Sisseton-Wahpeton
Federal Credit Union

45665 Veterans Memorial Drive * PO Box 627
Agency Village, SD 57262
Phone: (605) 698-3462
Fax: (605)698-3907
www.sisseton-wahpetonfcu.com

AUGUST 2016

Membership: Sisseton Wahpeton Federal Credit Union is a credit union providing services to those members and employees of the Sisseton-Wahpeton Sioux tribe, employees of area schools, Indian Health Service and bureau of Indian Affairs, Members of organizations of the above.

Credit Union Services:

E-Services
- It's Me 247
- CU*Talk

Loans
- Vehicle
- Secured
- Share Secured
- Unsecured

Insurance
- Credit Life
- Loan Protection

Savings
- Certificate of Deposit
- Direct Deposit
- Payroll Deductions
- Regular Shares
- Christmas Club Accts

Other:
- Coin Counting
- Copying Service
- Faxing Service
- Postage Stamps
- Wire Transfers
- Money Orders
- Student Scholarships
- NADA New/Used Guides

Your savings federally insured to at least $250,000 and backed by the full faith and credit of the United States Government
NCUA
National Credit Union Administration, a U.S. Government Agency

Federally Insured by NCUA

Sisseton-Wahpeton FCU will be **CLOSED** for the following Holidays:

Monday, September 5th: Labor Day

Monday, October 10: Native American Day

2016 SWFCU Board of Directors Election Results

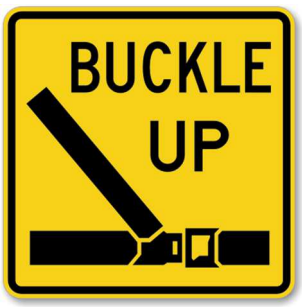
Patrick Deutsch, Jr - President
Geri Opsal - Vice-Chairwoman
Christine Fineday - Secretary
Derrick Redday - Treasurer
Angie Johnson - Member (to serve out Tamara St John's term)

****REMINDER NOTICE TO ALL MEMBERS***

- Update your mailing address, email address and phone number.
- All members are required to update their application and income verification, if their status has changed.
- Sisseton-Wahpeton FCU is currently reviewing old loans.

AUTO LOANS

Fasten your seatbelts! With rates as low as 4.000% apr, Sisseton-Wahpeton FCU will help you shift into gears and cruise on to the vehicle of your dreams. See Sisseton-Wahpeton FCU for details and qualifications. Some restrictions may apply.



Frauds and Scams

Be on alert. Stay Informed. Protect Yourself.

You receive a text message or an automated phone call on your cell phone saying there's a problem with your bank account. You're given a phone number to call or a website to log into and asked to provide personal identifiable information—like a bank account number, PIN, or credit card number—to fix the problem.

But beware: It could be a **"smishing" "vishing "**scam…and criminals on the other end of the phone or website could be attempting to collect your personal information in order to help themselves to your money. While most cyber scams target your computer, smishing and vishing scams target your mobile phone, and they're becoming a growing threat as a growing number of Americans own mobile phones. (Vishing scams also target land-line phones.)

"Smishing"—a combination of SMS texting and phishing—and "Vishing"—voice and phishing—are two of the scams the FBI's Internet Crime Complaint Center (IC3) is warning consumers about as we head into the holiday shopping season. These scams are also a reminder that cyber crimes aren't just for computers anymore.

Here's how smishing and vishing scams work: criminals set up an automated dialing system to text or call people in a particular region or area code (or sometimes they use stolen customer phone numbers from banks or credit unions). The victims receive messages like: "There's a problem with your account," or "Your ATM card needs to be reactivated," and are directed to a phone number or website asking for personal information. Armed with that information, criminals can steal from victims' bank accounts, charge purchases on their charge cards, create a phony ATM card, etc.

Sometimes, if a victim logs onto one of the phony websites with a smartphone, they could also end up downloading malicious software that could give criminals access to anything on the phone. With the growth of mobile banking and the ability to conduct financial transactions online, smishing and vishing attacks may become even more attractive and lucrative for cyber criminals.

Here are a couple of "smishing" examples:

- Account holders at one particular credit union, after receiving a text about an account problem, called the phone number in the text, gave out their personal information, and had money withdrawn from their bank accounts within 10 minutes of their calls.
- Customers at a bank received a text saying they needed to reactivate their ATM card. Some called the phone number in the text and were prompted to provide their ATM card number, PIN, and expiration date. Thousands of fraudulent withdrawals followed.

Other holiday cyber scams to watch out for include:

- Phishing schemes using e-mails that direct victims to spoofed merchant websites misleading them into providing personal information.
- Online auction and classified ad fraud, where Internet criminals post products they don't have but charge the consumer's credit card anyway and pocket the money.
- Delivery fraud, where online criminals posing as legitimate delivery services offer reduced or free shipping labels for a fee. When the customer tries to ship a package using a phony label, the legitimate delivery service flags it and requests payment from the customer.

theINbox…
good things to know

Tips to Protect Yourself From Cyber Scams:

- Don't respond to text messages or automated voice messages from unknown or blocked numbers on your mobile phone.
- Treat your mobile phone like you would your computer…don't download anything unless you trust the source.
- When buying online, use a legitimate payment service and always use a credit card because charges can be disputed if you don't receive what you ordered or find unauthorized charges on your card.
- Check each seller's rating and feedback along with the dates the feedback was posted. Be wary of a seller with a 100 percent positive feedback score, with a low number of feedback postings, or with all feedback posted around the same date.
- Don't respond to unsolicited e-mails (or texts or phone calls, for that matter) requesting personal information, and never click on links or attachments contained within unsolicited e-mails. If you want to go to a merchant's website, type their URL directly into your browser's address bar.