Information Technology News

May 2024

Did You Know?

Windows 11 is coming! Prepare to say goodbye to Windows 10.

Information Technology staff have been working behind the scenes in preparation for the transition of university computers from Windows 10 to Windows 11. As of March 2024, Microsoft's announced End-of-Life date (EOL) for Windows 10 is set for October 2025. After this End-of-life date, Microsoft will no longer provide security updates or bugfixes for the Windows 10 operating system.

IT staff are working diligently to prepare internal systems for deployment of Windows 11, with a tentative plan for a phased rollout in the following stages:

Summer 2024 – Final testing of Windows 11 within IT and other departments
Fall 2024 – Voluntary Windows 11 upgrade available in Software Center for WP employees
Spring 2025 – Newly imaged computers will have Windows 11 by default
Summer 2025 – All remaining computers (employees, labs, and shared computers) will be upgraded to Windows 11*

**One of the largest challenges with Windows 11 is that it has significantly stricter hardware requirements than earlier Windows versions. Generally, any university laptop provided from 2019 and later will meet the Windows 11 requirements. Computers that are more than 4 - 5 years old may encounter issues installing Windows 11.*

As was done with Windows 7, once the Windows 10 end-of-life date passes, IT will identify any university Windows 10 computers that remain on the campus network. As those computers will no longer be receiving security updates from Microsoft, they present significant security risks and will either be replaced or blocked from connecting to the campus network.

Important: How you can help the university prepare
While IT will be reaching out to departments in the coming months to discuss plans for older computers that cannot install Windows 11, we are asking for assistance with moving this process along. If you or your department have any older and unused (or little used) computers that you do not need, please open a Helpdesk ticket with the request type of Hardware – Disposal so that IT staff can properly remove the older computers from the university network and inventory. Reducing the amount of older, unnecessary computers will help to streamline the Windows 11 transition.

Please feel free to reach out to Information Technology if you have any questions. The recommended method is to create a new Helpdesk support ticket at www.wpunj.edu/helpdesk and indicate that your inquiry is related to the transition of university computers to Windows 11.

Windows 11

Technology Updates

Upcoming Changes to WPUNJ Login Experience

Information Technology is in the process of updating the way that WP employee accounts will login to various WPUNJ systems (including Office 365, Outlook, Office 365 desktop and web-based apps, OneDrive, all Microsoft mobile apps including the Outlook mobile app and more) as well as the Workday system.

As part of this transition, there are a few important changes to be aware of:

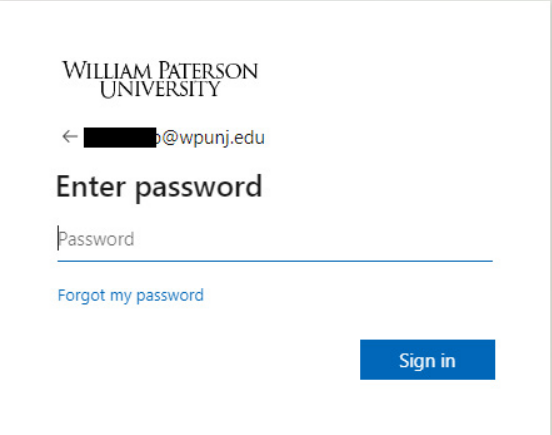
- When signing in to the listed systems, employee accounts will no longer be redirected to the orange and black 'adfs.wpunj.edu' login page. The login will be completed within Microsoft's login page.

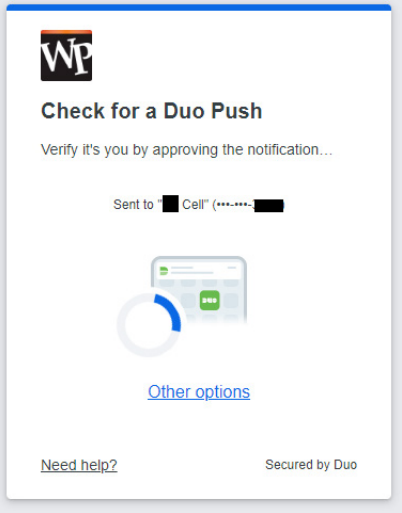
- The Duo multifactor authentication prompt will be changing the new 'Duo Universal Prompt.' You can view how the universal prompt looks compared with the current Duo prompt here.

- Once IT makes the change for all employee accounts (exact transition date to be announced,) you will be signed out of any applications where you are logged in and will be prompted to re-login or reauthenticate your account. This behavior is expected and part of the transition.

- The WPconnect (also known as Shibboleth) login will remain the same, though IT will gradually be transitioning various services over to the Microsoft-style login over the course of the next year.

We have put together an ITwiki article to highlight the changes, including screencaps of what to expect when this change is implemented. Please review so you aware are aware of what to expect. The exact date of the change will be announced via WP Announcements in advance of the transition date, though we are planning for a date shortly after the conclusion of the Spring 2024 semester.





Pharos Employee Printing Cost Center Change

With the transition to Workday for HR and financial operations, Banner FOAPs have been replaced by Workday Cost Centers. As part of that change, various university systems which use employee department and finance account information have been adjusted to use Workday Cost Center information.

One system yet to be updated to Workday Cost Centers is the Pharos system used for employee printing on Xerox. As many employees had Banner FOAP information manually assigned as Pharos Cost Centers, a decision was made to have this transition take place after the Spring 2024 semester concludes. Once Pharos has been updated to use the Workday Cost Centers, employees should see their Workday department/financial account information displayed as their available Cost Centers when printing from Xerox devices.

Should you have an issue with a Pharos Cost Center after this change, please submit a Helpdesk ticket (under the ticket type of Printing/Multi-Function Device -> Xerox) for additional assistance.

Cybersecurity Center

The following email message was sent out by Information Technology on Friday April 12, 2024.

As the email highlights the importance of individaul responsibility in protecting accounts, we felt it was a good reminder to include the email in its entirety.

From: WPUNJ IT Helpdesk
Sent: Friday, April 12, 2024 4:37 PM
Subject: Information on a cybersecurity incident (and your role in protecting your account)

William Paterson University employees and students,

We're writing to inform you of a cybersecurity incident that the university encountered earlier this week. The intent of this email is not to raise alarm but to help educate our employees and students on the continued need – and personal responsibility you have - for using caution before clicking on any links (or taking actions on unusual requests) in emails you may receive in your WPUNJ email account.

While what is shared below is lengthy, it's well worth your time to read fully so that you are aware of the potential personal repercussions of not using a careful eye when reviewing emails you may receive. While Information Technology staff do our best to put the proper security practices in place to establish protection of university accounts, it's important that you understand that your actions are the first line of defense in protecting both your information and university information. **In the situation described below, multiple individuals could have potentially had their paychecks stolen by cybercriminals if not for the diligent assessment and action taken by IT staff.** ***Note:*** The only individuals affected by this were those who fell for the phishing scam.

What Happened

On the evening of Sunday April 7th, Information Technology received several reports of a suspicious email claiming to be from the university's 'Health Center' with information about a possible Monkeypox exposure on campus. The message instructed recipients to click on an included link for more information about possible exposure. That link directed those who clicked to a fraudulent phishing login page which captured any usernames and passwords that were entered.

While investigating the reports, IT staff identified that the email was sent from a compromised email account at a separate university and was received by approximately 300 WP email accounts. Within 15 minutes of the reports and 45 minutes of the emails being received, IT staff had removed the malicious emails from all WP account inboxes that received the messages and blocked the target URL of the phishing link. IT staff also identified all individuals who had clicked on the malicious link and reached out to those individuals to let them know the email was a phishing scam and share actions they needed to take (changing their passwords immediately) if they had entered their login information into the page that loaded after clicking.

Early Monday morning (~6:45 am), the WP email account of one of the individuals who had clicked on the phishing link on Sunday night (but had not changed their password) was then used to send out a second round of similar scam emails to a larger number of WP email accounts. Once again, IT staff quickly identified the email and, prior to 7:30 am, took action to remove/block the email and notify anyone who had clicked on the link.

The Anatomy of the Scam and Why You Should Pay Attention

As part of the broader assessment and follow up on the incident, IT staff identified the following:

- The cyber criminals took the specific effort to design the fake webpage that loaded after clicking the phishing link so that it looked like an exact replica of the WPconnect login page. While this attack was targeted at William Paterson, it was not unique to William Paterson. IT staff have been in contact with staff at other institutions who have been experiencing similar attacks customized to their institutions.
- Once an individual clicked the link and entered login information into the fake login page, they were also prompted with a page designed to look like the Duo multifactor authentication login with a message that the Duo authentication had failed and a direction to open up the Duo Mobile app on their phone and enter the passcode displayed there. This action allowed the attackers to 'phish' the Duo passcode and allowed them to login to the individuals' accounts as they now had the individuals' WP usernames, passwords, and a valid Duo mobile passcode to compete the Duo authentication.

Cybersecurity Center

(email continued from prior page)

- After gaining access to the individuals' accounts, the attackers immediately took several actions including:
  - Adding a new mobile device (that they had access to) to the individual's Duo profile to allow for easier approval for future login request for the account
  - Setting up Inbox rules on the email accounts to automatically delete new emails with certain words and phrases
  - Logging in to the employee's Workday account and changing the bank account information on file to redirect the employee's direct deposits to another bank account that was under the cybercriminals control

Fortunately, IT staff were able to quickly identify the employees who had fallen for the scam email as well as the actions the attackers had taken, and we worked with the impacted employees and Payroll staff to make sure that their bank account details were corrected prior to the completion of this week's payroll.

While Information Technology staff will continue to do their best to identify these situations as they arise, it's important that it's understood that it ultimately comes back to individuals to best protect themselves from these types of scams.

Cybersecurity Tips to Keep in Mind

- Always check the email sender's email address and verify legitimacy before engaging with the content. And even the email is coming from a WPUNJ email, ask 'would this person be sending this request/information?'

- Use extreme caution before clicking any links and opening attachments, especially those prompting login actions or asking you to provide personal information.

- Be wary of unsolicited requests for sensitive information or unusual actions, even if they appear to come from within the university.

- If you receive unexpected Duo prompts or requests, do not approve them without verifying that it's you who initiated the login request. If something seems off with a Duo login or authentication, take a moment to fully review before taking action on the request.

- If you are an active student or employee who has not yet added Duo multifactor authentication to your account, we strongly recommend that you complete the enrollment process through WPconnect. Additionally, if your WP account password is the still the initial password you received and you have not changed your password to be a complex password (upper case and lower case letters, numbers, special characters, and at minimum of 8 characters in length, preferably longer) you should consider doing that soon.

- If you receive something suspicious, contact the university's IT Help Desk at www.wpunj.edu/helpdesk or (973) 720-4357 to ask for an IT staff assessment.

Information Technology staff continue to do our best to protect the university and our employees from cyber fraud attempts. With that said, the identification, follow up, and cleanup of issues that arise, often as the result of a 'quick click' without fully thinking first, is often incredibly time consuming and puts others in the WP community at risk of further cyber scams. We thank you and encourage your increased vigilance in helping maintain the security of both you own accounts and our university community.

Thank you.
The Information Technology team

Reminders

Improve Your Collaboration with Office 365's OneDrive and SharePoint:

Office 365's cloud-based storage allows for easier access to your files and improved collaboration. Employees who still use a campus network-based User Folder (or U: drive) for storing their documents can now request to migrate the files in their User Folders to their OneDrive. For more information on OneDrive and how to request a migration, read our announcement on requesting migration.

Departments can also request a SharePoint site for team-oriented work. SharePoint allows you to work collaboratively with colleagues on documents and files in a location that is similar to a cloud-based 'Group folder'. You can learn more about SharePoint in our ITwiki article. If you'd like a SharePoint site set up for a group or team you are working with, contact our IT Helpdesk to get that process started.

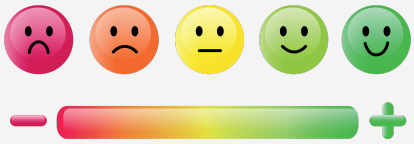
Where Are They Now?

The most magical place on earth has two greats from IT!

Max Kattermann, former Student Manager and Jason Mathew Rodriguez, former Technical Assistant have gratuated and were accepted in the Disney College Program at Walt Disney World. This is an awesome experience along the way to future careers in technology. It is no surprize that Max enjoyed time after class at the Whitman Gym Pool. "Working with IT allowed me to practice and understand the content taught in my courses." Jason's favorite times were working with other IT staff. "It was like having another family at school."

Picture by: Allison Murcaro WPU class of 2023 BA in Fine Arts

Please take our 2024 IT Satisfaction Survey



Access the survey by clicking the following link:

https://wpunj.qualtrics.com/jfe/form/SV_bdrf844UcGSStXU

Have technology questions or need assistance? The university's Information Technology team can be contacted through our IT Helpdesk ticketing system (www.wpunj.edu/helpdesk) or by calling our IT Helpdesk at **973-720-4357 (HELP)**. Additional information about the university's Information Technology team is available at **www.wpunj.edu/it.**