. An "urgent" e-mail or phone call or text appearing to be from a government agency (such as the IRS or the FDIC), a bank, merchant or other well-known organization may be a scam attempting to trick you into divulging personal and account information. It's called "phishing," a high-tech variation of the concept of "fishing" for personal information.

3. Don't open attachments or click on links in unsolicited e-mails from anyone you don't know or aren't sure about. Sometimes these attachments or links can infect your computer with "spyware" that can change your security settings and record your keystrokes. Or, the spyware may secretly steal your passwords, bank or credit card numbers, and your answers to security questions like your mother's maiden name or your high school. This information can be used to log into your account, make changes and transfer money, leaving your bank account empty.

4. Use a mix of security tools and procedures. At the top of the list of security tools to use — and keep updated — are anti-virus software to detect and block spyware and other malicious attacks, and a "firewall" to stop hackers from accessing your computer.

Even if your computer seems fine, schedule an automatic anti-virus scan to run at least once a week but preferably every day. Call or e-mail your anti-virus vendor right away if you get a warning message and you don't know what to do next.

CSU Extension offers up-to-date, unbiased, research-based information to families in Southeast Colorado. For more information, contact your local office: Baca County 719-523-6971, Bent County 719-456-0764, Cheyenne County 719-767-5716, Crowley County 719-267-5243, Kiowa County 719-438-5321, Otero County 719-254-7608, Prowers County 719-336-7734. Or find us on the web at: <http://www.extension.colostate.edu/SEA>. CSU Extension programs are available to all without discrimination.

###