Safeguarding Against Phishing

HU Communications <ouc@howard.edu>
Sat 9/11/2021 12:25 AM
To: Alfred, Marcus <marAlfred@Howard.edu>

View this email in your browser

Enterprise Technology Services (ETS)

September 10, 2021

Dear Howard University Community,

As we continue to keep you informed on the status of our Internet and technological infrastructure, we want to update you with an urgent notice regarding email and credential password resets, and scam attempts that have been reported in recent days.

MANDATORY PASSWORD RESET

We have performed a “golden ticket” password reset for the entire organization. ETS will need to share your password with you in order for you to gain access to any of our systems. Then, while in the presence of an IT team member, you will reset your password once more. This means that every user in the campus community will need to meet with the ETS team to reset their password. This exercise will start on Sunday, September 12 at 11 a.m. in the Undergraduate Library. We will share detailed instructions via an HU Comm on what to expect. All students, faculty and staff should be prepared to come to campus on Sunday to complete your password change, if possible. Otherwise, you will not be able to access any of Howard University’s systems on Monday and beyond. We will share separate instructions for remote students, faculty and staff.

SYSTEM UPDATES

To protect our University’s IT systems, we have taken a variety of measures to safeguard against illicit or illegal access:

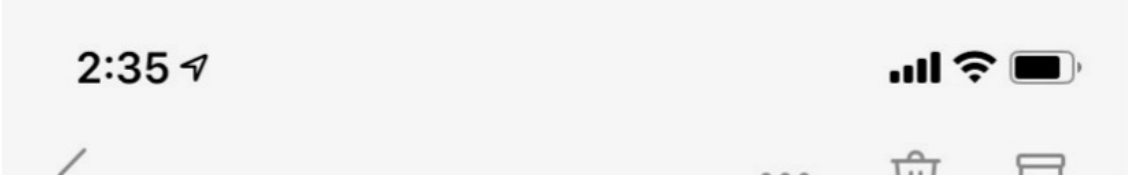
- No emails can be auto-forwarded from @bison.howard.edu or @howard.edu email to gmail, yahoo, aol or any other private email hosts at this time.
- We have disconnected all user access to most of our applications like Workday, Blackboard, Bison Web and others.

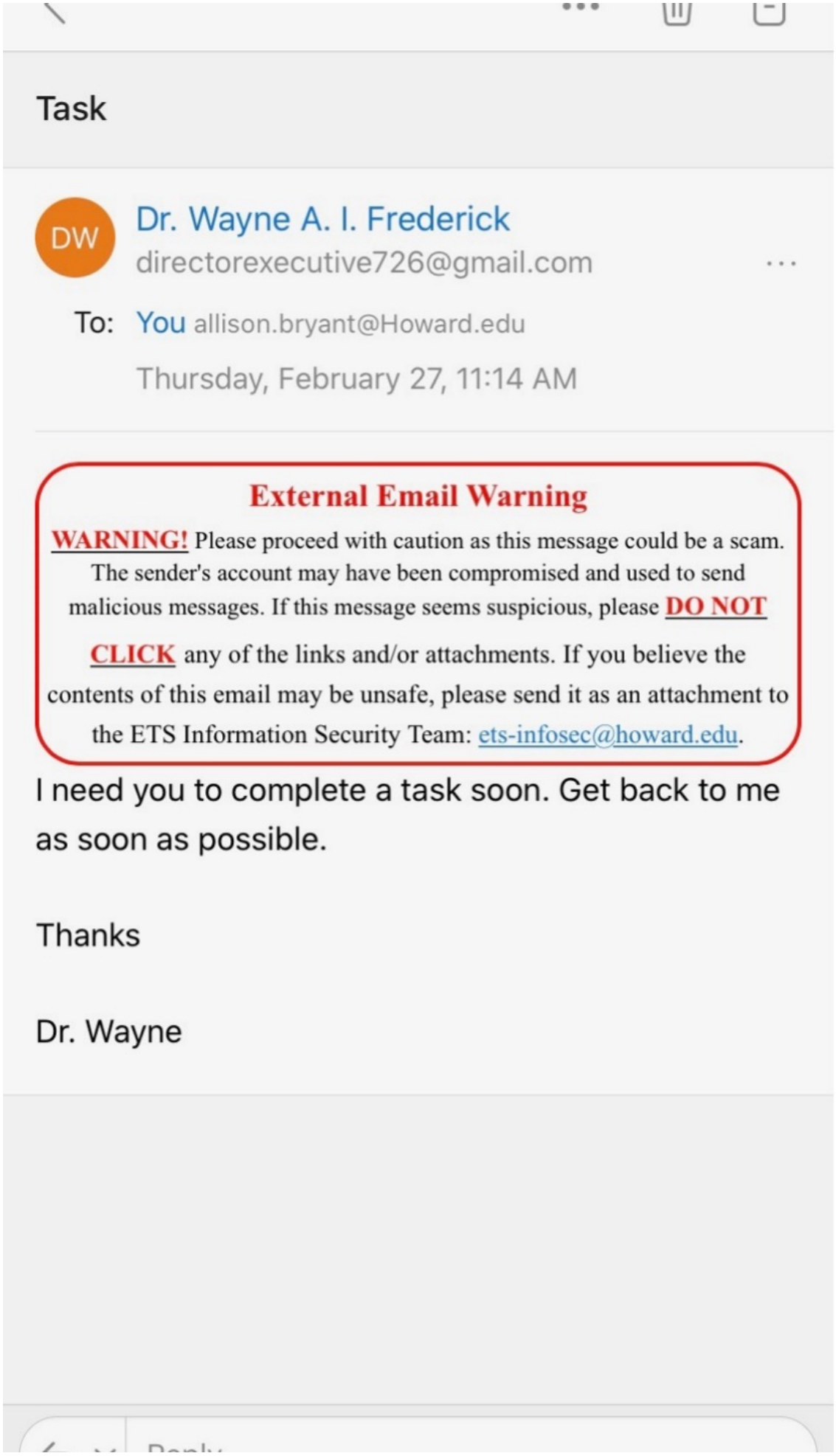
PHISHING SCAM ALERTS

The University is seeing a significant uptick in phishing attempts targeting students, faculty, and staff. Please do not click on links embedded within emails that appear to be suspicious. Do not reply to emails that look suspicious and do not forward them to anyone.

An example of a phishing attempt is below. The email appears to be coming from our University President, Wayne Frederick, but it is not:

There are a few ways that you can tell this email is suspicious:





Task

DW

Dr. Wayne A. I. Frederick
directorexecutive726@gmail.com

To: You allison.bryant@Howard.edu

Thursday, February 27, 11:14 AM

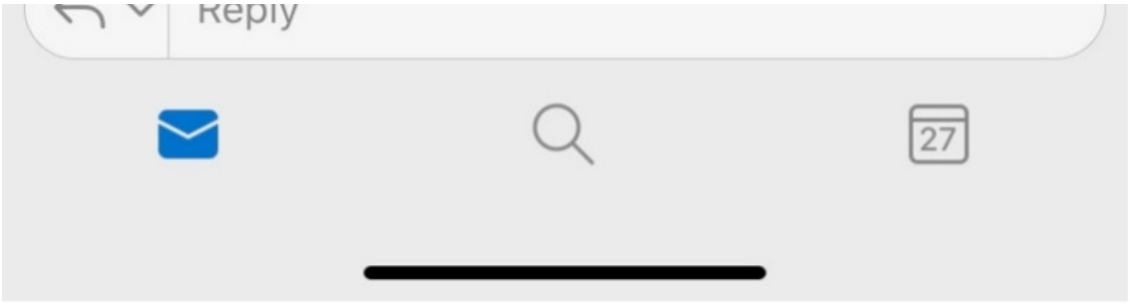
External Email Warning

WARNING! Please proceed with caution as this message could be a scam. The sender's account may have been compromised and used to send malicious messages. If this message seems suspicious, please **DO NOT CLICK** any of the links and/or attachments. If you believe the contents of this email may be unsafe, please send it as an attachment to the ETS Information Security Team: ets-infosec@howard.edu.

I need you to complete a task soon. Get back to me as soon as possible.

Thanks

Dr. Wayne



1. The language in the red box is the first indicator that this is an external email, and not an internal email. This red box should alert you to look closely at the sender, subject and email address. Treat all external email in a suspicious manner.
2. President Frederick uses his Howard University email address when conducting University business. Neither he, nor any official within the University, will use a personal or non-@Howard.edu email address to communicate with you.
3. Most phishing attempts will be obvious through context clues in sentence structure or language. President Frederick does not send emails to anyone signed by “Dr. Wayne” and maintains respect for recipients by writing in a formal business structure and tone.

If you receive an email like this, immediately report the incident to ets-infosec@howard.edu. Do not forward the email. Do not click on links embedded within it.

PERSONAL INFORMATION SCAMS

Cybercriminals are using numerous types of fraudulent emails to steal personal information and commit crimes of fraud or identity theft. Some of them look like they are coming from trusted sources within legitimate businesses. Please always remember: If something seems too good to be true, it probably is.

Often, students fall victim to CashApp traps or emails where someone asks them to send their banking information so that they can deposit money into their bank accounts.

DO NOT GIVE OUT YOUR BANKING INFORMATION VIA EMAIL, or to anyone who you do not know or trust.

Although Howard University maintains a system of controls to help protect our personal information, networks, and computers from cyber threats, we rely on you to be our first line of defense. No entity is completely immune to a

cyberattack. Continue to be vigilant and use the helpful security information and resources that Enterprise Technology Services (ETS) provides.

IMPORTANT TAKEAWAYS

- Howard University will never ask for your password or other sensitive information in an email.
- Just because an email appears to be from a trusted internal sender, that doesn't mean it isn't a scam.
- If a message has an external email warning embedded, that's a clear indicator that the email didn't come from an internal Howard University sender.
- Cybercriminals will use compromised email accounts to send out phishing attempts. Make sure every password is up to the University's new standards (15 alphanumeric characters long, with one capital letter and a special character). Each password should not be repeated. Or re-used on any other non-Howard University site.
- If there is an email that seems suspicious, but you are not sure, attempt to verify it first by using other means to contact the sender.

If you have been affected by a cyberattack or scam, immediately contact the ETS Information Security Team at ets-infosec@howard.edu to report it. Thank you for your vigilance and continued support.

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

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