



301 East North Street • Rapid City, SD 57701

"Guardians of your financial services"

Inside this Issue

Annual Meeting	1
Direct Deposit for Tax Refunds	1
Buying a Car	1
Closure Dates	1
Traveling?	1
Scam Alert	2
Phishing	2



Direct Deposit of Your Income Tax Refund

Direct deposit is the easiest, fastest way to get your refund. **Combine e-file with direct deposit to:**

- ★ Receive your refund faster
- ★ Avoid waiting lines
- ★ Get peace of mind—no lost or undeliverable checks.

Set Up Direct Deposit

- ◆ Enter your credit union nine-digit routing number on the return you're filing. You can find your checking account routing number on your checks or you may call us for assistance.
- ◆ Enter your account number on the return you're filing (up to 17

characters). Don't include your check number.

Tips

- You will receive an email notifying you when the IRS issues your refund if you create an Online Services account and sign up to receive email notifications.
- If you're signed up for email notifications and requested a direct deposit that can't be deposited in your account, they will send you an email when the paper check has been issued.



ANNUAL MEETING

A heartfelt thank you to all who attended our annual meeting in January. We enjoyed visiting with each one of you! Your current board members remain the same:

- Chair—Todd Bartunek
- Vice Chair—David Oerlline
- Treasurer—Debra Bartunek
- Secretary—Jim Stevenson
- Members—Jim Morrison, Gregg Brower and Kevin Speirs

We look forward to our next meeting on:

January 17, 2020

Buying a Car?

An automobile is a major investment. Just think about it—in the last ten years, have you bought anything that costs more than a car? A house or your kid's education, maybe. Yet, unlike a house, a car is not going to appreciate in value; and unlike an education, an SUV is not going to increase your offspring's earning potential.

A car is not an investment after all, because you are not going to receive a return on it. It is an expense, and the best you can do is to get the maximum use and pleasure from the money you spend. Getting the most out of your car is a matter of careful maintenance. Getting the most out of your money is a matter of getting a good price on the car and a good deal on the related financing.

Negotiating a good price on your car can be stressful, but arranging for a good deal on your loan might not have to be. When they think of car loans, most people think of banks

and dealer financing—but your credit union may offer the best, most flexible terms and the fastest loan process that's available to you:

- Before you go shopping, come to your credit union to get pre-approved for a loan. Pre-approval will mean you have one less thing to worry about when you find the vehicle you want.
- The rates that your credit union offers on auto loans are probably lower than those that are offered by most banks and car dealerships in your area.
- Refinancing an existing loan on the car you currently drive could lower your rate and monthly payment, putting more money in your pocket—a good thing at any time, but especially in a troubled economy.

Whether you buy a new or used car or refinance an existing car loan, come see us at the credit union!



ROAD TRIP!

Traveling out-of-state?

Call to let us know your travel itinerary and we'll put an alert on your account and debit card.



2019 IMPORTANT CLOSURE DATES TO REMEMBER

- May 27 Memorial Day
- July 4 Independence Day



SCAM ALERT!

A warning from the Better Business Bureau; don't click the link. Scammers are flooding email boxes with phony emails appearing to be from Amazon.com. Clicking the link may infect your computer with a virus and you could be putting your private information in the hands of crooks.

If you've noticed strange emails from Amazon.com, don't click any links or attachments. It's not just the average consumers getting the phony emails, they have even made it into the inboxes of employees at NBC12.

The Better Business Bureau warns it's a trick to get your personal information. Crooks have put some effort into making the emails look like legitimate Amazon emails. They come with a shipping confirmation number, an itemized rundown of the fake purchase and even an estimated

delivery date. The BBB says the emails have gone nationwide. The organization is spreading the word, hoping to catch consumers before they are fooled.

On the real Amazon website, there's a warning about these type of emails and what you should look out for. The company even provides a place to report fraudulent emails. It reminds consumers, legitimate Amazon emails will never ask for personal information, like a social security number, credit card number or your Amazon password. Grammatical errors should also raise red flags. You should also know that Amazon emails will never ask you to verify account information by clicking a link.

If you get one of these emails, the best thing to do is delete it. If you've done business with Amazon and are concerned about an email, contact the company directly or go to its website. The BBB is not sure who is behind the emails. Amazon says it takes these phishing scams seriously and says it is determined to crackdown on those responsible.

Tips to Avoid Being Phished



There are so many different types of phishing scams out there, you might not realize they all have one basic thing in common: In order for any phishing scam to work, it has to get you to do something.

- ▲ **Keep informed about phishing methods.** Cyber criminals are constantly developing new phishing scams; keep yourself informed of the latest scams.
- ▲ **Use Firewalls, antivirus software and anti-phishing toolbars.** Firewalls act as a buffer between you, your computer and outside intruders against vicious files. Antivirus software can guard against known technology loopholes. The most prevalent internet browsers can be customized with anti-phishing toolbars that can run quick checks on websites to warn you of potentially malicious websites.
- ▲ **Keep your security software and browsers up to date.** In the event that you are unable to recognize a phishing scam and actually click on a link or attachment which leads to malware, your updated browser or security software will stop many criminals from gaining access to your personal information.
- ▲ **Check your online accounts regularly.** Check your online accounts and statements regularly to look for suspicious activity and change your passwords on a regular basis.
- ▲ **Think BEFORE you click on popups and email links.** With hundreds of millions of personal data records compromised through data breaches since 2005, you cannot always guarantee that popups or an email from someone you know is legitimate.
- ▲ **Friends may innocently send infected links or files to download.** Be wary of a scammer impersonating one of

your friends or family. Even if a friend sent the email, there is a chance that it may be infected. If your browser or security software warns you that a link or download is malicious, do not click or download the content.

- ▲ **Just because an email looks good does not mean it is legitimate.** Beware of emails that are badly formatted or contained misspellings—especially from well-known companies. But, keep in mind that just because an email “looks right” doesn't mean it is right. Smart phishing scams can look virtually identical to legitimate messages.
- ▲ **While some emails addresses are obviously from a phony company, it is easy for sophisticated scammers to make an email address resemble a legitimate business.** Use caution and assume the email could be a phishing email—even if the sender looks legitimate.
- ▲ **Like email addresses, creating convincing URLs is easy for sophisticated scammers.** Hovering over (long-pressing on mobile) links in email can identify obvious fakes, but many phony URLs are made to be convincing. When in doubt, use a search engine to find the actual URL yourself.
- ▲ **Your safest choice is to always stay in the driver's seat by finding content yourself.** If you click a link, you are allowing that link or popup to pull you to wherever it wants to take you—whether it is safe or not. The extra 10 seconds it takes to search for a site yourself can save you from dealing with a difficult-to-remove virus, protect your information, and even prevent ID theft.

The secret to protecting yourself from fraud is simple: Stop and think before you respond to any request for anything. Trusted parties will NEVER ask you for sensitive information in an email. There is no single fool-proof way to avoid phishing attacks. An ounce of precaution is worth a pound of cure.

Mailing Address, Hours of Operation and Contact Numbers:

Lobby Hours
Monday – Friday
9:00 am – 4:00 pm

Drive Up Hours
Monday – Friday
8:30 am – 5:00 pm
Saturday: 8:00 am – 12:00 pm

301 East North Street
Rapid City, SD 57701
Phone (605) 394-1772



We do have a Night Depository located just pass our drive up window

