Protect Yourself Against Phishing Scams

What Are Spam and Phishing?

**Spam** is the use of email systems to send unsolicited, and usually undesired, bulk messages. Some spam is merely annoying, while other spam can cause damage to your computer or the entire campus network.

**Phishing** is a specific type of spam. Phishing or spoofing is the term used for deceitful or fraudulent emails designed to trick people into providing personal information that leaves them vulnerable to identity theft, computer viruses and compromised email accounts. The number and sophistication of phishing scams continue to increase. Other types of phishing can include phony websites or phone calls that ask potential victims to supply or verify their personal information.

**Spear Phishing** is an even more insidious form of phishing, where Rowan users are targeted by someone claiming to be from Rowan University.

- Change your password
- Outlook WebAccess
- Gmail for Students
- Banner Self Service
- Blackboard Login
- Access From Anywhere

Protect Yourself!

If you receive a suspicious email:

- **Do not reply**, even if you recognize the sender as a well-known business or financial institution. If you have an account with this institution, contact them directly and ask them to verify the information included in the email.
- **Do not click any links** provided in these emails (or cut and paste them into a browser). This may download viruses to your computer or, at best, confirm your email address to phishers.
- **Do not open any attachments**. If you receive an attachment you are not expecting, confirm with the sender that they sent the message and intended to send you an attachment.
- **Do not enter your personal information on an untrusted website or form** referenced in any email.
- **Delete the message**.

Want to test your phishing IQ and find out what kind of scams you're most likely to miss? Take this test.

If you have responded to a suspicious email with your Rowan username and password:

If you have already provided your Rowan account information in response to a phishing email, your email account may be disabled (all accounts that send over a certain number of emails an hour will be suspended).

It is critical that you:

- **Change your password immediately**.
- **Contact the Technology Support Center** to report the incident and get your Rowan account reinstated if needed.

Please remember:

No one involved with technology at Rowan will ever ask for your password through an email for any reason.

Any message you receive asking for the password to your Rowan account, even if the message claims to be from someone at Rowan, is a scam. Always ignore and delete such messages.

We do not send quota messages requiring your password or disable mailboxes and ask users to "re-validate" OR "update" them.

We need everyone to please be aware of this and never give out your Rowan username and password through a link in any email message.

STOP. THINK. CONNECT.
When you cross the street, you look both ways to make sure it's safe. Staying safe on the Internet is similar. It takes some common sense steps — Stop. Think. Connect.

Protect yourself and help keep the web a safer place for everyone.

**More Information**

For more information about phishing and how to avoid scams, visit:

- [OnGuardOnline.gov](http://OnGuardOnline.gov)
- [New Jersey Cybersecurity Lifehacker](http://New Jersey Cybersecurity Lifehacker)

Lifehacker also offers some simple phishing detection tips in this article: "How to Boost Your Phishing Detection Skills and Avoid Email Scams."

---

**W2 Scam Alert**

At tax time, there is an increase in spear phishing and social engineering attempts by cybercriminals who want to profit from stolen data. One scheme that circulated last year 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](http://Payroll Services website).