

UNIVERSITY OF DALLAS

Information Systems and Technology

January 12, 2022

Happy New Year from your Information Systems and Technology Team!

As we begin a new year we would like to take this opportunity to highlight some new technology features and a few security reminders. It is our hope that this information will help you work safely and efficiently with campus technology.

New Year, New Password - Change and Reset Passwords

It is recommended practice to change all your passwords every 90 days to increase security. If this is not your current practice, we recommend using the new year as a recurring reminder to update your older passwords.

Available to all UD faculty and staff, Microsoft Azure allows you to set-up multi factor authentication and change/reset your password as needed. Instructions for setting up multi factor authentication and the steps to reset your password can be found on the UD website in one easy to follow instruction guide. Feel free to bookmark this page or download a copy for quick reference: https://www.udallas.edu//offices/technology/_documents/Multi-Factor-and-Password-Reset.pdf

New Practice - Google Drive and Sharing Files

Google offers the ability to work collaboratively through the utilization of Google Drive. Within Google Drive you have the ability to create and securely share folders, documents, spreadsheets, slides, and forms. It is preferred practice to use programs like Google Drive over unsecure programs like email to share sensitive information. Please visit the Google site for more information on how to create and share using Google

Drive, <https://support.google.com/drive/answer/2494822?co=GENIE.Platform%3DDesktop&hl=en>.

New Feature - Phish Alert Button

In October we launched the Phish Alert Button as a way for the UD faculty and staff community to safely report potential phishing attempts to our department. The Phish Alert Button (PAB) allows you to forward email threats safely and securely to our team for analysis, and deletes the email from your inbox to prevent future exposure, all with a single click! If you suspect an email is a phishing attempt please do not hesitate to notify our department using the PAB



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 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, support@udallas.edu.
