IT Systems Recovery Plan

HU Communications <ouc@howard.edu>
Sat 9/11/2021 10:36 PM
To: Alfred, Marcus <marAlfred@Howard.edu>

View this email in your browser

Enterprise Technology Services (ETS)

September 11, 2021

Dear Howard University Community,

We are writing to make you aware of our IT Systems Recovery plan for tomorrow, Sunday, September 12.

Throughout the day, ETS and our IT partners worked to ensure stable network connectivity, further network segmentation, and harden our cyber security posture.

Today, Howard University stakeholders with access to sensitive data were provided with Yubikeys as an added security measure meant to protect access to the network, systems, applications and data. This effort will be ongoing until all customers in this category are served.

Other stakeholders with elevated user access will receive notifications on the new manner in which apps containing sensitive information will be accessed. To maintain optimum security, these users will be contacted directly. No details will be shared in this communication.

We are working on a mechanism to send push notifications for password resets to students, faculty and staff, to avoid the need for you to sit with an IT professional to do hard password resets. There are a few ways in which this can be accomplished remotely, but it has to be completed within the framework of the University's risk posture management. We will share more information in a future communication.

When the need arises for our stakeholders to present to campus for IT related triage, the ETS team will inform you to do so via an HU Communication.

Stakeholders who need to present to campus tomorrow have already been contacted. If you did not receive a notification, then you are not expected to meet with an ETS professional as yet for any remediation efforts related to the September 3 cyber attack.

CRITICAL THINGS EVERY HOWARD UNIVERSITY STAKEHOLDER MUST DO:

- Please unplug all laptops, desktops and external hard drives from the Howard University network. We are in dire need of every person in the organization who has a dormant desktop device to come to campus to unplug the device. If the device has encrypted files, please bring it in to the ETS team located at the iLab at Wonder Plaza. We must quarantine all devices that have encrypted files on them.
- Read all HU Communications and follow the directives included within at the requested time.
- Do not click on suspicious emails. There have been a significant increase in phishing emails and spoofs. Please read the details here regarding practices for Safeguarding Against Phishing.
- We are asking managers to maintain a list of alternate email addresses and mobile phone numbers for their faculty and staff in the event

alternative contact information is needed.

- Please contact your key direct reports via phone to convey critical messages as needed.

We recognize that a dynamic incident response may cause some of our stakeholders to experience a heightened level of anxiety. We are asking for your patience and understanding as we navigate the University's recovery together.

Excellence in Truth and Service,
Enterprise Technology Services (ETS)

Enterprise Technology Service
2301 Georgia Avenue, NW, Suite 334
Washington, DC 20059