THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Office of Research Security Newsletter

February 2021

Happy New Year! ORS is wishing everyone a great 2021!

UPDATES FROM ORS

- ORS has had many questions pertaining to the status of an individual's clearance. If you are unsure of your clearance status (clearance granted, interim clearance, etc.), please contact ORS for verification. Keep in mind if you are receiving this newsletter you have been granted a clearance.
- Contractors are no longer able to escort visitors (even if you have a CAC) on any Military Installation. All visitors must be entered into the Visitor Management System (VMS) by a Government Sponsor and processed through the Visitors Center for badge access. For additional information, please contact ORS.
- Be sure to report a new marriage, divorce, if you have relocated/moved, etc.
- If you receive any emails that are questionable/raise red flags, please forward these emails to ORS and expand the header of the email. If you are unsure if it needs to be reported, REPORT IT!
- Annual ORS required trainings to be completed: CITI Export Control, Insider Threat and 2021 Annual Security Refresher trainings. Be on the lookout for the training emails.

INTELLIGENCE THREATS & SOCIAL MEDIA DECEPTION

Office of the Director of National Intelligence | The National Counterintelligence and Security Center

Do you want to connect? Understand that foreign intelligence entities and criminals routinely use deception on social media platforms to try and connect with people who have access to information they want. Before you link online with someone you don't know, think about the risks it may pose to yourself, your family, your organization and even national security.

The FBI and the National Counterintelligence and Security Center (NCSC) have released a new movie, "The Nevernight Connection," to raise awareness of how hostile actors use fake profiles and other forms of deception on social media to target individuals in government, business and academic communities for recruitment and information gathering.

Inspired by true events, the 30-minute video details the fictional account of a former U.S. Intelligence Community official targeted by a foreign intelligence service via a fake profile on a professional networking site and recruited to turn over classified information.

On professional networking sites and other social media platforms, hostile actors routinely pose as headhunters, interested employers or people with enticing career opportunities in order to connect and develop relationships with people who have access to valuable information.

Read the full article:
https://www.dni.gov/index.php/ncsc-features/2780%E2%80%A6

SECURITY IMPLICATIONS OF FOREIGN FUNDING AND ACCESS AT U.S. COLLEGES AND UNIVERSITIES

Kaylee Cox Bankston, Richard Hartunian, Scott Lashway, & Matthew Stein | JD Supra | December 9, 2020

While global media outlets have focused attention on election security, major U.S. healthcare facilities have been under direct cyberattacks in recent months. This follows disruptive cyberattacks on municipalities earlier this year. These attacks, and the often short news cycles around them, underscore the reactive attention to threats and the inability to foresee or prepare for emerging threats. Too often, industry verticals and their participants use the "not us, we're too small" approach to security preparedness.

The next emerging threat—which in our view is already present—is to U.S. higher education, a big business due to its ability to generate new industries and technology from the ground up (e.g., social media). Like healthcare facilities and research organizations, higher education institutions and their electronic infrastructure are built for collaboration, which exposes a soft underside to threat actors. This presents serious security risks to the U.S. higher education sector and, in a larger sense, to U.S. national security interests.

Read the full article:
https://www.jdsupra.com/legalnews/security-implications-of-foreign-57716/

OFFICE OF RESEARCH SECURITY STAFF

DENISE SPILLER
Security Administrator
824-6444, denise.spiller@uah.edu

JANINE WILSON
Associate Security Administrator
824-3025, janine.wilson@uah.edu

APRIL MCMEANS
Assistant Security Administrator
824-6048, april.mcmeans@uah.edu

CAITLYN SCHOENIG
Security Assistant
824-4717, caitlyn.schoenig@uah.edu

RYAN WILKINSON
Student Specialist I
824-4818, ryan.wilkinson @uah.edu