Ben

[**Weekly Relays User Guide**](https://ispace.utmb.edu/xythoswfs/webview/_xy-12470404_1)

**TOPICS LEGEND**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| C:\Users\krhensle\Desktop\SMALL LOGO (2).jpg | | WEEKLY RELAYS | | **April 6, 2023** |
| **YOUR DEPARTMENT NEWS** | | | **UTMB NEWS** | |
| **OEA Does Stop the Bleed Training**        OEA learns life-saving techniques!!  OEA learns life-saving techniques!!      **OCE in Action!**  IMG_4883.jpg    OEA learns life-saving techniques!!    IMG_4879.jpg  IMG_4878.jpg  **SNMA Fundraiser** | | | **MONTHLY CYBERSECURITY UPDATE**  **How Are We Doing:** During March, 4.2% of recipients opened an attachment or revealed credentials in simulated phishing attacks initiated by the Office of Information Security. Our goal is less than 3%. A breakdown of department success and failure rates can be found at [https://utmb.us/66g](https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2Futmb.us%2F66g&data=05%7C01%7Ctrallyn%40utmb.edu%7C90d233b966b642166a8e08db3619c93b%7C7bef256d85db4526a72d31aea2546852%7C0%7C0%7C638163256595051283%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=pujDl7JGNd0ozGPCg2KUSfc%2BaAhUhdgB%2FQ5EXa%2BBHr8%3D&reserved=0). Learn more about cybersecurity at <https://www.utmb.edu/infosec> and report potential phishing to [cirt@utmb.edu](mailto:cirt@utmb.edu).  **Insider Threats (We are not pointing fingers—OK, we are pointing fingers)**  Insider Threats are defined as potential risks introduced, initiated or perpetrated by users within the organization. Insider threats are especially troublesome due to the threat actors (institutional users) already having established access within the protected network, systems and/or data sets; threat actors circumventing established, documented security controls; and, threat actors having signed and acknowledged Security and Non-disclosure Agreements indicating they are aware of and will follow the established security controls.  Insider threats can be the result of negligence, mistakes or deliberate action (or a combination of the three); however, the results of the threat becoming a real risk are the same.  The most common insider threats seen at UTMB include:   1. Insecure device configurations: Devices (servers, desktop, and mobile) are not properly configured, or maintained and upgraded to properly protect the system, the data within, or UTMB’s networks. 2. User account compromises: Falling victim to phishing attacks; even willful, deliberate password and session sharing (allowing a user to use or access resources under a different login) have been reported. 3. Lost or stolen mobile devices: Unsecured mobile devices are frequently lost or stolen. A common scenario includes laptops being stolen from cars at the user’s home. 4. Administrative access abuse: Users misuse their legitimate administrative access to their computer to install (or allow to be installed) unapproved, inappropriate software, or to disable or modify security controls, such as anti-malware scanning, event logging or data encryption processing.   Commonly cited reasons or excuses for threatening actions include:   * Lack of knowledge or understanding of security policy or the potential impacts resulting from or consequences of an actual security event * Desire to expedite work processes (do things more quickly or easily) * Belief that information security is “someone else’s job” | |
| OPICS  LEGEND | PATIENT CARE EDUCATION & RESEARCH INSTITUTIONAL SUPPORT CMC | | | |
| **AROUND UTMB** (Use the legend above to quickly find items of interest to your team) | | | | |
| **MONTHLY CYBERSECURITY UPDATE (cont.)**  Potential impacts of an insider threat becoming a real event include:   * Malware or ransomware infection * Loss of use or denial of service for mission-critical functions * Data breach or loss of control * Civil or criminal litigation, including sanctions and/or fines * Loss of contracts, business and reputation * User discipline (up to and including termination)   All UTMB users need to accept and acknowledge their role in protecting the critical resources (including data) needed to complete UTMB’s mission. UTMB’s security policies and practice standards are available online at <https://www.utmb.edu/infosec/resources/policiesstandards>. If you are uncertain about a situation or need further clarifications regarding any security control, please ask. UTMB’s Office of Information Security and the Security Operations Center are available via email at [cirt@utmb.edu](mailto:cirt@utmb.edu) or [ISOC@utmb.edu](mailto:ISOC@utmb.edu). Please don’t be the insider whose threat becomes a real event.  **REMINDER:**  **April 14 UTMB Health Earth Day Celebration and Recycle in Style Fashion Show**  Join us on Friday, April 14, from 11 a.m. – 1 p.m. for UTMB's annual Earth Day celebration in the Moody Medical Library Plaza on the Galveston Campus. This year’s theme is “A Tree Saved is a Future Earned.” Come by and visit the many exhibitors, enjoy music and food, meet our keynote speaker Dr. Deborah Jones, listen to Mayor Craig Brown’s Earth Day proclamation, and watch the Recycle in Style Fashion Show. UTMB’s Care Closet will be accepting donations, such as non-perishable food items, hygiene items and clothing. For more information, visit <https://www.utmb.edu/earthday> or <https://intranet.utmb.edu/care-closet>. | | | **IN CASE YOU MISSED IT:**  **March 30 Thought Leader Series—The Lunar Mars Surface Integration Facility and New Lunar Economy**  Presented by UTMB Health and introduced by C. Aaron LeMay, vice president and interim chief business and finance officer, the March 30 Thought Leaders Series explored the lunar economy and discussed the new lunar Mars surface integration facility. The technology and infrastructure needed to prepare the moon as a life-sustaining gateway to Mars provides tremendous possibilities for private industry and government partners to work together and thrive. Space has always been a catalyst for innovation, and it’s reasonable to anticipate a surge in discovery and development in communication, construction, food science and health care, among others. To watch the rebroadcast, visit [https://utmb.us/8nl](https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2Futmb.us%2F8nl&data=05%7C01%7Ctrallyn%40utmb.edu%7C90d233b966b642166a8e08db3619c93b%7C7bef256d85db4526a72d31aea2546852%7C0%7C0%7C638163256595051283%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=SAVOJRnheWx587n1f1Z41sDTAGGVyJQGgoXtaXh7NkE%3D&reserved=0).    **PATIENT CARE**  **Heartbeat newsletter—call for content**  There’s still time to share your favorite recipe, photos (from work or home), kudos and congrats for the April issue of the Health System Heartbeat newsletter. Email information to [mmbattis@utmb.edu](mailto:mmbattis@utmb.edu). | |
| **DID YOU KNOW?**  On Sunday, April 2, UTMB Health participated in IRONMAN 70.3 Texas as the official medical provider for the prestigious competition, which combines swimming, biking and running. UTMB Health staff and students provided medical care and event-related support to more than 2,000 athletes from around the world. Volunteers from Physical Therapy, Galveston Emergency Room, Family Medicine, Orthopedics, School of Nursing, League City Campus Cancer Center, Point of Care Testing, Transportation, Supply Chain and Pharmacy Services made the event a success. For more information, visit <https://utmb.us/8nk>. | |