

FINANCIAL AWARENESS NEWSLETTER



October 2025

Contact Information:

Website: psbup.com

Phone: 906-387-2006

Fax: 906-387-4209





HELLO
OCTOBER

**We are excited to share our
Monthly Newsletter with all of
our customers new and existing!**

This month's newsletter will cover the
following topics:

Christmas Clubs
National Savings Day
Homecoming Tailgate Party
Halloween Spooky Hallway
Scam Alerts
Cyber Lunch-N-Learn Event
October Cyber Security Month

OCTOBER 6TH, 2025



**IS THE LAST DAY TO MAKE YOUR
CHRISTMAS CLUB DEPOSITS FOR 2025!**



CYBER LUNCH-N-LEARN

Join us for a free cyber-tastic
discussion presented by Lasco, Inc.
with lunch provided on
Wednesday, November 5th from 12-
1PM

RSVP HERE!



WWW.PSBUP.COM

NEW FACES

You may have noticed some new
faces on the teller line. Please
welcome them the next time you
stop in. Also note, during this time
we are working diligently to make
sure our staff is fully trained to
help with all your banking needs.
We ask that you be patient during
this time of learning.

Happy Plaidurday from all of us!



Unfortunately, cybercriminals often use sad news to trick you. Scammers are taking advantage of Pope Francis' recent death by using AI to create fake images and news articles about the event. They post this phony information on social media accounts in hopes of capturing your attention.

However, if you click the links in these social media posts, they'll take you to harmful websites that steal your personal and financial information.

Scammers have also made fake news websites with stories about Pope Francis. Some take you to fake Google pages that try to sell you gift cards as a scam to steal your information and money.

Others will install malware on your computer that is designed to steal your data. These malicious websites can even appear in online search results, so you might accidentally click on them. You could visit a dangerous website without even knowing!

Follow these tips to avoid falling victim to these types of scams:

- Keep your browser and computer's operating system updated with the latest security features.
- Don't click unknown links on websites, in emails, or in social media posts. You should only visit trusted news websites.
- Be careful when viewing exciting headlines or viral content. Scammers often use these to trick you into visiting malicious websites.

*** OCTOBER 12TH IS**
*National Savings Day **

- ✓ OPEN A SAVINGS ACCOUNT IF YOU DON'T ALREADY HAVE ONE!
- ✓ DOWNLOAD OUR APP - TRACK YOUR SPENDING AND SAVING HABITS FROM ANYWHERE!
- ✓ CREATE A BUDGET AND PUT EXCESS MONEY INTO YOUR SAVINGS ACCOUNT

****Peoples State Bank is not a financial advisor. Consult your financial advisor with any financial related questions****

HAPPY HALLOWEEN

Join Us In Our Spooky Hallway For A Sweet Treat
October 31st from Noon - 4:30

Is candy corn a fun tradition or a sugary sin?

Your bank will never pose candy corn conundrums. They won't call to ask for sensitive info like your social security number, either. Find out other things your bank will never ask, and test your scam spotting skills at BanksNeverAskThat.com. #BanksNeverAskThat

OCTOBER IS CYBERSECURITY MONTH

Are you staying cyber safe? Read on for some cyber tips to take part in not just for cybersecurity month, but every day!

-Malware/Ransomware

- o Back up your files on a regular basis; this will help protect your files from cybercriminals by making the files inaccessible
- o Using a secure network gives you the extra protection you need; using an un-secured W-Fi network opens you up to cybercriminals
- o Never pay the ransom. If you suspect you've become a victim to a ransomware attack, contact your IT team immediately. Paying the ransom doesn't guarantee you anything!

-Phishing

- o As phishing is still the most common attack, remember to think before you click. Check to see if there is an urgency within the email, who it came from and what time the email was sent, see if there are any attachments, and hover to discover over any links within the body of the email. If your organization uses PAB (Phish Alert Button), use it to report suspicious emails to your IT department; and if you don't use PAB, still report any suspicious emails to your IT department

-QR Codes

- o Stay alert and be cautious of the QR codes you're scanning. With the rise of QR Code scams, you'll want to know the origin of the QR code. If you're not sure whether or not to use a QR code, check out their website or ask for the physical items to look at that information instead

-Passwords

- o Use a password manager to store all of your passwords and to help generate new passwords for each website/app when it's time to change your password. Use passphrases that would be hard to guess when creating a password. Don't share your passwords with anyone!

-Social Media Oversharing

- o Oversharing on social media can make you an easy target for cybercriminals to gather data
- o Don't use the same password for work as you would for your personal accounts
- o Keep your personal and work business separate

-2FA

- o Enabling 2 factor authentication gives you a sense of protection because your data cannot be accessed without proper identity verification
- o 2FA includes hardware and software tokens (physical device/authenticator app), biometric 2fa (face/fingerprint), push notifications, email notifications, SMS text messages, and phone calls

-Devices up to date

- o Keeping your devices up to date will help protect against new cyber threats. Out-dated software is an easy target for cybercriminals