



CYBERSECURITY

DIGEST

Spring 2021

 DUQUESNE
UNIVERSITY
Computing and
Technology Services

TABLE OF CONTENTS

Letter from the Chief Information Security Officer.....3

Go Virtual: Connect to a Computer Anytime, Anywhere.....4

Caution Ahead: Job Scam Emails.....6

Tech Bytes.....7





Letter from the Chief Information Security Officer

As we journey into a new year and new semester, technology is still playing an integral role in our daily lives. Whether you're conducting meetings over Zoom or collaborating on files in Box, technology services are helping keep us connected to one another more than ever before. However, with more computers and mobile devices connecting to the internet comes an increased risk for cybercriminals to disrupt your life.

If your devices are not secured, cybercriminals can hack into them and steal your personal information or install infectious malware. Common forms of personal information stored on computing devices include Social Security numbers, driver's license numbers, passport information and financial account numbers, none of which you want falling into the hands of a cybercriminal.

An effective way to secure your devices is to install antivirus software. Think of antivirus software as a shield that protects your devices from unwanted spyware, malware and other online threats. Many people unintentionally download these pieces of harmful software. Duquesne students can download Sophos Home edition for free at duq.edu/sophos; faculty and staff can download Sophos Home Commercial edition for free at home.sophos.com/employee by signing up with their University email address.

Another way to prevent unauthorized access to your personal information is to use using multi-factor authentication (MFA). Many online accounts, from email to financial to social, offer the option to enable MFA. Duquesne students, faculty and staff can secure their MultiPass account with Duo, the University's MFA tool. More information about Duo and how to use it to secure your University and personal accounts is available at duq.edu/duo.

Tom Dugas
AVP, Chief Information Security Officer (CISO)



Think of antivirus software as a shield that protects your devices from unwanted spyware, malware and other online threats.



GO VIRTUAL

CONNECT TO A COMPUTER ANYTIME, ANYWHERE



Virtual machines remotely store their computing environment on a server. This allows you to access a computer 24 hours a day, 365 days a year, from just about anywhere in the world.



Duquesne students are taking classes near and far from campus this spring. Technology plays a key role in the University's HyFlex learning model, keeping students connected to campus from wherever they are learning.

But challenges can arise if the device you use does not have access to software needed for your coursework. That's why Computing and Technology Services (CTS) introduced Duquesne's online virtual environment (DOVE), a service that provides remote access to virtual computer labs, last fall.

PERKS OF USING A VIRTUAL MACHINE

A computing environment consists of several components, such as an operating system, software and apps, folders, drivers and even your desktop wallpaper. If you're using a personal computer, the computing environment is stored locally on the computer itself. Virtual machines (VMs), on the other hand, remotely store their computing environment on a server. This allows you to access a computer 24 hours a day, 365 days a year, from just about anywhere in the world.

Storing a VM's computing environment on a server eliminates having to download extra software or applications that take up valuable storage space on your computer. Plus, you only need minimal computing power to connect to a VM's server, which is ideal when using an older device or one that has limited computing power.

LEARN ANYWHERE WITH DOVE

DOVE provides remote access to VMs that feature popular academic software titles, including Microsoft Office, EndNote and SPSS. Two versions of DOVE are available: DOVE Student and DOVE Classroom.

DOVE Student provides students access to a Windows 10 computing environment like one found in a campus computer lab. DOVE Classroom enables Duquesne faculty to create an online classroom lab that features VMs equipped with Windows OS, macOS and Linux. More information about each version of DOVE is available at duq.edu/dove.

Faculty interested in using DOVE Classroom must request a virtual lab, install their desired software titles and invite their students to the lab. Students can then access software and tools needed to complete their coursework for that specific class. To request a DOVE Classroom lab, please email labrequests@duq.edu.

CONNECT TO DOVE

Students can connect to DOVE Student with a Windows or Mac device by following the steps listed to the right. If using an iOS device to connect to DOVE Student, download **VMware Horizon Client** from the Apple App Store and then create a new server using vdesktop.duq.edu as the server address.

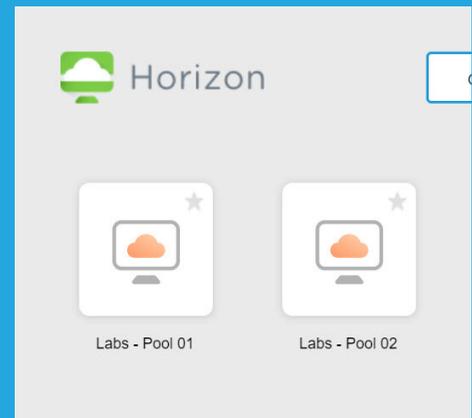
If your professor uses a DOVE Classroom virtual lab, you must register for the lab after being invited to it. Once registered, go to labs.azure.com and sign in with your University email address and password to access your classroom VM.

When using DOVE Student or DOVE Classroom, upload any files you create or edit to a cloud storage service, such as Box (duq.edu/box) or OneDrive (duq.edu/onedrive). This ensures access to your files on any device you use, whether it's a VM or your personal computer.

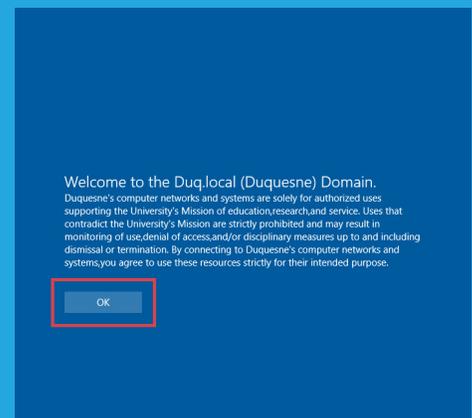
If you have questions about DOVE, contact the CTS Help Desk at 412.396.4357 (HELP), help@duq.edu or duq.edu/chat.



Step 1: Go to <https://vdesktop.duq.edu> and select **VMware Horizon HTML Access**. Then, sign in with your MultiPass username and password.



Step 2: After signing into VMware, select an available **virtual lab pool**.



Step 3: Click **OK**. You will then arrive at your virtual machine's desktop.



Caution Ahead:

JOB SCAM EMAILS

From: [Redacted] <[redacted]@gmail.com>

Subject: PART TIME JOB OFFER

This Job is currently recruiting. A Job that will not affect your present employment or studies, fun and rewarding. You get to make up to \$300 Per week, I tried it and I made cool cash, If you are interested at Pet sitting, send an email to [redacted]@gmail.com for more information about the Pet sitter Position. Kindly include your cellphone number and personal contact email address when applying.

Thanks.

Have you ever received an email like this, offering you a job opportunity? While making \$300 per week pet sitting sounds nice, this email is anything but nice. Cybercriminals use this type of phishing to lure you into a conversation with them. They then ask for your bank account routing number so they can mail you a check to deposit in your account. If you deposit the check, you're looking at headaches and stress as you try to recover from being a victim of cybercrime.

While the nature of job scam emails can vary, always look for

these common signs to determine if the message is a scam.

There are grammatical errors or misspellings in the email

The example at the beginning of this article is an actual job scam email sent to members of Duquesne in 2020. Looking through the email, you can find several typos, from sentences ending with commas instead of periods to inconsistent capitalization. If a company reaches out to you about a job opportunity, their email will be free of typos and grammar errors.

The email was sent from a Yahoo, Gmail or Outlook email address

If you receive an email about a job offer or opportunity, it will most likely be from an individual's corporate email account. For example, emails from members of Duquesne University come from an email address that ends with @duq.edu.

The email does not directly address you

When companies reach out to you about a job opportunity, they will address you by your first name. An email that does not include

a salutation or features a generic greeting such as "Good day" is most likely a scam.

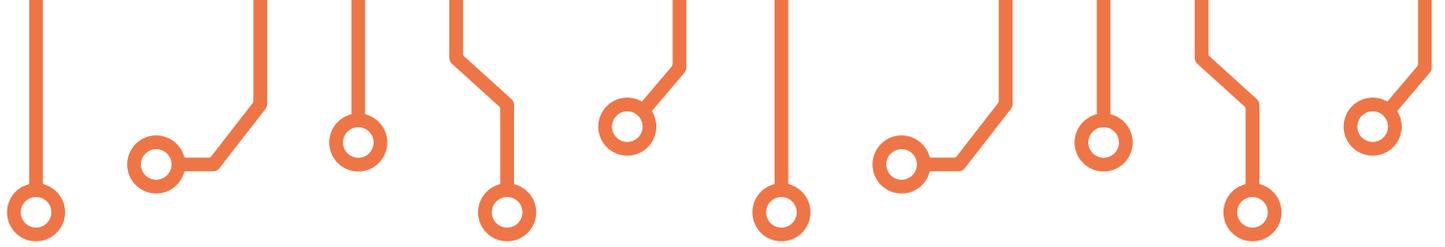
The sender asks you to share personal documents via email

Legitimate job opportunities require you to apply on a company's website. In a phishing email, you'll be asked to provide your contact information and resume. Never share this information over email, especially with someone you don't know.

The sender offers to pay you in advance before you perform any work

In these cases, the sender may send you a check and ask you to deposit it. After the check has been deposited, they'll ask you to send a portion of it back, giving them the opportunity to steal money from you.

If you receive a message that shows any of the signs described in this article, do not reply to the sender; instead, forward the message to the Computing and Technology Services (CTS) Help Desk at help@duq.edu and then delete it. To learn more about job scam emails and phishing, visit duq.edu/safe-computing.



TECH BYTES



COMING SOON TO CAMPUS: macOS BIG SUR

CTS is in the process of testing macOS Big Sur, Apple’s latest operating system, and will make it available to the campus community in the coming months. macOS Big Sur features an updated menu bar, a customizable control center, a redesigned notification center and an improved Safari experience. For a full list of new features and enhancements in macOS Big Sur, visit apple.com/macos/big-sur/features/.

Updates about the release of macOS Big Sur for University-managed Mac devices will be posted at duq.edu/about/campus/computing-and-technology-services/macos-recommendations.

FLASH PLAYER REACHES END OF SUPPORT

Effective Dec. 31, 2020, Adobe is no longer providing updates or security patches for Adobe Flash Player. In addition, Adobe blocked Flash content from running in Flash Player as of Jan. 12, 2021. Unsupported and out-of-date software on your computer can leave your device susceptible to security vulnerabilities. **Computing and Technology Services (CTS) recommends uninstalling Flash Player** from your computing devices.

CTS will automatically uninstall Flash Player from University-managed devices. Instructions for uninstalling Flash Player on a personal computer are available at duq.edu/about/campus/computing-and-technology-services/flash-player-eol.

WINDOWS 10 UPDATES: FEATURE VS. QUALITY

After releasing Windows 10, Microsoft introduced a new method for delivering updates: feature updates and quality updates. As the name suggests, a feature update integrates new features into Windows 10. These updates are released twice per year rather than introducing a new operating system every few years. Quality updates are monthly security updates released to patch flaws or bugs in Windows 10.

CTS tests and releases feature updates at least once per year to University-managed Windows 10 devices. Quality updates are released every month following Microsoft’s release schedule. To learn more about updates and patches for University-managed computers, visit duq.edu/software-updates.



Computing and
Technology Services



duq.edu/cts



[@DuqCTS](https://twitter.com/DuqCTS)



[@duqcts](https://www.instagram.com/duqcts)



[@CTSduq](https://www.facebook.com/CTSduq)