Information Resources & Technology

November 2017 Newsletter

Latest News

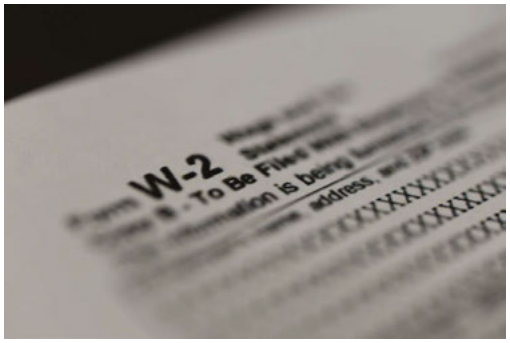
Beware of W-2 Scams

As tax season approaches, we would like to warn Rowan University employees 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.

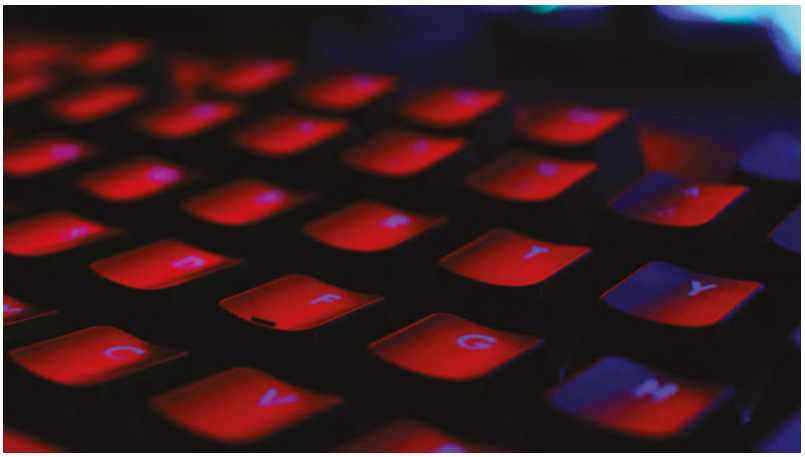
Rowan University will never send you an email to view or print your W-2 form.

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.



Tip of the Month

Help Others Become Cybersecure

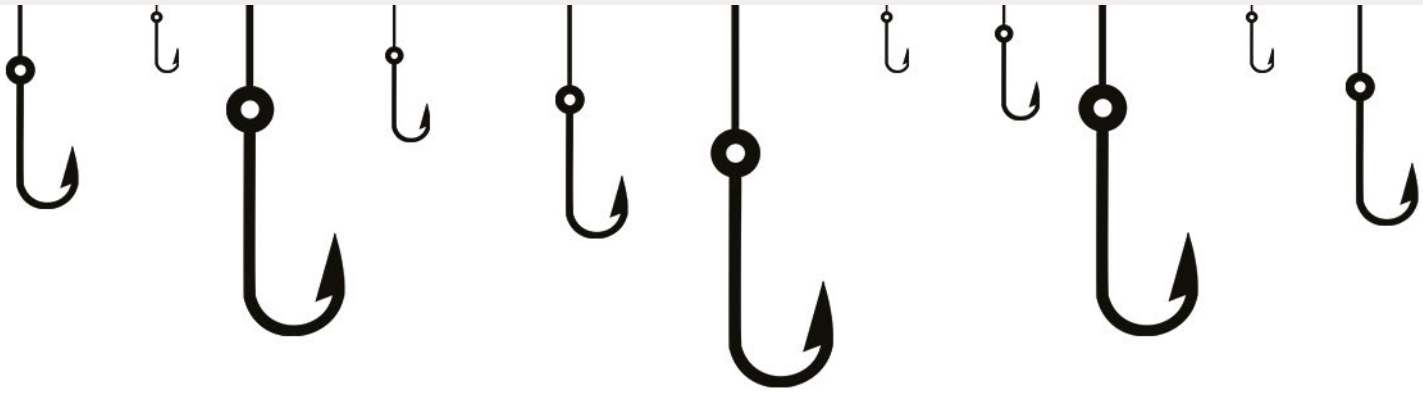


While you may know how to safely and securely use technology, other friends and family members may not feel so comfortable. Some of your loved ones may find technology confusing or scary, making them vulnerable to cyber attacks.

Here are five steps an information security expert recommends you take to help your friends or family members overcome their fears and make the most of today's technology.

- **Explain social engineering:** Share examples of common social engineering attacks, like phishing emails.
- **Create strong passwords:** Teach your loved ones how to create strong passwords and enable two-step authentication.
- **Enable automatic updates:** Ensure devices are fully up-to-date by enabling automatic updates whenever possible.
- **Install anti-virus software:** Install anti-virus software on computers and make sure the software is current and active.
- **Set up a backup system:** Put an automated backup file system in place to help recover data if it's lost.

Don't Fall Prey to Phishing Attacks



The phishing scams that hackers use in an attempt to steal your personal information are more sophisticated than ever. Cybercriminals have recently targeted Netflix subscribers and Google Docs users in convincing email schemes that mimic the look and feel of legitimate messages from those services.

That's why it's more important than ever that Rowan University students and employees know how to spot a potential phishing scam. If you receive an email you were not expecting, take the following steps to identify and avoid phishing attacks.

Verify Before You Click.

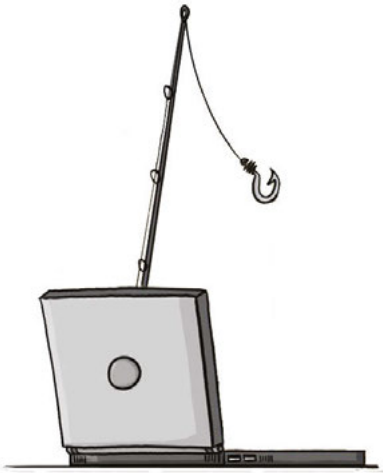
Hover your cursor over links in emails to see where they will lead you before clicking, even if you think you know the sender.

Look for Red Flags.

Be skeptical of emails with obvious spelling mistakes and generic greetings, as well as those demanding you take immediate action.

When in Doubt, Throw It Out.

If you receive an email that you find suspicious, even if you think you know the source, it's best to delete the message.



Don't Take the Bait!

Email scams that try to trick recipients into providing sensitive personal and financial information pose a direct threat to universities around the world.

One recent phishing attack on MacEwan University in Canada resulted in staff members making nearly $10 million in payments to a fraudulent account. We need to make sure that if students or employees at Rowan University receive a phishing email, they don't take the bait.

For more information about protecting yourself against phishing scams, visit the Security and Safe Computing section of the IRT website at irt.rowan.edu.

IRT Policy Spotlight

Data Governance Policy

Any person that accesses University data should be familiar with the Data Governance Policy, which details responsibilities for managing different classifications of data and sets standards for data storage, destruction and access mechanisms.

That policy states:

- University Data is a valuable asset. It involves all University constituencies (students, faculty, staff, etc.) and resources (funds, space, technology, etc.) that are captured and used in the operations of the University.
- No one person, department, division, school, or group "owns" the data used by the University, even though specific units bear the primary responsibility for some data.
- Controlling access to University Data is important to protecting the University and its constituency from liability and acts of malice. All public records requests are routed through University Counsel.

To review the entire Data Governance Policy, visit irt.rowan.edu/display/POLICY/Data+Governance+Policy.

Security Threats

In October, we detected and blocked 195 virus attacks and 28,700 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. Acting quickly will minimize the risk to the University's network.

Need computer 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 Us

facebook.com/RowanIRT

@RowanIRT

Rowan University
INFORMATION RESOURCES & TECHNOLOGY