Our Two Cents

EMPLOYEE SPOTLIGHT

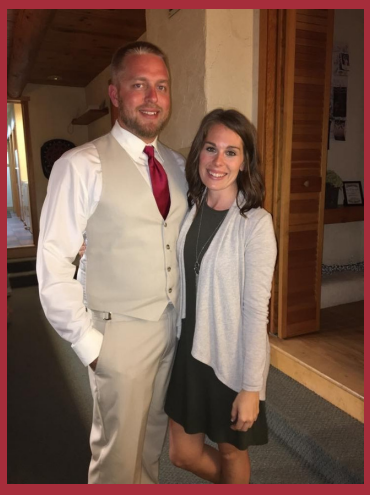
Sydney Strom has been working at First State Bank Southwest for 2 years and is the Staff Accountant.

She graduated from Augustana University in 2013 with her BA Sign Language Interpreting degree.

First State Bank Southwest introduced her to the banking world where she appreciated the learning curve and looks forward to every day. Sydney can be found upstairs at the Oxford office diligently working on financial reports, reconciling accounts, paying the bank's bills, assisting HR and the Audit/Compliance Officer, and helping wherever a hand is needed.

Sydney and her boyfriend, Ricky, live in Fulda, MN. They spend as much time as they can traveling the world.

She enjoys going for walks, planning the next adventure,being outdoors, spending time with family and friends, and going to NASCAR races—her and Ricky hope to check all the race tracks on the circuit off their list someday.



Beware of Phishing Scams - Don't Take the Bait

Identity thieves like to go "phishing" (pronounced "fishing") on the internet for consumers' personal financial information using fake emails and websites to trick people into providing social security numbers, bank account numbers and other valuable details.

Typically, the most common phishing emails pretend to be from a bank, retail store, or government agency to lure you into divulging person financial information, and often use a variety of tricks to make the email look legitimate. They might include a graphic copied from a bank's website of a link that looks like it goes to a bank's site, but actually leads to a fake site.

Also beware of "pharming". In this version of online identity theft, a hacker hijacks internet traffic so when you type in the address of a llegitamate website you're taken to the fake site. If you enter personal information at the phony site, it is harvested and used to commit fraud or sold to other identity thieves.

BUSINESS SPOTLIGHT

"It has been a pleasure to work with First State Bank Southwest as we move towards opening the doors at Forbidden Barrel Brewing Company in Worthington MN, August 29th, 2019.

We are new to First State Bank and have had the opportunity to work with Mark Vis. He has been supportive of our business plan and been a champion for us throughout this journey.

Brent started brewing beer as a hobby in 2009 after receiving beer brewing equipment as a Father's Day gift. Brent and Cheryl have since turned this hobby into a business. They have always enjoyed entertaining friends and hosting parties and after a lot of hard work are finally ready to realize that dream.

Forbidden Barrel Brewing Company is a family owned and operated brew pub and one of a kind everything! The concept of a brew pub that has the goal to sell locally sourced ingredients and locally crafted spirits and wines is new to everyone we have met.

We are local and want to support other businesses that are doing the same thing we are. We will be selling craft beer that is made right here in Worthington MN! We have a small menu of light snacks. We offer non-alcoholic options as well. The jalapeño lemonade is the right mix of sweet and spicy.

We currently have 8 employees including two of oursons that have decided to join the family business! Our goal is to have a great space to hang out with friends while enjoying some wonderful drinks."

- Brent and Cheryl Droll

Here are some tips to avoid becoming a victim of a phishing or pharming scam.

Be suspicious if someone contacts you unexpectedly online and asks for you personal information. It doesn't matter how the legitimate the email of website may look. Only open emails that look that they are from people or organization you know, and even then, be cautious if they look questionable.

For example, scam artists may hack into someone's email account and send out fake emails to friends and relatives, perhaps claiming that the real account owner is stranded abroad and might need your credit card information to return home.

Be especially wary of emails or websites that have typos or other obvious mistakes. "Because some requests come from people who primarily speak another language, that often contain poor grammar or spelling," said Amber Holmes, a financial crimes information specialist with the FDIC.

Remember that NO FINANCIAL INSTITUTION will email you and ask you to put sensitive information such as account numbers and PINs in your response. In fact, most institutions publicize that they will never ask for customer personal information over the phone or in an email because they already have it.

Assume that the request for information from a bank where you've never opened an account is probably a scam. Don't follow the link or enter your personal information.

Verify the validity of a suspicious -looking email or a pop-up box before providing personal information. Criminals can create emails stating that "you're a fraud victim" or a pop-up box with another urgent sounding message to trick people into providing information or installing malware (malicious software). If you want to check something out, independently contact the supposed source using an email address or phone number you know if valid.

If you ever question something that is sent out by First State Bank Southwest, please call any of our locations to verify that it came from us. We want all of our customers to be safe!