CIO Insight

KENNESAW STATE UNIVERSITY
UNIVERSITY INFORMATION TECHNOLOGY SERVICES

April 2022

Mandatory Spring 2022 Cybersecurity Training is Almost Here!

Since 2020, all USG employees are required to complete cybersecurity awareness training twice annually. KSU conducts the first training throughout the month of April and the second later in the year as the USG-provided “USG Cybersecurity Awareness Training”.

The April Cybersecurity training will be released on April 1, 2022, and run through midnight on April 30, 2022. The training is completely online and will take about 15 minutes to complete. The focus is on identifying a phishing attack and the risks related to phishing emails.

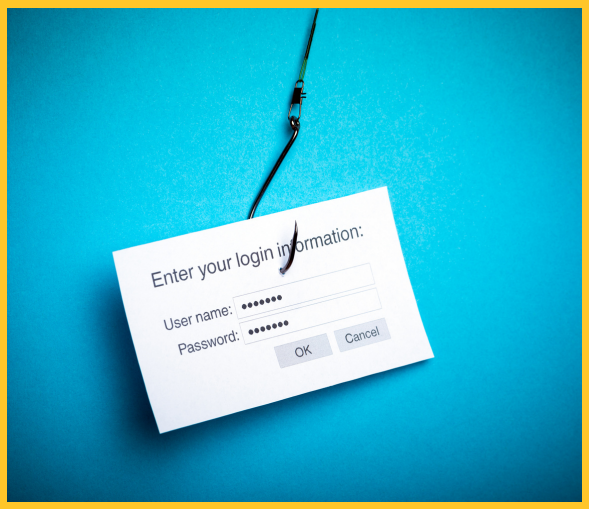
New Voices in ReadSpeaker

In the coming days, new voices (speech personas) will be added to ReadSpeaker. This update will improve the functionality and usability of the ReadSpeaker's Text to Speech tool in D2L. New speech personas that can be easily selected from within the ReadSpeaker widget have been added. For more information, please review the ReadSpeaker guide in the UITS Documentation Center.

Do You Have a Technology Problem or Question? Search in ServiceNow!

When you have problems or questions, did you know KSU's service portal, ServiceNow (service.kennesaw.edu) is always there to help! You can discover solutions in the knowledgebase, request support, and even check on the status of a ticket or request you have submitted.

Visit the service portal now: service.kennesaw.edu



New Tool to Report Phishing Emails

UITS is excited to offer faculty and staff an easier way to report suspicious/phishing emails. Reporting suspicious emails is as simple as clicking the "Phish Alert Report" button in your KSU email application and confirming your submission in the pop-up panel on the right-hand side of the screen.

Find answers to some common questions below:

What does the "Phish Alert Report" button look like?

The "Phish Alert Report" button can look slightly different based on whether you're using Outlook on the Web (ksumail.kennesaw.edu), the Outlook app on your computer, or a mobile device. See the image below to familiarize yourself with the variations.

What happens when I click the "Phish Alert Report"?

When a user clicks the "Phish Alert Report" button, another pop-up on the right-hand side of the screen will confirm your choice to report the email. The email will then be deleted from your inbox and forwarded to the UITS Office of Cybersecurity for investigation.

What if I made a mistake in clicking the "Phish Alert Report" and need to access a reported email?

If a user needs to access a message that has been reported, the message can be found in that user's "Deleted Items" folder until it is emptied—which makes the deletion permanent, similar to any other deleted message. As long as the message is still in the "Deleted Items" folder, it may be moved back to the user's inbox.

What if I'm not sure whether an email is a phishing attempt?

It's always better to err on the side of caution. If you are unable to verify a sender's unusual or suspicious request in-person, by phone, or through a Teams message, you can report that message by clicking the "Phish Alert Report" and confirming your submission on the pop-up panel on the right-hand side of the screen.

Learn more about phishing here.

ChangeGear Decomissioning

During the Spring 2022 semester, UITS will be decommissioning the ChangeGear ticket management system. Current users of ChangeGear are strongly encouraged to migrate to the ServiceNow platform.

New Employee Onboarding

New employees are required to complete required cybersecurity training in the first 30 days of their employment. This training is in addition to the semi-annual required employee cybersecurity training.

Workshops & One-on-One Technology Support

Are you ready to build your skills and learn something new? Are you trying to use a new-to-you piece of campus software and have questions or feel stuck? Consider joining a workshop to learn new software and use it more effectively. Booking a one-on-one training session lets you work with a trainer one-on-one to address specific questions or needs.

PROJECT MANAGEMENT COMING TO SERVICENOW

The UITS Project and Process Management Team will be migrating from Team Dynamix to ServiceNow in the Spring of 2022, offering customers several advantages:

- Simple IT web intake request form
- Enterprise platform integrated with an existing service ticketing system to reduce the learning curve
- Project reporting and historical performance analytics data to align projects with University strategies and goals
- Visibility over the entire project progress from request, prioritization, and qualification, to closure for improved stakeholder collaboration
- Flexibility with management tools: traditional Waterfall, Agile, and Hybrid to maximum project outcomes

GALILEO Changes Coming Soon

If you link to GALILEO resources such as articles, databases, or eBooks in your D2L Course, please note that your course links will need to be updated by Monday, June 13, 2022, to ensure easy access to resources from D2L for students.

Updates are needed because GALILEO has changed the way users access their library's electronic resources. This change has impacted all USG institutions, including Kennesaw State University.

Previously, access required using a GALILEO password but now, using the OpenAthens platform, users may access their library resources using their campus credentials. They no longer need to retrieve a separate password.

You may begin updating the links effective immediately, and all updates should be completed by Monday, June 13.

To Update GALILEO Links in D2L:

1. Log in to D2L and navigate to your course.
2. Wherever you have a link to a GALILEO resource:
   a. navigate to the resource
   b. copy a new link
   c. replace the link in your course

If you encounter issues with updating your links, please email service@kennesaw.edu for assistance.

CYBERSECURITY TIPS FROM THE USG

In light of recent events in Europe, you may have questions and concerns about cybersecurity. Am I or is our organization more likely to come under attack? Am I at greater risk?
We don't have all the answers, nor do we know what will happen next. But we do know from a cybersecurity perspective, continuing to focus on the fundamentals is key to protecting yourself at home and at work. While the sense of urgency may have changed, how cyber attackers target us has not. Here are the fundamentals upon which to focus:

1. **Phishing:** Phishing and related scams are when cyber attackers attempt to trick or fool you into doing something you should not do. Often these scams are sent as emails, but they can also be text messages, phone calls, or social media posts. Anytime someone is creating a tremendous sense of urgency and rushing you to take an action, or someone is promoting an offer that sounds too good to be true, it is most likely an attack.
2. **Passwords:** Strong passwords are the key to protecting your online, digital life. Make sure each of your accounts is protected by a unique, long password. The longer your password, the better. To keep it simple, use passphrases, a type of password made up of multiple words like "honey-butter-happy". Can't remember all your passwords? Neither can we. That is why we also recommend you use a Password Manager such as Last Pass to securely store all your passwords. Finally, whenever possible, enable Multi-Factor Authentication (MFA) on your important personal accounts as we have for the USG accounts.
3. **Updating:** Keep your personal computers, devices and apps updated and current by enabling automatic updating on all your devices. Cyber attackers are constantly looking for new vulnerabilities in the devices and software you use. Keeping them automatically updated makes sure these known weaknesses are fixed and your devices have the latest security features.

In addition, there is going to be a tremendous amount of false information spread on the Internet. Do not trust or rely on information from new, unknown, or random social media accounts, such as posts on LinkedIn, Instagram, Facebook, or Twitter. Many accounts on these sites were created for the sole purpose of putting out fake information. Instead, follow only well-known, trusted news sources that verify the authenticity of information before they broadcast it. Finally, if you wish to donate to any causes in support of recent events, make sure you are donating to a well-known, trusted charity. There will be many scams attempting to trick people into donating to fake charities run by cybercriminals.

Continue to focus on the fundamentals you have learned from USG Cybersecurity, and you will go a long way to protecting yourself, no matter who the cyber attacker is. Contact cybersecurity@usg.edu if you have questions.