STAYING SECURE WHILE WORKING REMOTELY

Dear University employees,

Over the last few months, many of you have been working remotely, some for the first time. With University business being completed from home, the importance of staying secure online is greater than ever.

Computing and Technology Services (CTS) encourages you to follow these tips for securing your home computing environment for work and personal use.

Eliminate Viruses & Malware

SOPHOS HOME

Use antivirus software

All University-managed computers use Sophos Endpoint Agent to protect against viruses and malware. You can offer similar protection to your home computer by installing antivirus software on it.

Employees can download **Sophos Home Commercial edition** Sophos Home Commercial edition on their personal computers for free by going to home.sophos.com/employee and signing up with their @duq.edu email address.

Download Sophos Antivirus

Note: Do NOT install Sophos Home Commercial edition on your University-managed computer.

Lock Down Your Home Wi-Fi

Secure your home wireless network

Your home Wi-Fi router acts like a turnstile that all network traffic travels through. Yet, many people forget to secure this important device, leaving it susceptible to hackers. Secure your home wireless network by changing the default password required to adjust your router's settings.

Resources for changing your Wi-Fi password

- Verizon
- Xfinity

PATCH UP YOUR PC

Install the latest security updates

An unsecured computer can become littered with security vulnerabilities and

bugs, making it an easy target for cybercriminals. One of the most effective ways to secure your computer is by installing recent security updates and patches.

Read our "Patch Up Your PC" article in the spring 2020 edition of "Cybersecurity Digest" for steps on installing updates on your personal computer.