PERSONAL DEVICES: Best practices for use in research

In certain circumstances, research team members may need to use personal machines to work on research projects. In these instances, please have the team member using a non-Duke managed device review and attest to following the data security best practices.

PATCH YOUR COMPUTER & APPLICATIONS

Patching your computer and applications is one of the most important ways to protect yourself online. Attackers can use vulnerabilities in browsers, and popular browser to take over your computer.

SECURE YOUR PERSONAL MACHINE

If personal machines are used for research, they should be maintained using minimum security standards, must have strong passwords, anti-virus software, and be updated per these standards regularly. Consider enabling device tracking in case your device is lost or stolen.

IF POSSIBLE, DO NOT WORK FROM YOUR LOCAL MACHINE

Avoid downloading restricted or sensitive data to non-Duke laptops or computers. Instead access data directly from allowable locations listed in your protocol.

NOTE: Using Duke Box or the VPN does not mitigate downloading data to your personal machine.

Research Team Member

PI or Supervisor

Date

Duke | RESEARCH & INNOVATION

PERSONAL DEVICES: Best practices for use in research

In certain circumstances, research team members may need to use personal machines to work on research projects. In these instances, please have the team member using a non-Duke managed device review and attest to following the data security best practices.

The Fundamental practices

Follow these steps to ensure good cyber hygiene for personal devices.

- ✓ Run an up-to-date operating system (Windows | MacOS)
- ✓ Apply operating software updates to patch security issues (Windows | MacOS)
- ✓ Apply application software updates to patch security issues (Windows | MacOS)
- ✓ Install and run an anti-virus or antimalware application (Windows | MacOS)
- ✓ Enable OS encryption (Windows | MacOS)
- ✓ Enable the OS firewall (Windows | MacOS)
- ✓ Screen protector settings (Windows | MacOS)

The Expert practices

After addressing the basics, further enhance your personal security.

- ✓ Enable Duke Unlock or MFA for all Duke logins
- ✓ Enable MFA for critical personal accounts
- ✓ Update your browser and make use of ad blocker or privacy add-ons
- ✓ Know your research data classification and use approved Duke services
- ✓ Use the Duke VPN if accessing Duke resources from a public network

Practices to avoid

When working with research or Duke-owned data, avoid these practices.

- x Forwarding your Duke email to a personal email account
- x Using a personal collaboration or storage suite (e.g., DropBox) as opposed to a Duke service (e.g., Box, OneDrive)
- x Using a personal account on a development platform (e.g., GitHub as opposed to Duke's development tools (e.g., gitlab.oit.duke.edu).

References

Data Security Guide

Duke Services & Data Classification

Email Security Guide

Minimum Security Standards

Personal Device Security Guide

Safe Browsing Guide

Secure Access Guide

SecureIT

https://security.duke.edu
https://research.duke.edu