Top 3: Security News in December 2023

1. Kremlin-backed hackers attacking unpatched Outlook systems, Microsoft says
   TheRecord.media
   Hackers associated with Russia's military intelligence are still actively exploiting a vulnerability in Microsoft software to gain access to victims' emails.

2. Booking.com clients prone to cyber fraud, warns analyst
   CyberNews.com
   One of the world's largest online travel agencies says its customers are being increasingly targeted by scammers, according to a cybersecurity firm.

3. Google Unveils RETVec - Gmail's New Defense Against Spam and Malicious Emails
   ITTheHackerNews.com
   Google has revealed a new multilingual text vectorizer called RETVec (short for Resilient and Efficient Text Vectorizer) to help detect potentially harmful content such as spam and malicious emails in Gmail.

Cybercriminals Escalate Microsoft Office Attacks By 53% in 2023
   Report reveals an average detection of 411,000 malicious files per day this year, Click to read more.

Suspected digital shopping fraud up 12% during Cyber Five holiday
   An new report released by TransUnion highlights global e-commerce fraud that occurred during the start of the 2023 holiday shopping season. Click to read more.

75% of sports-related passwords are reused across accounts
   33% of Americans have used a sports-themed password. Click to read more.
As the holiday season beckons, the excitement of gift-giving and festive bargains fills the air. However, amidst the joyful hustle and bustle, the need for cyber vigilance is paramount. With cyber threats looming, students, esteemed faculty and staff at our university must gear up for a cyber-safe shopping spree.

### 1. Check Your Devices: Strengthen Your Cyber Armor
In the realm of cybersecurity, fortifying your devices is the first line of defense:

- **Implement Multi-Factor Authentication (MFA)**
  Elevate your account security with MFA—it’s like adding a lock to your digital front door. Protect your valuable information with this powerful shield against potential cyber intruders.

- **Update & Automate Your Software**
  Stay ahead in the cyber race by regularly updating your device software. Activate automatic updates to ensure your defenses are always reinforced against evolving threats.

### 2. Shop Only Through Trusted Sources: Navigate the Digital Marketplace Safely
In the labyrinth of online shopping, steering clear of cyber threats requires informed choices:

- **Think Before You Click**
  Phishing emails are the gateway for many cyber-attacks. Exercise caution and verify sources before clicking any link. Your careful consideration could thwart potential cyber threats.

- **Use Strong Passwords & Managers**
  Craft sturdy, unique passwords and consider employing a password manager. It’s the digital equivalent of safeguarding your valuables in a high-security vault.

### 3. Use Safe Methods for Purchasing: Secure Your Financial Transactions
When it comes to transactions, adopting secure methods is non-negotiable:

- **Opt for Secure Payment Channels**
  Prioritize safety over expediency. Choose encrypted websites and secure payment options to shield your financial information from prying eyes.

- **Stay Vigilant**
  Regularly monitor your financial statements and promptly report any suspicious activity. A vigilant eye can detect and deter cyber adversaries.

As our university community spreads the holiday cheer, let’s fortify our digital defenses and shop with confidence. By integrating these cybersecurity practices into our shopping routines, we can ensure a joyous season without falling prey to cyber grinches.

Remember, a proactive approach to cybersecurity is the best gift you can give yourself this holiday season. Stay safe, stay savvy, and embrace the spirit of secure shopping!