Staying Secure While Working Remotely

To:
Campus Community
Names and titles:
Information Security Office

Date:
March 24, 2020

New scams continue to arise around the COVID-19 virus. Stay alert, particularly for:

- **Phishing Emails.**
  - Recent attempts offer governmental financial support and attempt to gather personal information including your SS number.
  - Messages promise personal COVID-19 test kits but have a malware attachment.
- **False Websites.** Scammers can prey on fears or make sensational claims.
- **Illegitimate Charities/Donation Campaigns.** Only donate to known, reputable charities.

Search for verified information on your own from sources like the Centers for Disease Control and Prevention[^1] and major news outlets. There are also local resources for COVID information[^2].

Remote Work Cybersecurity

Working remotely also brings about new nuances that might not have been considered in your or your staff's normal business practices. Here are a few things to keep in mind around safe computing in a remote environment:

Data Classification

As information sharing changes, make sure you use the appropriate technologies for the classification of data you handle (Regulated, Confidential, Internal, Public). See the Data Classification and Handling Standard[^3].

Check with the appropriate Compliance Partner[^4] for which technologies can be used with Regulated Information.

HIPAA compliance information[^5] is available online.

Conference Call Meetings

Many campus units are using Zoom as a means to stay connected for meetings and other social interactions. Add protections to your meetings to ensure they’re not interrupted by
unwanted participants.

- Password protect meetings and securely share the password with participants.
- Enable a waiting room so that you grant access as people enter the meeting (not practical when you expect a large number of participants).
- Use the Only Host Can Share their Screen setting.
- Turn off Allow Removed Participants to Rejoin.

Home Computer Security

All computers used for University business should have a screen lock and be protected by antivirus/anti-malware. Remote staff who are using their personal computers to do work are eligible to install Sophos Home Premium. More information [6] is available online.

It is recommended to do the following:

- Apply all Updates for Operating System and other Software.
- Use VPN to connect securely to campus.
- Utilize approved cloud storage instead of your local hard drive (protects from ransomware and other malware accessing documents).

For more information or to report a phish [7], visit the Information Security Office website.


Source URL: https://uaatwork.arizona.edu/uannounce/staying-secure-while-working-remotely

Links
[3] https://security.arizona.edu/content/data-classification-and-handling-standard
[4] https://compliance.arizona.edu/compliance-partners
[5] https://research.arizona.edu/communicating-health-information-online
[7] https://security.arizona.edu/