Information Resources & Technology

September 2018 Newsletter

Celebrating NCSAM 2018

We have been getting ready to celebrate National Cyber Security Awareness Month (NCSAM), which is observed every October. NCSAM is an opportune time for every member of Rowan University to take stock of their online behavior and learn a few tips to stay safe in an increasingly connected world.

Throughout October, we will be promoting NCSAM and the “STOP. THINK. CONNECT.” campaign by sharing best practices for securing your online accounts, providing tips on how to identify common scams and offering other advice to ward off potential cyber attacks.

Visit Our NCSAM Page for More Info

Throughout the month, visit go.rowan.edu/ncsam for tips for protecting yourself online.

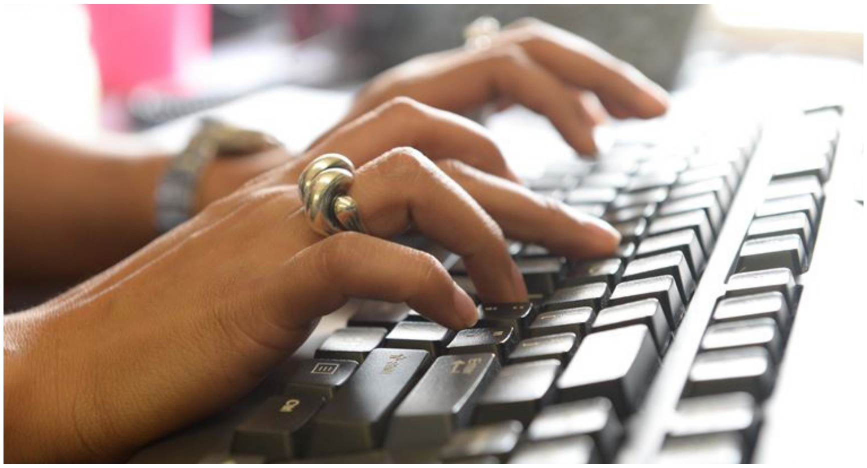
We will be posting these valuable resources on our website and social media accounts.

Visit go.rowan.edu/ncsam and follow us on Twitter and Facebook to stay up to date with the latest NCSAM content.

Cyber security is everyone’s responsibility, and we look forward to helping you stay safer and more secure online.

TIP OF THE MONTH

Responded to a Scam? Take These Steps



Email and phone scams are becoming increasingly sophisticated, which may make it difficult to identify whether a message is legitimate or trying to trick you into releasing personal information.

Shared a Password?

If you do fall victim to a scam and shared personal information, like your password, we recommend that you change the passwords to your online accounts immediately. You should also update your software and run a virus scan.

Shared Financial Information?

If you responded to a scam and shared financial information, such as your bank account number, contact the Rowan University Department of Public Safety at 856-256-4922 and ask to speak or meet with a police officer so they can file a report.

We also recommend you change your passwords, update your software, check your accounts regularly, contact credit agencies, banks, credit card companies and other agencies. For details, review our What to Do If You Responded to an Email or Phone Scam article.

Help Us Keep Rowan University Safe

We rely on every member of Rowan University to learn and follow best practices for staying safe online. Use these tips to get started, and visit go.rowan.edu/ncsam for more information.

Lock Down Your Login

Your usernames and passwords are not enough to protect key accounts. Use strong authentication tools whenever offered.

Keep a Clean Machine

Keep all software on internet-connected devices current to reduce risk of infection from ransomware and malware.

When in Doubt, Throw it Out

If an email, tweet or other post looks suspicious, even if you know the source, it's best to delete or, if appropriate, mark it as junk.

Back It Up

Protect your valuable work, music, photos and other digital information by making an electronic copy and storing it safely.

Own Your Online Presence

Set the privacy and security settings on websites to your comfort level for information sharing. It is OK to limit information you share online.

Share With Care

Think before posting about yourself and others online. Consider what a post reveals, who might see it and how it might affect you or others.

Value Personal Information

Information about you, such as purchase history or location, has value — just like money. Be thoughtful about who gets that information.

IRT POLICY SPOTLIGHT

Two-Factor Authentication Required for Rowan Services Protected by Duo

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 August, we detected and blocked **50** virus attacks and **44,500** 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

Hours:

Monday - Thursday: 8 a.m. to 8 p.m.
Friday: 8 a.m. to 5 p.m.

Follow @RowanIRT

RowanUniversity
INFORMATION RESOURCES & TECHNOLOGY