Information Resources & Technology

January 2019 Newsletter

Build Custom Org Charts With RIMS

Rowan University employees may now create custom organizational charts with data from the Rowan Identity Management System (RIMS).

By downloading RIMS data and using an online application called LucidChart, employees may develop organizational charts that suit their specific needs.

RIMS: Training & Support Materials

Want to learn more about RIMS? Review training and support information at go.rowan.edu/rims.

Employees may also easily modify a chart's style and layout and export a chart as a PDF to share or post online.

We have compiled several how-to guides to help employees get started with creating organizational charts using RIMS and LucidChart. Please review these resources for assistance in creating a custom organizational chart.

How-To Resources

- RIMS: Customizing Your Organizational Chart
- Video: Create an Organizational Chart in LucidChart
- LucidChart: First Time Login Using Rowan Google Account

Gift Card Email Scam Targets Faculty, Staff

TAKE NOTE!

An email scam that is targeting faculty and staff members at universities and colleges across the country, including Rowan University, aims to trick recipients into buying iTunes and Amazon gift cards.

These emails are often crafted to appear like they are coming from a person in a leadership position, such as a dean, department chair or vice president, by including the name of the person in the email address and in the "From" field of the message.

The emails may start by asking the recipient: "Are you available?" If the recipient of the email responds, the scammer — posing as the university leader — claims they are caught in a meeting, requests the recipient purchase gifts cards on their behalf and promises to reimburse them later.

The Chronicle of Higher Education reports that the scam has targeted faculty members at "more than a dozen universities."

If you receive such an email, do not respond to it. Delete it, and remember to never respond to purchase requests or requests for assistance with financial transactions without directly verifying with the individual that the request is real.

Watch Out for W-2 Scams During Tax Season

TIP OF THE MONTH

As tax season approaches, we would like to warn Rowan University employees and student workers of scams aiming to trick people into giving personal information to cybercriminals who want to profit from stolen data. One scam that circulated in previous years targeted tax records through emails that notified employees their W-2 forms were ready to view online and provided a direct link to view the form.

Rowan University will **never** send you an email **with a direct link** to view or print your W-2 form. If you elected to print your W-2 form online from Self-Service Banner, instructions on how to do so are available on the Payroll Services website.

The Information Security Office at Rowan University would also like to remind all University employees and student workers of the spear phishing and social engineering examples covered in your security awareness training modules and urge you to:

- Never divulge any personal information in response to an email, social media request or phone call. If there is reason to believe that the request is real, please contact the Technology Support Center at 856-256-4400 or support@rowan.edu to verify.
- Never click on links or open attachments contained in unsolicited email messages.
- Before clicking on any link in an email, always verify the link's legitimacy by hovering your cursor over the link to see where it leads.
- Never use the same password for your email account, bank accounts, social media, etc. In the event you do fall victim to a phishing scam, the thieves may attempt to use your stolen password in as many places as they can. If you suspect that you have been compromised, change all of your passwords as quickly as possible and inform the Technology Support Center.
- Take extra precaution when using your mobile device to view email. It may be easier to miss telltale signs of phishing attempts when reading email on a smaller screen.

Please contact the Technology Support Center at 856-256-4400 or support@rowan.edu with any questions.

Follow Us on Social Media

One of the best ways to keep up with the latest news and information about technology at Rowan University is to follow us on social media.

We're regularly posting helpful tips, links to resources and other information to our Twitter and Facebook accounts. Follow us!

Twitter

@RowanIRT

Facebook

facebook.com/RowanIRT

Duo Now Required for All Students, Employees

All Rowan University students and employees are now required to use Duo two-factor authentication. If you haven't enrolled yet, you will be prompted to do so the next time you change your password. Don't wait ... enroll in Duo today by taking these three steps:

1. Go to https://duo.rowan.edu and log in with your Rowan Network username and password.

2. **Create a Portal Security PIN & Don't Forget It:** Once you log in to the Duo Portal you'll be prompted to create a six-digit Portal Security PIN. Enter a six-digit number you can easily remember. Don't forget your PIN!

3. **Register at Least One Device:** We recommend using the Duo app on your smartphone as your primary device, but there are several options available to use with Duo.

Visit go.rowan.edu/duo for FAQs and other information about Duo.

Two-Factor Authentication Required for Rowan Services Protected by Duo

IRT POLICY SPOTLIGHT

Two-factor authentication adds a second layer of security to Rowan Network accounts, which helps to prevent unauthorized access to an account even if the password is compromised.

Rowan University currently uses a product called Duo for two-factor authentication. Duo can provide a second form of authentication via a mobile device app, phone or hardware token. The mobile device app is recommended. Rowan users must use at least one but are encouraged to have at least two registered methods of two-factor authentication in Duo so that they can always log in to a Rowan service even if one method is temporarily unavailable.

Per the Two-Factor Authentication Policy, using Duo for two-factor authentication is mandatory for all Rowan services protected by Duo. A list of Rowan services currently protected by Duo is available in our Knowledge Base.

To review the entire Two-Factor Authentication Policy and other IRT policies, visit go.rowan.edu/irtpolicies.

Security Threats

In December, we detected and blocked **27** virus attacks and **18,800** emails with malicious URLs sent to our network.

Universities are prime targets for cyberattacks due to the amount of personal data and sensitive research material stored on their networks.

Please immediately contact the Technology Support Center if you think you have clicked on a malicious link or attachment in an email. Acting quickly will minimize the risk to the University.

Request Support Help

Visit our support portal to request help and search our knowledge base for answers to common questions.

Double-click on the support icon shown below from a Rowan-managed computer, or go to support.rowan.edu.

You may also call or email us for help.

Phone: 856-256-4400
Email: support@rowan.edu

Follow @RowanIRT

RowanUniversity
INFORMATION RESOURCES & TECHNOLOGY