Top 3: Security News in April 2023

1. **Microsoft Introduces Microsoft Security Copilot**
   [CSOOnline.com](http://CSOOnline.com)
   Microsoft’s new generative AI security system grafts GPT-4 into its security offerings for integrated analysis and responses.

2. **Jefferson County Schools Hit by Ransomware**
   [GovTech.com](http://GovTech.com)
   The second-largest public school system in Alabama has taken down its network systems while it works with outside cybersecurity experts and law enforcement to investigate whether data was compromised.

3. **Genesis Market Platform Seized by Police**
   [TheRecord.media](http://TheRecord.media)
   Genesis Market was seized on Tuesday in an FBI-led operation involving more than a dozen international partners, scuttling one of the most significant online criminal platforms.
**In Other (Security) News...**

**Security Alerts**

- **Multiple Google Chrome Vulnerabilities Could Allow for Arbitrary Code Execution**
- **Microsoft Internet Explorer Memory Corruption Vulnerability**

**Hackers Exploiting WordPress Elementor Pro Vulnerability**

Unknown threat actors are actively exploiting a recently patched security vulnerability in the Elementor Pro website builder plugin for WordPress, [Click to read more.](#)

**UK Bans TikTok from Government Mobile Phones**

Move brings Britain in line with US and Europe and reflects worsening relations with China, [Click to read more.](#)

**Bing Search Results Hijacked via Misconfigured Microsoft App**

Wiz researchers found that when creating an application in Azure App Services and Azure Functions, the app can be mistakenly configured to allow users from any Microsoft tenant, including public users, to log in to the application, [Click to read more.](#)

---

**Around Campus Update**

**MFA for Webcourses**

Starting May 8, all students, staff and faculty will be required to use Multi-Factor Authentication (MFA) to access Webcourses (Canvas).

In the University's ongoing efforts to enhance the security and maintain the academic integrity of our Higher Education institution, all students, staff and faculty will be required to go through the MFA process to access their Webcourses accounts.

**Students:** Students will be required to use Microsoft Authenticator - the same application used to protect Knights mail - to sign onto their Webcourses account.

**Staff and Faculty:** Most staff and faculty will be required to use DUO - the same application used to protect Workday and myUCF - to sign onto their Webcourses account. Staff who are currently enrolled in the 'Passwordless Authentication' pilot program will be prompted to use Microsoft Authenticator for Webcourses.

For questions, please reach out to Joshua Thomas (joshua.thomas@ucf.edu).

---

**DUO Enrollement Guide**

**Microsoft Authenticator Knowledge Base Article**

---

**UCF Info Sec Office**

Contact: [InfoSec@UCF.edu](mailto:InfoSec@UCF.edu) | [Twitter: @UCF_InfoSec](https://twitter.com/UCF_InfoSec) | University of Central Florida