Remote Home/Office Cybersecurity Preparedness Workshop

On June 14th, the University of Memphis' Center for Information Assurance (CfIA), in collaboration with UMRF Ventures, hosted a proctored session for the FEMA certified course entitled—Remote Home/Office (RHO) Cybersecurity--developed by CfIA as a member of the National Cybersecurity Preparedness Consortium. Participants included professionals from companies such as Raymond James, Sedgewick, MLGW, Methodist Le Bonheur, and System Analytics.

Ensuring strong cybersecurity practices at home and in office environments is vital as remote work grows. The training highlighted the vulnerabilities of remote workers using personal devices and less secure home networks, which are

susceptible to phishing, malware, and data breaches. It emphasized the need for comprehensive cybersecurity training and stringent security controls, such as multi-factor authentication (MFA), virtual private networks (VPNs), and regular software updates.

The course covered essential practices like recognizing phishing attempts, creating strong passwords, and securing home networks. By regularly implementing cybersecurity training, using MFA, VPNs, and ensuring software updates, remote workers can significantly enhance their cybersecurity, protecting sensitive data and maintaining operational integrity. The proctored session was a great success with 54 completions (out of 75 participants) of the RHO course as part of FEMA cybersecurity online training.