An OSU Call to Action on Cybersecurity

A recent phishing attack on OSU resulted in more than 500 compromised accounts. It demonstrated the incompatibility between the way IT systems and accounts are managed by OSU and the cyber risks we face, and it requires OSU IT and the OSU community to take action. These actions will affect faculty, staff, and student devices and accounts.

This is a community issue. Decisions about management of individual IT devices and services has a broad impact. When cybersecurity is inadequate, and a phishing or other attack penetrates a particular device, or an account is compromised, a broad general risk to the university is created. That device or account will be used to attack other devices and accounts at OSU or elsewhere.

We must act to mitigate or prevent these threats. To protect IT systems and the OSU environment and minimize the impact of cyber risks, action has been taken this Spring Term, and OSU IT will be implementing several cyber efforts this summer and the upcoming year:

Short-term – Before End of Term

1. Improved protection of student accounts
2. Increased detection of phishing and malware in e-mail

Impact

- Student Password Reset

Medium-Term – Summer 2022

1. Inventory & identify university IT equipment and services
2. Ensure IT services use appropriate accounts and authentication
3. Improve ability to detect compromised systems

Impact

- Need to reconfigure IT equipment with support team of IT staff
- Isolate equipment from OSU network where other protections are unavailable

Long-Term – AY 2022-2023

1. Replace Identity management system
2. Transition student email to Exchange
3. Advocate for funding to replace old equipment

Impact

- New approaches to assigning accounts and permissions
- Improved detection and faster response to compromised accounts
- Fewer workarounds required to continue use of old equipment
- Add: Provide for higher availability of services that support teaching, learning, research, outreach and engagement.