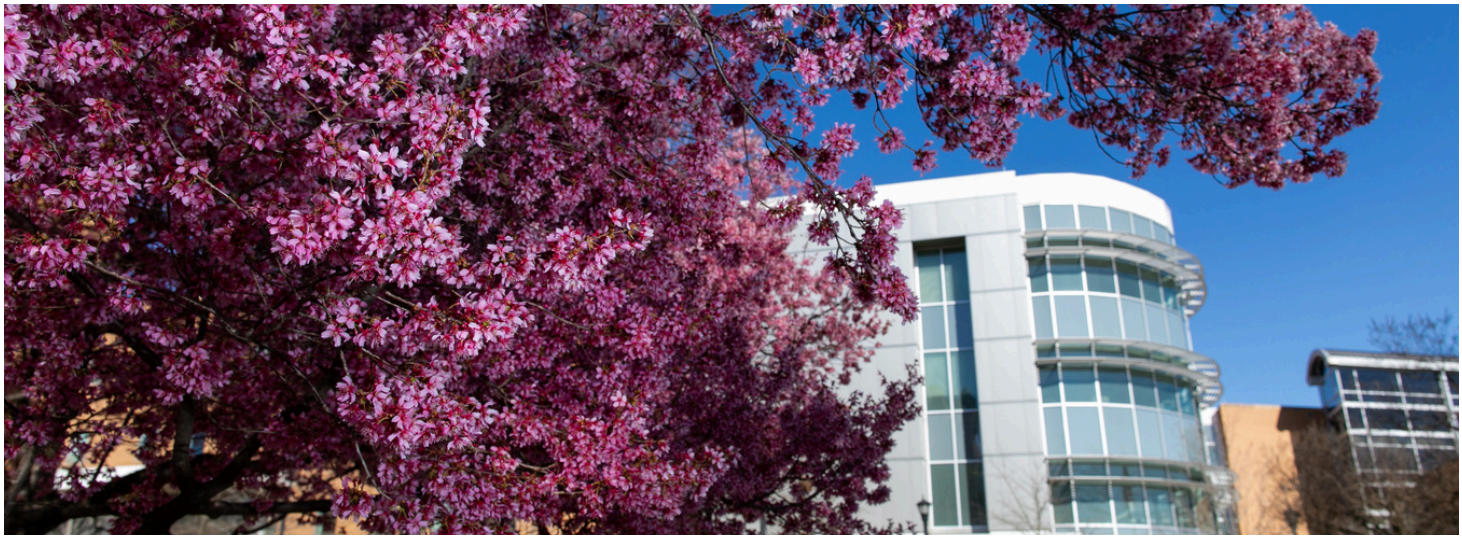
Spring 2026

KENNESAW STATE UNIVERSITY

RETIREES ASSOCIATION NEWSLETTER



Welcome!

Spring is here! The Kennesaw State University Retirees Association (KSURA) wishes you a happy Spring!

In the Spring newsletter you will find:

- pictures from the recent Biennial Reunion held in March
- a recap of the Cybersecurity presentation
- a welcome to the newest retirees
- the latest info on KSU retiree email accounts
- call for volunteers to fill our various committees

We hope you find this newsletter helpful and we encourage you to attend any and all events that match your interests. KSURA events are open to ALL retirees, regardless of whether you are a member. Attending an event will give you the opportunity to learn something new as well as catch up with your fellow KSU/SPSU retirees!

Find us on Facebook - https://www.facebook.com/kennesaw.retirees

Calling all retirees- join us for our Events Planning Retreat! On April 30, we invite retirees of KSU and SPSU to come together and help us plan for 2026-2027.

When: Thursday, April 30, 2026
Time: 10:00 a.m. - 1:00 p.m.
Where: KSU Town Point, Conference Room 4750 (3391 Town Point Dr NW, Kennesaw, GA 30144)

Lunch will be provided. RSVP is required by Monday, April 27, 2026. Click here to register.

Biennial Reunion 2026

KSU Golden Owls gathered for our Biennial Renuion this March. We had a great turnout, lots of fun, and renewed friendships! Here are a few of the pictures. You can see more photos online at https://www.kennesaw.edu/retirees/news-events.php then click on “Photo Gallery” under “Quick Links”

Congratulations to the newest class of Retirees! They were celebrated at the Retirement Ceremony held on April 1, 2026.

Donna Adams
Finn Ahlberg
Viola Alexander
Nancy Ballard
Michael Beach
Cynthia Bowers
Daniel Branham
Donald Brookshire
Guthrie Brown
Teresa Clements
Nathan Davies
Tammy DeMel
Thomas Devaney
Jennifer Dickey
Christina Emerson
Adrian Epps
Kimberly Friedrichs
Davide Gaetano
Bobby Gaskins
Gina Gavin
John Haseltine
Paul Hearn
Heather Hermanson
Carol Hulsey
Lee Hunter
Joyce Ingram
David Jones
Amy Jordan
Géza Kogler
Vickie Lee
Alan Lipschitz
Marie Manuel
Beth Marks
Diana McClintock
Laura McRath
Marietta Monaghan
Nina Morgan
Huggins Msimanga
Arlene Paige
Richard Parker
Tara Parker
Marsha Powell
Michael Redd
Stephanie Roper
Gail Scott
Mary Smith
Pamela Smith
Thomas Thibodeau
Christina Turner
Paul Wakeman
John Warren
Ryan Whitfield
Jo Williamson
Kenneth Williamson

Cybersecurity for Retirees

On March 24, 2026, Tobias Simpson, Director of Data Security and Awareness for the Office of Cybersecurity in UITS, presented to the KSU Retirees Association on the topic of Cybersecurity for Retirees. Here are some important take-aways from the presentation.

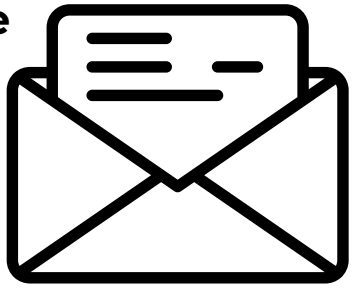
Retirees are a top target for scammers. We often have retirement savings, we are trusting and polite, we have less awareness of the "digital world", and we often delay reporting when scammed out of embarrassment or uncertainty.

Top tactics of scammers

How to spot scams

Want more information, including how to protect yourself and what to do if you are the victim of a scam? The full presentation is included at the end of this newsletter. There are 11 slides, each with important information to help keep you protected against fraud and scams.

Sunsetting KSU Retiree Email Accounts



At our April Steering Committee meeting, members of UITS Leadership gave us an update on the university's plan to "sunset" retiree email accounts. They also answered questions from our members. Here is a summary of the discussion.

Who is affected?
KSU email accounts for emeritus professors will not be removed, per USG policy. All other retiree email accounts will be closed.

When will this happen?
Some retirees received a message from HR stating emails would be closed May 1, 2026. However, that email was sent prematurely, as **a date has not yet been determined**. The most likely timeline is in the Fall. UITS has two related projects to implement before they will sunset retiree email accounts. More information will be shared as UITS moves through their processes.

Why is this happening?
The main driver of sunsetting our email accounts is cybersecurity risk management. Many accounts are not being used which allows scammers potential access. Dormant accounts may still have access to sensitive data that would be useful to scammers.

What can/should you do now?
Make sure you have an email account other than your KSU email. Start moving anything you want to keep from your KSU account to your personal email. Update your email address on other accounts where you used your KSU email as your log in or account for communications.

What is the KSU Retirees Association doing?
Through our university liaisons, Glynnis Holt and Frances Beusse, we are monitoring the timeline from UITS and have requested they provide resources to assist retirees in moving their information. We are also investigating setting up our own training class(es) to assist retirees with setting up new accounts and navigating this change. We will provide additional information as it becomes available.

Volunteers Needed!

Spring 2026 Forever Owl Fest is right around the corner! This is always a great time to help welcome a new class of graduates as we celebrate them on the Campus Green. There are TEN commencement ceremonies so a lot of opportunities to get involved.

What do volunteers do?

- Greet and Welcome New Owls to the Nest!
- Help with crowd control and lines as grads and their families take pictures at one of our photo ops!
- Wayfind / Provide directional support to guests when needed

Click Here to Sign Up!

KSU Alumni & Friends invites all who love KSU or are connected to the university to travel together! We have an upcoming trip: Treasures & Temples of Singapore & Bangkok, October 7 - 16, 2026

Click here for more info.

Reminder: The KSU Retirees Association supports **CARE Services** by accepting donations at all KSU Retirees Association events. You can visit the CARE Campus Pantry page here, to see what items are needed for the pantry and a link to their Amazon wishlist.

Join the KSURA

The Kennesaw State University Retirees Association provides opportunities for all former KSU and SPSU employees to stay connected to one another and the University.

We have several committees that help keep the association organized and running smoothly. Please consider joining any of our committees. We need committee chairs as well as committee members.

The Retirees Association Steering Committee is the overarching committee that reviews and approves programming and financial decisions, as well as sets the direction of the association.

Committees

Membership - creates and maintains a plan for recruitment of new members.
Scholarship - promotes a culture of giving among retirees and annually reviews the criteria for our Legacy Endowed Scholarship.
Bylaws - ensures that association activites align with our bylaws and reviews our governing documents annually.
Events - assist the association with planning and implementing events and provide ideas and feedback for new events.
Communication - provides timely announcements of importance to the membership through emails, newsletters, and social media.
Colloquium - invites experts in the field to present their work to the membership.

How to get involved:

1. Email or call the KSU Retirees Association
2. Contact one of the Co-Chairs
3. Come to a Steering Committee meeting (2nd Friday of each month at 10am in Town Point room 4750, Kennesaw campus - August through May, we do not meet June and July)

Your Golden Owls Newsletter

The KSU Retirees Association Golden Owls Newsletter is for you. Please let us know what features you would like to read about, information you would find helpful, and suggestions you may have for us. You can send your comments to retirees@kennesaw.edu, and they will be shared with the Communications Committee.

Retiree Resources

(Click the link to open that resource)

- KSU Retirees Association
- Osher Lifelong Learning Institute (OLLI)
- KSU Fitness Center
- USG Retirees page
- AROHE - Assoc of Retirement Organizations in Higher Ed
- GA-HERO - Georgia Assoc of Higher Ed Retiree Orgs

Photos!

You can see photos from past events by going to our website: kennesaw.edu/retirees, then click on “News and Events”, then click on “Photo Gallery” under “Quick Links”.

KSU Retirees Association
2025-26 Co-Chairs

David Baugher
Herb Smith
Ann Vancza
Chris Ziegler

The KSURA is an affinity group under the KSU Office of Alumni and Constituent Engagement

Thank you to Glynnis Holt, Program Coordinator, for assisting the KSU Retirees Association.

KSU RETIREES ASSOCIATION
www.kennesaw.edu/retirees retirees@kennesaw.edu 470-578-2112

FOOD FOR THOUGHT

Cybersecurity Strategies

for Kennesaw State University Retirees

Protecting Your Digital Life — Simple Strategies That Work

Staying Safe in the Digital Age

Why Are We a Target?

Cybercriminals specifically target retirees because of predictable advantages they perceive:

Retirement Savings

Retirees often hold significant savings and pension income — making them high-value targets for financial fraud.

Trust & Politeness

Many grew up in an era of greater trust. Scammers exploit this social courtesy to gain access.

Less Digital Exposure

Less daily workplace cyber training means fewer red-flag recognition skills for newer scam tactics.

Delayed Reporting

Victims often hesitate to report — embarrassment or uncertainty about who to contact can delay action.

⚠ **The FBI reports Americans over 60 lost $3.4 BILLION to cyber fraud in one recent year alone**

Today's Threat Menu

— The Dishes You Don't Want to Be Served

Phishing Emails

Fake emails mimicking banks, Medicare, or Amazon asking you to click a link or verify credentials.

Vishing (Voice Calls)

"Your Social Security number has been suspended." Scammers use fear and urgency over the phone.

Smishing (Text Scams)

Fraudulent SMS messages with links claiming package delivery issues, prize wins, or account alerts.

Ransomware

Malicious software that locks your computer files and demands payment — often via gift cards.

Identity Theft

Stealing personal data to open accounts, file tax returns, or claim benefits in your name.

Grandparent Scam

"Grandma, I'm in trouble!" — Criminals pose as grandchildren or lawyers needing emergency money.

Password Power: Your First Line of Defense

✓ WHAT TO DO

- Use at least 12 characters — length is strength
- Mix uppercase, lowercase, numbers, and symbols
- Use a unique password for EVERY account
- Try a passphrase: 'BlueDog!DancesTango9'
- Use a Password Manager (LastPass, Bitwarden, 1Password)
- Enable Two-Factor Authentication (2FA) everywhere

✗ WHAT TO AVOID

- Your name, birthday, or pet's name
- "Password123" or "123456" — top guessed passwords
- Reusing the same password on multiple sites
- Writing passwords on sticky notes near your computer
- Sharing your password over the phone or email
- Answering password reset questions truthfully (use fake answers!)

Pro Tip: A password manager remembers ALL your passwords — you only need to remember ONE master password.

Don't Take the Bait: Spotting Phishing Scams

If you receive a suspicious email or text, look for these RED FLAGS before clicking anything:

⚠ Urgency & Fear

"Act NOW or your account will be closed!" — Scammers create panic to override careful thinking.

⚠ Unexpected Requests

No real bank, government agency, or tech company will ask for your password or SSN via email.

⚠ Suspicious Sender Address

"support@amaz0n-help.net" — hover over the email address. Tiny misspellings are a dead giveaway.

⚠ Generic Greetings

"Dear Valued Customer" instead of your name. Legitimate companies know who you are.

⚠ Links That Don't Match

Hover over any link BEFORE clicking. The web address shown should match the company's real website.

⚠ Too Good to Be True

A prize, refund, or inheritance you weren't expecting. If it sounds too good, it almost certainly is.

When in doubt — DO NOT click. Call the company directly using a phone number from their OFFICIAL website.

Safe Browsing & Public Wi-Fi

Safe Browsing Habits

- Look for HTTPS (padlock icon) before entering any personal or financial info
- Keep your browser and operating system UPDATED — updates patch security holes
- Only download software from official websites — no pop-up offers
- Use an ad-blocker (uBlock Origin) to reduce malicious ads
- Clear your browser cache and cookies regularly
- Avoid saving credit card numbers in browsers

Public Wi-Fi Dangers

- Coffee shops, airports, hotels — hackers can see your traffic on open networks
- NEVER do online banking or shopping on public Wi-Fi
- Consider a VPN (Virtual Private Network) — it encrypts your connection
- Turn off automatic Wi-Fi connection on your devices
- Verify the exact network name with staff — fake "Free Airport Wi-Fi" networks are common
- When in doubt, use your phone's cellular data instead

Home Wi-Fi: Use WPA3 encryption, change the default router password, and hide your network name (SSID).

Social Media & Privacy: What You Share Matters

Every detail you share publicly can be used to guess your passwords, answer security questions, or craft a targeted scam.

What NOT to Share Publicly

- Your full birth date
- Your home address
- Vacation plans (while away)
- Phone number
- Mother's maiden name
- Photos of mail, IDs, or documents

Privacy Settings Checklist

- Set Facebook to 'Friends Only'
- Limit who sees your posts and photos
- Turn off location tagging in photos
- Review apps linked to your accounts
- Opt out of data sharing in settings
- Google yourself to see what's visible

Friend Requests & Messages

- Only accept people you actually know
- Beware duplicate accounts — even from 'friends'
- Never send money to online contacts
- Be skeptical of investment tips via social media
- Romance scams often start here — be cautious
- When in doubt, call the real person directly

Think of social media as a public bulletin board — only post what you'd be comfortable seeing in a newspaper headline.

Securing Your Devices

Keep Everything Updated —
Enable automatic updates for Windows/Mac, your smartphone, and all apps. Updates patch critical security vulnerabilities that hackers exploit.

Install Antivirus Software —
Use reputable antivirus (Bitdefender, Malwarebytes, Windows Defender is free). Run scans weekly. Never buy antivirus from a pop-up ad.

Back Up Your Data — Regularly! —

Follow the 3-2-1 rule: 3 copies, on 2 different media, 1 offsite (cloud). If ransomware strikes, you can recover everything.

Secure Your Smartphone —
Use a PIN or fingerprint lock. Enable 'Find My Device' and remote wipe. Only install apps from the official App Store or Google Play.

Physical Security Matters —
Lock your computer when stepping away (Windows+L). Don't leave devices unattended in public. Use a privacy screen in coffee shops.

If You've Been Hacked or Scammed — Act Fast

It is NOT your fault. Scammers are sophisticated professionals. What matters now is acting quickly.

1

Don't Pay More

If you've already sent money, stop all further payments immediately. Scammers will ask again.

2

Change Your Passwords

Change passwords for all affected accounts immediately. Start with email — it's the master key.

3

Contact Your Bank

Call the number on the back of your card. Report fraud, freeze accounts if needed, request a new card.

4

Report It

FTC: reportfraud.ftc.gov | FBI IC3: ic3.gov | Local police report (needed for insurance claims).

5

Credit Freeze

Contact Equifax, Experian, and TransUnion to freeze your credit — prevents new accounts being opened.

6

Tell Someone You Trust

Tell a family member or trusted friend. You need support, and they can help spot further risks.

✅ Your Personal Cybersecurity Checklist

START TODAY

- Change weak passwords to strong ones
- Turn on 2-factor authentication on email
- Run an antivirus scan on your computer
- Check your bank statement for anything odd

THIS WEEK

- Back up your computer to an external drive or cloud
- Review Facebook/social privacy settings
- Install a password manager
- Check if your email was breached: haveibeenpwned.com

ONGOING HABITS

- Pause before clicking ANY link in email or text
- Keep devices and apps updated
- Never give personal info to unsolicited callers
- Shred documents with account numbers or SSN

You don't need to be a tech expert — just curious, cautious, and consistent.

You Are Your Best Cybersecurity Tool

Stay skeptical. Stay safe. Stay connected.

HELPFUL RESOURCES

FTC Consumer Protection
consumer.ftc.gov

FBI Internet Crime Center
ic3.gov

AARP Fraud Watch Network
aarp.org/fraudwatchnetwork

StopBullying / StaySafeOnline
staysafeonline.org

Have I Been Pwned (email breach check)
haveibeenpwned.com

FTC Fraud Report
reportfraud.ftc.gov

Questions? Let's Discuss!