Mandatory Instructions from ETS Concerning Device Triage

HU Communications <ouc@howard.edu>
Wed 9/8/2021 11:09 PM
To: Alfred, Marcus <marAlfred@Howard.edu>

View this email in your browser

Enterprise Technology Services (ETS)

September 8, 2021

Dear Howard University Campus Community,

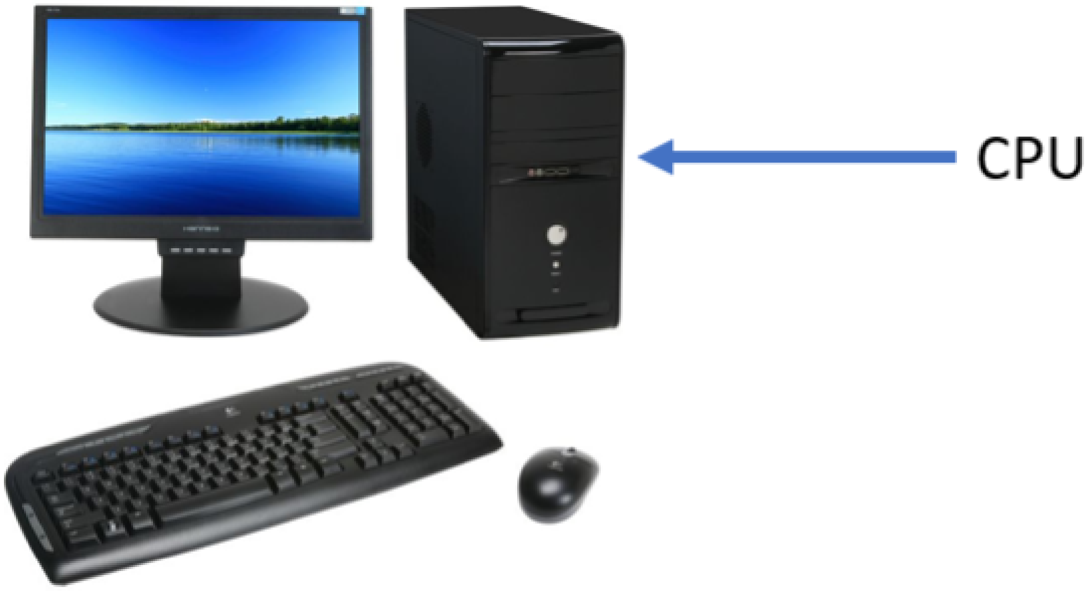
We are writing to share guidance on the process the University will be taking to triage all Howard University devices of interest that may have encrypted files, associated with the September 3rd cyberattack, and the priority in which we will be doing so.

ETS has set up a triage center at the Undergraduate Library (UGL), where all University personnel must bring in devices outlined within this communication,

so that we can conduct inventory on all compromised equipment.
We are amidst the first phase of our triage process. There will be additional phases, and they will be announced over the coming days and weeks.

It is critical that you read this message in its entirety, and follow the instructions as outlined.

If you have a workstation or a desktop, **you are required to bring the Central Processing Unit (CPU) and power cord** to the Undergraduate Library. The Central Processing Unit is the main device where the computing operations are controlled and executed. An example of a workstation/desktop is below. The blue arrow to the right in the image below is directly pointed at the CPU.



Some computers have CPUS and monitors that are integrated into one piece of equipment. Please bring the entire device to the UGL.

All University personnel, especially personnel who have a workstation or desktop are being asked to come to campus tomorrow, September 9th, in order to unplug their equipment and take their CPUs to the Undergraduate Library.

If you have a laptop that you know has files that have been encrypted in association with the September 3rd cyberattack, please bring it to the UGL.

How will you know when files are encrypted?

In relation to this cyber breach, and the pattern we have seen, when an employee’s computer is started up, two common ways to know if a user’s files are encrypted are outlined below:

1. The user may see a “Read Me – To Unencrypt” file saved on your desktop
2. Files saved on a user’s hard drive may be titled “**Encrypted**”, followed by an unintelligible file name, with accompanying numbers.

PLEASE DO NOT CLICK ON ANY FILES.

At this time, we know that the majority of devices impacted are desktops, but no devices are immune to the cyberattack. The triage process will help ETS to triangulate data that has already been collected remotely, using our monitoring systems.

If an employee has an ambulatory issue that prevents them from transporting a device to the Undergraduate Library, please send an email to HUDesktop@howard.edu, with the subject “Device of Interest Notification”, and ETS will assist.

In this phase of triage, please do not bring the following devices to the UGL:

- Servers
- Phones
- iPads
- Tablets
- Monitors
- Keyboards
- A Mouse
- Laptops without encrypted files related to this incident

If you are a researcher, and you have a lab that contains servers or other large equipment/devices that have files that you think may be encrypted, please take a picture of your device, and send an email to HUdesktop@howard.edu with the subject title “Device of Interest Notification”.

HOURS OF OPERATION

- The ETS team will be on site at the Undergraduate Library starting at 10AM until 3PM on September 9th. Employees will be met at the entrance and escorted to the triage area.

- Please bring your University ID **and** an official government ID.

Be prepared to provide your User ID and password for your device as they will be needed for remediation. As part of the recovery effort, ALL passwords will be changed within the constraints of the University's new security requirements. **PLEASE DO NOT CHANGE YOUR PASSWORD PRIOR TO COMING TO THE UGL.**

All University personnel will be issued new laptops. We will do so at a later date, after devices are imaged, and security features are installed.

If you have any questions or concerns about this, ETS representatives will be on site to answer them when you drop off your device.

Please remember to follow the University's health protocols and wear a mask at all times when indoors and outdoors.

It is critical to note that the university is still amidst a cyber incident, and as such, we are asking our stakeholders to be diligent, and read all communications sent to you, and act upon the instructions given when asked. We need the assistance of our entire organization in order to execute the University's dynamic response to the cyberattack.

Thank you kindly for everything you have been doing to assist our University amidst the current incident. Your support and patience are much appreciated.

Excellence in Truth and Service,

Enterprise Technology Services (ETS)

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

This email was sent to marAlfred@Howard.edu
why did I get this? unsubscribe from this list update subscription preferences
Howard University · 2225 Georgia Ave NW · Washington, DC 20059-1014 · USA