EMORY
LIBRARIES &
INFORMATION
TECHNOLOGY
Enterprise Security

Threat Advisory

Best Practices for Telecommuting Securely

03-13-2020

Contents

03-13-2020

Executive Summary

Due to the ongoing outbreak of COVID-19, the number of employees shifting to telecommuting has risen. Over the coming weeks, many Emory University employees and Emory Healthcare employees not directly involved in patient care may also shift to telecommute options to help reduce individual risk and the pressure on healthcare systems. As a result of this, Emory LITS Enterprise Security assesses that there may be a corresponding rise in cyber risks related to or exacerbated by telecommuting. We are urging all users to take the precautions below and report any unusual activity as soon as possible to security@emory.edu.

Patching & Antivirus

Emory telecommuters should verify that their devices are running updated anti-virus software, and that software updates have been installed. If you are using an Emory owned and managed device, it will have anti-virus software already, and will be receiving patches regularly. **Emory LITS Enterprise Security strongly urges all telecommuters to use only Emory owned and managed devices to connect to Emory's network whenever possible. Please do not use personal devices unless you have no other option.** If you are unable to use an Emory owned and managed device, you must ensure that you have installed anti-virus software, and installed all Windows or MacOS updates.

Physical Security & General Data Hygiene

Telecommuters should always remain in physical possession of their devices. Do not leave laptops or devices storing Emory data unattended in public locations. This includes not leaving these devices inside vehicles, even in the trunk. The majority of laptops are stolen from vehicles.

LITS Enterprise Security asks that all telecommuters keep in mind general data hygiene practices.

Avoid downloading and storing Emory data on any device that you may be using that is not Emory owned and managed. While all Emory-owned laptops are encrypted, it is always good practice to store as little data as possible on laptops and desktops. Use supported options such as Emory Box (https://it.emory.edu/office365/BOX.html), or OneDrive (https://it.emory.edu/office365/onedrive.html), or file servers to store Emory data.

If an Emory device is lost or stolen, notify Emory LITS Enterprise Security as soon as possible – **security@emory.edu**

03-13-2020