February 2025 • Issue 18

SERVICE UPDATES

- St. Clair College transcripts are now available online through a secure platform called **MyCreds**, making it easier then ever to access your official records. As part of the ARUCC National Network, MyCreds lets you securely manage and share your transcripts from a portable, learner-focused wallet. Once you request your transcript, you'll receive an email withing 1-2 business days with instructions on setting up your MyCreds account. Full-time students already pay a fee that includes two free official transcripts per year, with additional copies available for just $10 each. You can find the MyCreds tile in the MyStClair Portal. For more details, check out the St. Clair College website.
- The College has implemented a new Identity Management system, which will work differently then the former system. New Students and Staff will receive an email with a Claim Code. This Claim Code is used to grant you initial access to the system to setup your account. It will walk you setting a new password and Multi-Factor Authentication. You can see a sample of this new email here.
- Along with this new Account system, there are changes to access limits on accounts. Students who no longer enrolled and are not a Alumni will have 90 days of access before their account is longer available. Graduates will keep their accounts but the level of MS Office licensing changes to Online only. Part-time Faculty will have 180 days of access to their accounts after the contract end date. All other staff will have 14 days of access after contract end.

MONTHLY FEATURES

- Unclear how to print in Classrooms and Labs? These steps can help.

THE CYBERSECURITY CORNER

How to Avoid Tech Support Scams: Protect Yourself from Fraudulent Calls

Tech support scams are a common type of fraud, often starting with an unsolicited call, email, or pop-up claiming that there's a serious issue with your computer. The scammer impersonates a tech company, like Microsoft or Apple, and offers to "fix" the problem by remotely accessing your computer. Their goal is to steal personal information, install malware, or charge for unnecessary services. Here's how to recognize and avoid these scams.

Signs of a Tech Support Scam

1. **Unsolicited Contact:** Legitimate companies don't call you out of the blue. If you didn't request support, it's likely a scam.
2. **Urgency and Pressure:** Scammers create panic, claiming that your computer is infected or at risk.
3. **Remote Access Requests:** Fraudsters will ask for remote control of your computer-never allow this from an unsolicited caller.
4. **Payment Demands:** Scammers often ask for payment for "fixes" that aren't needed. Real tech companies usually offer free support for common issues.
5. **Grammar or Technical Errors:** Watch for suspicious mistakes in messages or odd language that seems unprofessional.

What to Do If You Receive a Suspicious Call

1. **Hang Up Immediately:** If it's unsolicited, end the call right away.
2. **Don't Share Personal Info:** Never give out payment details or login information over the phone.

3. **Verify the Caller:** Call the company directly using a verified number to check if the issue is legitimate.
4. **Check for Pop-Up Messages:** If you get a pop-up claiming your computer has a virus, close it immediately. Don't click on anything.
5. **Run Antivirus Software:** If you've already engaged with the scammer, run a full virus scan to check for malware.

How to Protect Yourself

1. **Be Skeptical of Unknown Calls:** If you didn't contact the company first, it's probably a scam.
2. **Use Trusted Antivirus Software:** Keep your devices protected with up-to-date antivirus tools.
3. **Monitor Financial Accounts:** Watch for unusual charges if you've provided payment information.
4. **Report Scams:** If you suspect a scam, report it to relevant authorities to help protect others.

What to Do If You've Fallen for a Scam

If you've already provided access or paid a scammer:

1. **Disconnect from the Internet:** Prevent further damage.
2. **Change Passwords:** Update your passwords, especially for sensitive accounts.
3. **Contact Your Bank:** Report any financial fraud.
4. **Run Antivirus and Report the Incident:** Remove any malware and report the scam to authorities.

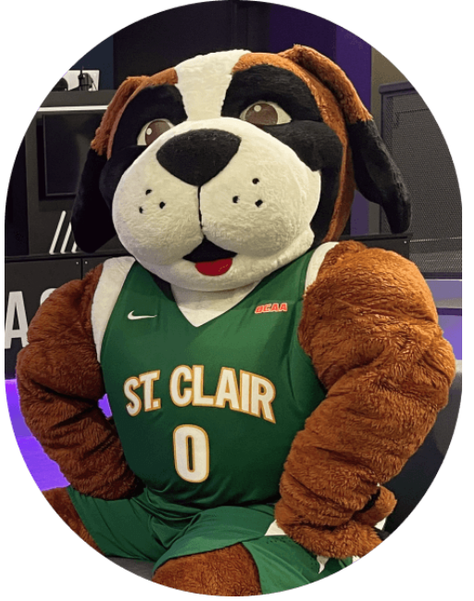
Conclusion
Tech support scams are becoming more common, but you can protect yourself by being cautious of unsolicited calls and messages. Always verify the legitimacy of the request, never grant remote access without confirmation, and report suspicious activity to prevent further harm. Stay vigilant to keep your information and devices secure.

GRIFF'S PRO TIP OF THE MONTH

Don't Lose Your Data

Sometimes the IT Department has to erase computers to fix problems. Make sure you don't have any data saved to the local C:\ drive of computers, ***because it could get deleted without notice***. Make sure you're saving your

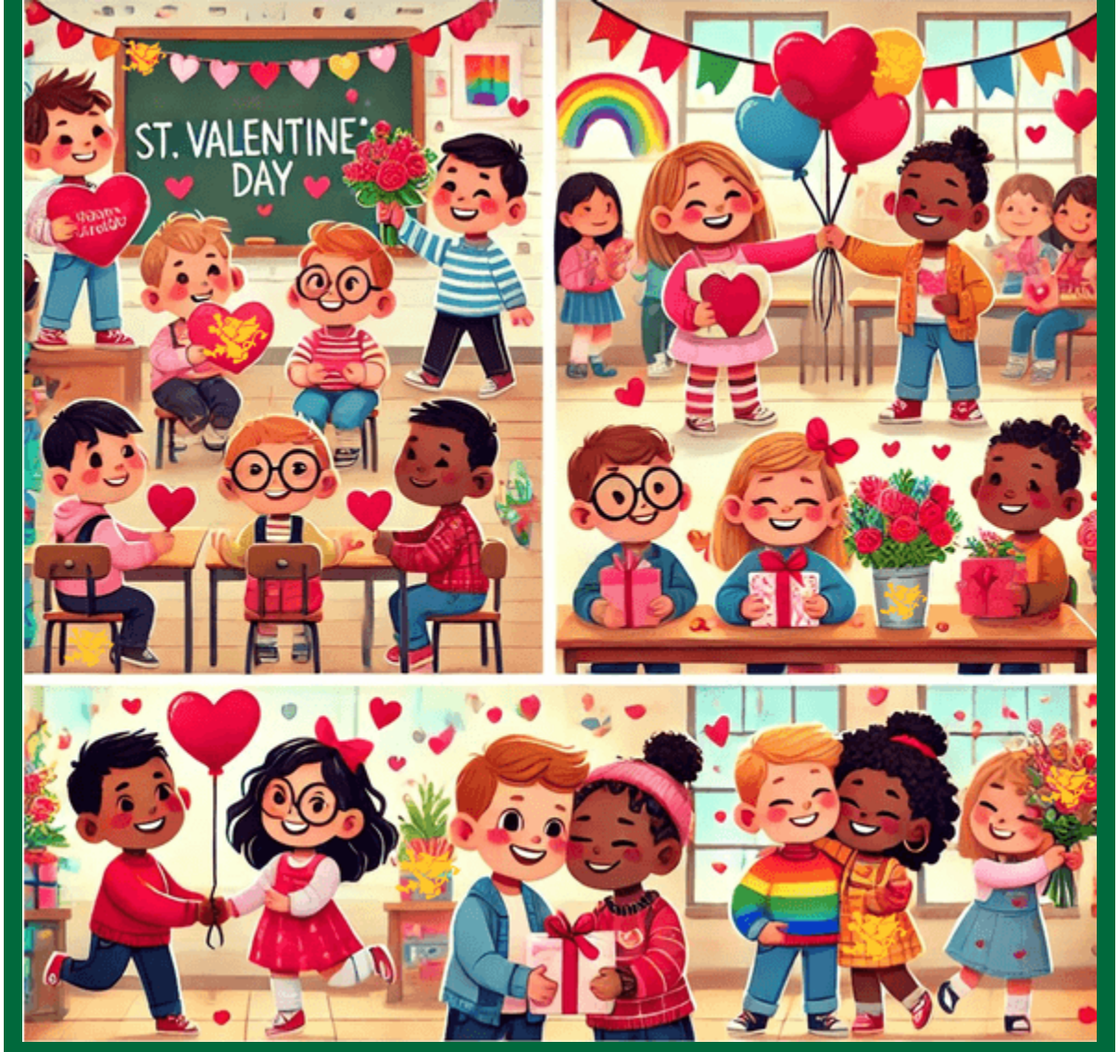
files to your OneDrive or to a trusted external device (USB key).



THIS MONTH'S CONTEST

Find the Hidden Griffins

Scour the St. Valentine's scene below to find all of the hidden griffins.



Use this online form to submit your answer. Three (3) winners will be chosen at random.

See contest rules.

DECEMBER'S CONTEST WINNERS

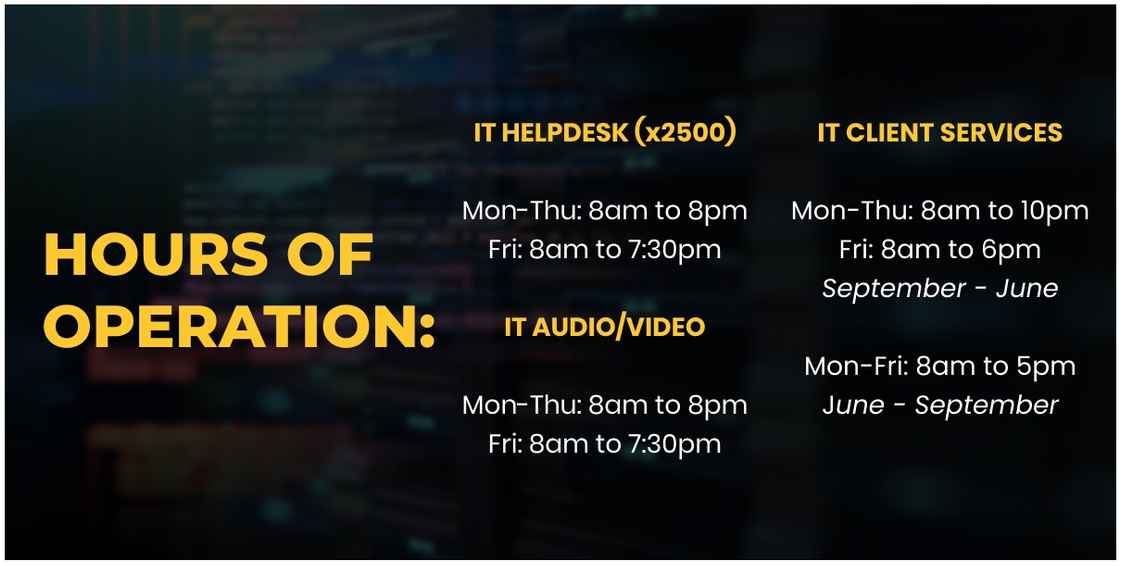
Congratulations to our 3 WINNERS from last month's contest!

The answer to last months riddle is: **A Smartphone**

REG ROBINSON	MEHAK SHRIVASTAV	BRIANNA VICENTE

SELF SERVICE

Need assistance? We're here to help! Simply click the links to Open an IT Support Ticket or Book an Appointment with Front Desk.



Something you'd like to see in future issues?
Drop Us a Line