Two-Factor Authentication (2FA) FACT SHEET

PHISHING SCAMS AND OTHER METHODS OF STEALING PASSWORDS CONTINUE TO PUT UW SYSTEMS AND DATA AT RISK. USING 2FA SECURES UW DATA AND PROTECTS STAFF AND FACULTY FROM POTENTIAL FRAUD.

OVERVIEW

- In 2016, thousands of UW email addresses were effected by phishing scams. Increasingly, these phishing scams target our community to steal UW NetID passwords for the purpose of tax fraud.
- Over 3,700 UW NetIDs were compromised and disabled last year.
- Since the late 80's, the UW has used two-factor authentication (2FA) to protect UW administrative systems. While these uses of 2FA have been effective in reducing risk, they're limited to users with access to the most sensitive systems and data.
- In the spring of 2017, UW-IT is rolling out a new 2FA solution from Duo Security. It expands 2FA to all faculty, staff, and student employees who sign in with UW NetID to access systems protected by two-factor authentication, including Workday.

TWO-FACTOR AUTHENTICATION

Two-factor authentication (2FA) adds a second layer of security when signing in with your UW NetID. Without 2FA, only a password is needed to sign in. 2FA adds a second factor, like a mobile phone or other device, to prevent others from signing in as you, even if they obtain your password.

Because two-factor authentication mitigates the risk of stolen passwords, it's an effective response to current threats to UW systems and data, including employee information managed in Workday.

In the future, many systems accessed by UW NetID will take advantage of 2FA. It's becoming the norm for doing business online.

USING 2FA AT UW

At the UW, all employees can enroll in Duo for two-factor authentication (2FA). Self-service enrollment will be available on Identity.UW (identity.uw.edu) in early April, where you can choose your mobile phone, tablet, or landline as a second layer of security. Some hardware tokens will also be available from UW-IT.

Most people choose to enroll their mobile phone or tablet by downloading the Duo Mobile application. It's free, secure, and simple to use.

Once enrolled, you can sign in using 2FA whenever it's required, including each time you sign in to Workday.

When you sign in using 2FA, your options depend on what kind of device you enrolled. The most common sign-in options include:

- "Send Me a Push" – Duo sends a notification to the Duo Mobile app on your mobile phone or tablet. You then tap "Approve" to sign in.
- "Call Me" – Duo calls your mobile phone or landline. Press any button to approve.
- "Enter a Passcode" – Enter a passcode generated by Duo Mobile or hardware token. Or enter a bypass code provided by the UW-IT Service Center.

IMPLEMENTATION

Two-factor authentication (2FA) is coming in the spring of 2017 as UW-IT prepares for all employees to move to UW's new HR/Payroll system, Workday. Workday will be implemented on campus in June 2017.

Enrollment information for Duo will be available in April, and enrollment efforts will continue through June 2017. **In order to be prepared for Workday, we recommend that all UW employees enroll in Duo by May 31, 2017.**

MORE INFORMATION

More details on how to enroll in Duo will be available from UW-IT and HR/Payroll Program Readiness Teams in April 2017.

All phishing messages received by UW email accounts should be forwarded to help@uw.edu.