Information Resources & Technology

January 2018 Newsletter

Latest News

McAfee Anti-Virus Upgrade

In January, Information Resources & Technology accelerated the planned release of McAfee Endpoint Security to students and employees for use on their personal Windows computers.

We sped up our deployment timeline in order to address issues raised by the recently-found Meltdown and Spectre vulnerabilities in computer chips.

What Are Meltdown and Spectre?

Meltdown and Spectre are chip flaws that pose a security risk for most modern computing devices. Go to the next page for details.

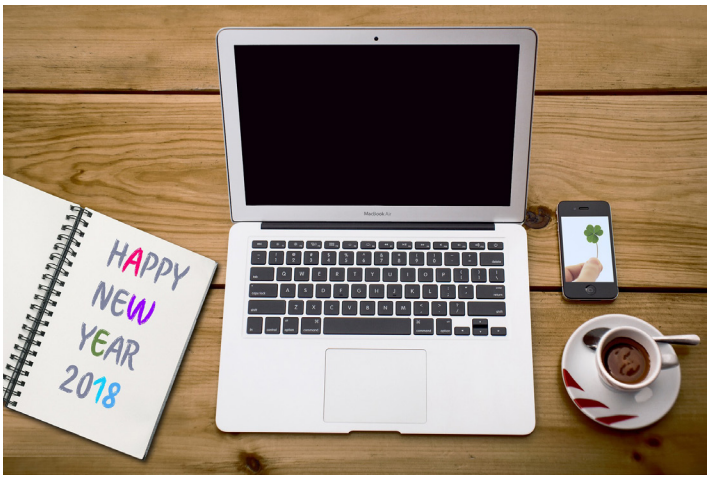
Software updates being rolled out to address these security flaws may affect the anti-virus software students and employees need to access the University's secure wireless network from a personal Windows computer. Mac users are not affected by these updates.

If ClearPass (correctly) blocks you from joining the Rowan Network, you will need to uninstall your current anti-virus software and install a new product.

Visit rowan.edu/irt and click on McAfee Endpoint Security under Quick Links for download instructions.

Tip of the Month

Start 2018 With a New, Secure Password



It's one month into 2018, and it's likely that many of you have already broken at least one of your New Year's resolutions.

Don't fret! We've got another goal for you to pursue that you can easily accomplish and that will make your online life more secure. Kick off 2018 with a new, secure password.

Put aside common nouns and simple variations on words when creating passwords. Are you using qwerty, 123456 or password to protect any of your accounts? Fix that now!

You want complex passwords with a combination of capital and lowercase letters, numbers and special characters to protect your personal data from potential exposure.

For more help creating a secure password, review our article on choosing strong passwords. Visit rowan.edu/irt and click Choose a Strong Password under IRT Links. Our Security Awareness page at rowan.edu/go/security also includes helpful information about protecting yourself online.

Meltdown and Spectre: What You Need to Know

Researchers recently discovered security flaws in the design of computer chips that affect most modern computing devices. These flaws, called Meltdown and Spectre, could provide hackers with a way to steal personal data from computers and smartphones.

There is no evidence that these flaws have been exploited yet, and technology companies are releasing software patches to address the problem and limit risk. Here's what else you need to know.

What Are Meltdown and Spectre?

Meltdown and Spectr, which were publicly announced earlier this year, are the names given to security vulnerabilities in computer chips.

These vulnerabilities are caused by a design flaw in computer chips involving a technique known as speculative execution.

Speculative execution is used to improve the performance of computer processors, but may also provides hackers a way to access sensitive data.

Why Should I Care?

Nearly every computer chip manufactured in the last two decades is affected by these flaws.

That means that every computing device you own, including desktops, laptops, tablets and smartphones, are at risk.

If a hacker successfully exploited one of these vulnerabilities, they could access information, like passwords and security certificates, that was previously thought to be inaccessible.

Can These Flaws Be Fixed?

The underlying vulnerabilities exist at the hardware level and completely eliminating the issue will require new hardware, but technology companies are releasing software patches to work around the vulnerabilities.

While experts have so far identified three attack methods involving these vulnerabilities, more may be discovered that will require new patches.

Expect to continue hearing about Meltdown and Spectre over the next several years.

What Should I Do Now?

Companies are releasing patches to address these flaws that will require updates to your devices. Keep an eye out for those updates, but note that some of these updates may conflict with other software. A recent Windows update interfered with some anti-virus software. That update may have affected students and employees trying to connect personal laptops to Rowan's Network.

We accelerated our planned release of McAfee to address that issue, which did not affect Rowan University-owned and managed machines.

Where Can I Learn More?

Many news outlets are closely following the Meltdown and Spectre developments. You can also reach out to us with any questions or concerns. Email us at support@rowan.edu or call us at 856-256-4400, and we will get back to you as soon as possible.

IRT Policy Spotlight

IT Acquisition Policy

Are you aware of the University's IT Acquisition Policy?

That policy mandates that most hardware and software purchases and renewals receive approval from IRT to ensure compatibility with existing technology and compliance with the University's security requirements and regulations.

ITAP approval is required for all new IT acquisitions and renewals including software, hardware, IT consulting and IT services by academic, administrative, clinical and research departments, as well equipment that comes with specialized software.

Also remember that the department or college acquiring an IT resource is responsible for paying the costs associated with purchasing, installing and maintaining that resource.

To review the entire IT Acquisition Policy and other IRT policies, visit the University Policies website.

Security Threats

In December, we detected and blocked **96 virus attacks** and **73,000 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, email or visit us in Memorial Hall for help.

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

Walk-In Help Available:

Monday - Thursday: 9 a.m. to 7 p.m.
Friday: 9 a.m. to 5 p.m.

Follow @RowanIRT

Rowan University
INFORMATION RESOURCES & TECHNOLOGY