Ping Wang <wangp@rmu.edu>

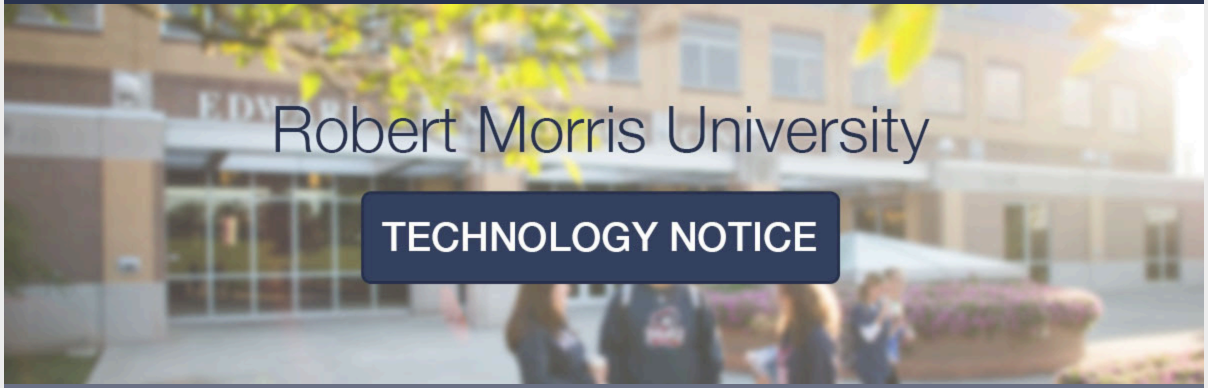
RMU Technology Notice: Cybersecurity Awareness Month

1 message

Help Door <help@rmu.edu>
Reply-To: help@rmu.edu
To: Help Desk <help@rmu.edu>

Tue, Oct 21, 2025 at 6:15 PM

RMU Technology Notice
Cybersecurity Awareness Month



Important: Robert Morris University Information Technology will **never** ask you to provide sensitive information including passwords.

Cybersecurity Awareness Month

With Cybersecurity Awareness Month well underway, here are some valuable cybersecurity tips.

We all have a shared responsibility to protect the University against cybersecurity threats. Technical security measures managed by the RMU IT and Information Security teams help to protect the institution from technical cyber attacks, but social engineering attacks remain a common cause of major data breaches across the world. Our people are our first line of defense against these threats. Stay vigilant, report suspicious email, and ask the Help Desk or me if you are ever unsure about something.

Cybersecurity Awareness Month Top 10 Tips:

1. Think before you click! Be careful with email and stay on the lookout for malicious phishing messages. Report anything unusual using the Phish Alarm button in your email, which is on the toolbar on the right side or at the bottom of the message in the mobile app.
2. Always use Multi-Factor Authentication wherever it is available. Use it across all platforms: education, banking, shopping, social media, and more.
3. Regularly check your bank accounts, credit cards and your credit rating for anomalies. Consider freezing your credit - it is an easy and free way to protect yourself.
4. Always change the default password on your smart devices. This includes anything that you connect to your home network, like Alexa / Ring Doorbell / Nest Thermostat, etc.
5. Keep your software up to date with security patches. Unpatched software can lead to vulnerability to malware, which could lead to identity theft or worse.
6. Secure your home network by changing the default router password and using strong encryption. If possible, provide a guest network for visitors also using strong encryption and a unique password.
7. Always be cautious when using public wireless networks.
8. Use strong, unique 14 character or longer passwords whenever possible.
9. Backup your data regularly. University computers are provided with Google Drive and Microsoft OneDrive. For personal computers, consider using a cloud provider like Google or Dropbox, or even a USB device.
10. Regularly check your privacy settings on your social media accounts. These settings are often changed by the platforms, and need to be reviewed and adjusted regularly.

Cybersecurity Contest:

We are conducting a Phishing Tournament that goes through the end of October. The first 5 employees who report 3 simulated phishing messages using the Phish Alarm button will receive prizes.

If you have any questions about any of the above tips, or any other cybersecurity topic, please reach out to me directly, Jim Mahony at mahony@rmu.edu. I would be happy to provide more information via email or even during a Google Meet if schedules allow.

Thank you,

Jim Mahony
CISO

Robert Morris University
Information Technology
Help Desk
412-397-2211
help@rmu.edu

Did you know?

- You can reactivate your account by going to www.rmu.edu/reactivate.
- You can reset your RMU passwords by going to www.rmu.edu/password.

Verify the authenticity of this email at **rmu.edu/verifyemail**
EMAIL ID: WSE-41B38AF0DD9875B8E0635018600AA96A