Working Remote ? Security Recommendations

To: University Employees
Names and titles: University Information Technology Services

Date: April 27, 2020

The COVID-19 situation quickly moved University faculty and staff to working remotely. It has been six weeks since remote work has begun and for many, has meant balancing family with the logistics of setting up a home office space. Just as working on campus requires security awareness and monitoring, there are several steps we recommend for keeping your work at home secure.

VPN Connection

Connecting to the University VPN ensures a secure connection between you and the university network. Use the VPN connection for access to sensitive information or limited access systems such as UAccess Financials or Confluence.

Below are general guidelines for connecting to the Campus VPN. However, many IT support units have their VPNs configured differently. For specific VPN instructions for your computing environment, please contact your IT support.

The university has a campuswide VPN that can be accessed, and more information [1] can be found at the UITS Website.

Working Remote Considerations ? VPN

Windows Computers: If you have a Windows computer, it is recommended that you connect to the VPN prior to logging into Windows. This will allow continued connections to the university network. More information [2] on how to accomplish this is available online.

MAC Computers: If you are experiencing any login issues, please contact your local IT department for individualized support.

Security Tips while working remotely:

- Don’t share login credentials with family members!
- Don’t approve NetID+ authentication requests if you didn’t initiate them.
- Keep a current antivirus subscription up to date.
  - Sophos Central can be installed on University-owned machines. Check with your IT department if you are unsure.
  - For Home computers, the free Sophos Home Premium antivirus software [3] is
COVID and other Phishing Scams are still occurring.

- Scams continue to occur referencing COVID, job opportunities, loan reduction, and other urgent notifications.
- Never respond to any suspicious email by clicking on links, opening unexpected attachments, or providing personal or financial information.

Additional resources and FAQs can be found at the Technologies for Working Remotely resources page. Get help from the 24/7 IT Support Center by calling (520) 626-8324 or via an online ticket or chat.

Source URL: https://uaatwork.arizona.edu/uannounce/working-remote-security-recommendations

Links
[1] https://it.arizona.edu/service/ua-virtual-private-network-vpn
[4] https://it.arizona.edu/working-remotely
[5] https://uaservice.arizona.edu/
[6] https://support.arizona.edu/