MARIST UNIVERSITY
Information Technology

Cybersecurity Newsletter

NOVEMBER 2025 EDITION • VOLUME 2

Welcome to the second Marist IT Cybersecurity newsletter. November introduces new cyber threats as holiday shopping is on the rise. This month we are passing along some tips on how to stay safe while shopping for your friends and family this year.

1 ALWAYS CHECK YOUR DEVICES

Always make sure that your devices and browsers are up-to-date before online shopping. Vulnerable devices or software can leave your devices susceptible to cyber attacks.

2 ONLY SHOP WITH TRUSTED SOURCES

Always verify the sources you visit before you enter your information on websites. Ensure that you are visiting legitimate wesbites. If you recieve an unsolicited email, do not click any links or provide any information. Ensure when online shopping that you are connected to a secure internet connection to protect your information.

3 UTILIZE SAFE METHODS FOR ONLINE SHOPPING

When possible, use credit cards when online shopping. Debit cards do not offer the same fraud protections as credit cards do. Check your bank statements often as well to check for fraudulent charges.

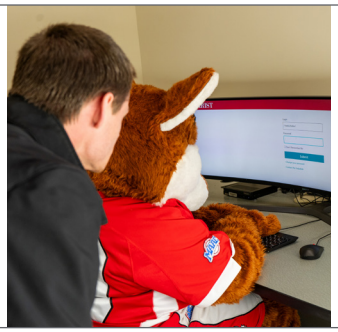
4 KEEP AN EYE OUT FOR SEASONAL PHISHING

The holiday season is a popular time for fake package delivery notifications, e-cards, and charity donation requests. Emails requesting purchase confirmations are also popular. Always verify emails before providing information.

5 MAINTAIN GOOD ACCOUNT SECURITY

When creating online accounts, always maintain good password hygiene by creating strong passwords and utilizing two-factor authentication when possible.

November 30th is NATIONAL COMPUTER SECURITY DAY!



Need to reset your password?

Utilize our self-service portal: https://myaccount.marist.edu/react/

See more cybersecurity resources by checking out the Information Security Website: marist.edu/information-security