Information Resources & Technology

December 2018 Newsletter

Duo to Protect Outlook Web App

More security is coming soon to Rowan University's Outlook Web App.

On Sunday, Dec. 30, Duo two-factor authentication will be enabled on the Outlook Web App, also known as OWA, which allows employees and medical students to check their Rowan University email from a web browser.

This means that starting on Dec. 30 when you log in to exchange.rowan.edu or outlook.rowan.edu, you will be prompted to verify your identity through Duo. The process will be the same as if you were logging in to any other Duo-protected website or application at Rowan University, such as Blackboard or Google Drive.

Visit Our Duo Page for More Info

Check out go.rowan.edu/duo for more information about Duo two-factor authentication.

Only those who are enrolled in Duo will start to be prompted to verify their identity on Dec. 30. But all employees and students will be required to enroll in Duo during the spring semester, and we encourage you to sign up now.

Visit go.rowan.edu/duo for additional information about Duo at Rowan.

Duo Required for All Students as of Jan. 2

TAKE NOTE!

Rowan University students: do you Duo? If you don't, beginning January 2, 2019, you will be required to enroll in Duo the next time you update your Rowan Network password. Don't wait until then… 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.

   If Your Password Has Expired: You must click on the "My Rowan Network password has expired" link under "Alternative Login Options" to get access to the Duo Portal.

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.

8 Tips for Staying Secure in a Connected Home

TIP OF THE MONTH

Google Homes and other Internet of Things (IoT) devices give you the power to turn on your lights, place an online order or read your email with a simple voice command. While convenient and increasingly popular, this smart technology also raises security risks and privacy concerns.

Thomas F. Duffy, Senior Vice President of Operations and Services at the Center for Internet Security, offers these tips for protecting your information in a smart home.

1. **If you don't need to connect a device to the Internet, don't.** If a device isn't connected, it isn't as big of a cyber-security risk.
2. **Isolate IoT devices from other devices on your network** by creating a separate WiFi network just for them. This protects your other devices if your connected IoT devices are compromised.
3. **Research the privacy, security, and accessibility options** that are available for customizing your device. You may find some options that provide greater security and privacy if you opt-in.
4. **Always update your devices and apply patches when available.** When selecting which IoT devices to purchase, ensure they offer patching and updates from the manufacturer to keep them up-to-date. Enable auto-updates on any IoT devices that support them.
5. **Setup a separate unique, strong password for every device.** Don't share credentials across devices.
6. **Replace devices when they are no longer supported by the vendor,** as security flaws will remain unpatched.
7. **Turn off Universal Plug and Play if it is available** on the device. You don't want the device having this ease of connectivity with so little control.
8. When requested to provide information to use a device, **do not provide personally identifiable information** (PII), like Social Security Numbers and dates of birth. If you must share PII to use the device, you may want to consider a different make or model or keeping it off your home network.

Visit the Center for Internet Security's website for more information about staying cyber secure with IoT devices.

Holiday Support Hours

Please note that our support teams will have updated hours of service over the upcoming holidays. All of our offices will be closed on Tuesday, Dec. 25, and Tuesday, Jan. 1.

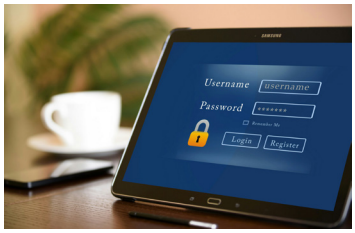
Technology Support Center

From Monday, Dec. 24, to Friday, Jan. 4, the Technology Support Center will be open Monday to Friday from 8 a.m. to 5 p.m.

The Technology Support Center's extended evening hours will return on Monday, Jan. 7.

Visit https://irt.rowan.edu/help/ for a full list of holiday support hours on all campuses.

How Do You Remember Your Passwords?



We want to know how Rowan University students and employees keep track of all the passwords you need to log in to important online accounts.

Do you write them down? Do you use a password vault, like LastPass? Or are you frequently resetting forgotten passwords?

Let us know by casting your vote in our poll.

VOTE IN OUR **PASSWORD POLL**

Technology Purchased With University Funds Is the University's Property

IRT POLICY SPOTLIGHT

The Technology Ownership Policy states that any technology, including laptops, desktops, tablets, cell phones, software, printers, monitors, keyboards and cables, purchased with University funds is the property of Rowan University.

Per this policy, all technology purchases must be delivered to IRT before deployment to ensure that items are properly configured to comply with the University's security and technology policies.

If an employee separates from the University, the Technology Ownership Policy states that it is the responsibility of that employee and his or her supervisor to ensure that all technology is returned to the University at the time of employee separation.

If an employee fails to return University-owned devices, they will be charged the initial cost of the device.

To review the entire Technology Ownership Policy and other IRT policies, visit go.rowan.edu/irtpolicies.

Security Threats

In November, we detected and blocked **198** virus attacks and **34,000** 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