July 6, 2022

Greetings from your Information Systems and Technology Team!

Please take a moment to review some important technology updates highlighted below. If you have any questions or would like more information on these or other technology related topics please do not hesitate to reach out to technology@udallas.edu.

Your UD Technology Teams

Network & Infrastructure

The network and infrastructure team manage the connectivity of IT systems on and off campus. They design, install, and maintain systems for core functionalities - such as internet connectivity, telecommunications, and security.

User Support Services

The user support services team is responsible for maintaining the university's desktop and environment, engaging in the troubleshooting of technical issues with end-users. They also manage user accounts for email and general systems access.

Admissions Information Systems

The admissions information systems team manages the student and HR application system, Slate. They manage system information and data flow for the purposes of the student lifecycle, employee onboarding, and enrollment management.

Information Systems Team

The Information Systems team manages the core information system, Ellucian Banner, and its affiliate connections to other applications across campus. This team also manages data reporting to internal and external stakeholders.

Additionally, our department org chart can be found on the About IT page.

Types of Phishing

We have recently seen an increase in phishing (email) and SMishing (text message) attacks. Below is a brief explanation of some of the different types of cyber-based attacks.

Phishing – An email designed to trick the recipient into providing sensitive information like a password, or performing an action like downloading a malicious attachment or clicking a spoofed link. Use the Phish Alert Button (PAB) in your udallas email account to securely report any suspicious message directly to our office.

SMishing – Phishing through SMS or text message. Messages will be similar to a phishing email with a malicious link and/or an urgent request. Often the number will be new or unknown. If the message seems suspicious, use a secondary method (phone call or in-person communication) to confirm the legitimacy of the message.

Vishing – “Voice Phishing” using a phone to steal information by pretending to be a trusted individual, or authoritative institution like a bank or hospital.

Phish Alert Button - Now in Outlook

We have now launched the Phish Alert Button (PAB) to Outlook users as a way for UD faculty and staff to safely report potential phishing attempts to our department. If you suspect an email is a phishing attempt please do not hesitate to notify our department using the Phish Alert Button. More information on the PAB button for Outlook can be found on the KnowBe4 Knowledge Base Page.

If you have a KnowBe4 cyber training account, supplemental training on the Phish Alert Button can be found on the KnowBe4 training website, https://training.knowbe4.com/ui/login under the "Library" header. If you have any questions about the Phish Alert Button or are missing the license key please email technology@udallas.edu.

Questions

If you have any questions or would like additional resources on these topics please reach out to technology@udallas.edu or the UD Help Desk at