

FINANCIAL AWARENESS NEWSLETTER



January 2026

Contact Information:

Website: psbup.com

Phone: 906-387-2006

Fax: 906-387-4209

Member
FDIC



HELLO
January

THANK
YOU!

We would like to send a huge THANK YOU to everyone who has read our Monthly Newsletters over the last year. We look forward to continuing our newsletters through 2026 and providing all of you with happenings around the bank, as well as, Fraud and Scam Tips & Tricks.

HAPPY NEW YEAR
2026

From all of us at Peoples State Bank

JANUARY FINANCIAL WELLNESS MONTH

Financial Wellness Month
is a wonderful way to start
off the new year!

January can help prioritize
your upcoming financial
goals and well-being for
2026



NATIONAL USE YOUR GIFT CARD DAY

JANUARY 17TH, 2026

TODAY IS THE DAY TO USE UP THOSE GIFT CARDS YOU RECEIVED DURING THE HOLIDAYS!

DID YOU KNOW? ACCORDING TO RESEARCH BY MERCATOR ADVISORY GROUP, INC, \$3.5 BILLION IN GIFT CARDS GO UNREDEEMED EVERY YEAR. THAT'S A LOT OF WASTED MONEY!



THIS DAY SERVES AS A REMINDER TO NOT LET THOSE GIFT CARDS EXPIRE. IF YOU DON'T THINK YOU'LL USE IT, DONATE IT TO A GOOD CAUSE INSTEAD!



NATIONAL TECHNOLOGY DAY JANUARY 6, 2026

Today we recognize the technology we are surrounded by each and every day! The apps on your smartphone are due to the tech world for their advancements in technology. Their advancements have made an impression on all of us that impact us every day!



Social media platforms such as Facebook, Twitter, Instagram, and LinkedIn are wonderful tools for staying connected. Unfortunately, these platforms are also wonderful tools to manipulate and phish unsuspecting users. One way cybercriminals use social media to their advantage is through account spoofing. Account spoofing is when a scammer copies information from a social media account, such as the user's name, location, and photos, to create a look-alike account of that user. And then, from the spoofed account, the scammers send connection requests to everyone on the original account's list. Sometimes they even message these users with an excuse, such as "Sorry, I got hacked and had to make a new account!", to make the request more convincing.

How Can I Spot a Spoofed Account?

We tend to trust the people we are connected with, so the bad guys exploit this trust to phish for sensitive information, share malware, and even request money. It can be tough to tell if a social media account is authentic just by looking at it. Luckily, scammers like to make the first move. Keep the following in mind:

- Be cautious of any links sent through social media. Especially those that are off-topic, unusual, or outlandish such as gossip videos, dramatic news articles, or fabulous prizes.
- If you're being asked for money—it's probably a scam. If you feel the request may be legitimate, validate who you are speaking with and request proof of their claims.
- Don't trust connection requests or a suspicious message from someone who you are already connected with. Before responding, try to contact the person through a different form of communication like phone, text, or email.
- If you suspect that an account is a spoof of a real account, alert the owner of the legitimate account and report the suspicious account to the platform's customer service department.

How Can I Prevent My Account from Being Spoofed?

Keep your friends, followers, and reputation safe by following these tips:

- Keep your account private.
- Review and edit your privacy settings to be sure your information is kept private.
- Only accept connection requests from people you know and are comfortable sharing your posts with.