HARVARD
Financial Administration
RISK MANAGEMENT AND AUDIT SERVICES

Date: February 2021
Subject: Fraudulent Email Activity Notice

Fraudulent Activity by Persons Posing as Harvard Procurement Staff

Please be aware that there has been an uptick in fraudulent Harvard purchase orders / requests that have been sent to external vendors, often with forged attachments. The purchase orders / requests fraudulently represent that they are coming from "Harvard Procurement" staff and often are inquiring about the purchase of branded marketing items (backpacks, water bottles, etc.) or asking vendors for sensitive tax information. While vendors have been reaching out to Harvard contacts to verify the legitimacy of orders, some vendors have experienced losses as a result of the scheme.

Notice to Vendors: Always ensure that a purchase request has come from a legitimate Harvard email or individual. If unsure, contact a known Harvard email or phone number. If you are the victim of fraudulent activity, please contact your local law enforcement.

Notice to the Harvard Community: If a vendor asks for confirmation of a Harvard purchase request, please review the request for legitimacy and alert RMAS Fraud Alert at RMAS-FraudAlert@harvard.edu if you have reason to think the request is illegitimate.

Examples

Fraudulent requests/emails could come from domains similar but not limited to @harvard-edu.net, @harvard-educ.com, @harvardd-edu.com, @harvardcollege-edu.com, harvard-edu@financier.com, or harvard_eduinfo@aol.com.

Valid Harvard email addresses ALWAYS end in 'harvard.edu' or 'hbs.edu'. (e.g. john_harvard@harvard.edu or jharvard@fas.harvard.edu)

Characteristics of Common BEC/EAC Schemes

Please be sensitive to additional types of attempted Business Email compromise / Email Account Compromise (BEC/EAC) schemes.

- Targeting businesses and individuals who perform legitimate transfer of funds requests
- An urgent need or attempt to conduct unauthorized transfer of funds or sensitive data, e.g., requesting a change in wire transfer details
- An unexpected inquiry from a vendor looking for confirmation of orders for physical and/or branded goods, e.g., procurement fraud
- Often sent from accounts appearing to be valid (e.g., John_Harvard.harvard.edu@outlook.com) or compromised Harvard emails

Harvard community members, please contact RMAS-FraudAlert@harvard.edu if you become aware of these types of emails, either through direct receipt or outreach from a vendor.

Other suspicious emails should be forwarded to phishing@harvard.edu. For more information about Phishing, please visit HUIT Security.