

TECH TALK

Fall 2019, Vol. III



IN THIS EDITION

- Double Down on Security with Duo
- Help Desk Service Center Summer Upgrade
- New Security Features on The Bluff
- Maintaining a Well-Oiled Computer
- CTS Help Desk Implements Online Chat

DOUBLE DOWN ON SECURITY



Phishing attacks and email spoofing are very real cybersecurity threats at Duquesne University. Each of these cyberattacks is designed to steal personally identifiable information (PII). A strong password helps keep your personal information secure, but it's just not enough to fight off increasingly sophisticated cyberattacks.

This year, Computing and Technology Services (CTS) implemented multi-factor authentication (MFA) with Duo to continue combating cybersecurity threats. MFA (also referred to as two-factor authentication or 2FA) ensures additional security when signing into an account.

How Duo Works at Duquesne

For individuals enrolled in Duo at Duquesne University, MFA is required when accessing web applications such as DORI, Blackboard, Office 365

email, Box, Qualtrics, Handshake and Zoom. One form of authentication is your MultiPass username and password. The second form is completed through the following:

- Responding to a Duo Push notification sent to your mobile or wearable device
- Entering a one-time passcode generated with the Duo Mobile app or a Duo hardware token
- Answering a mobile or landline call and following a prompt
- Authenticating with a YubiKey or other USB authentication device.

After both authentication factors are accepted, you are granted access to the application. A complete list of MFA-enabled applications at Duquesne is available at duq.edu/authentication.

Duo Multi-Factor Authentication By the Numbers



2213

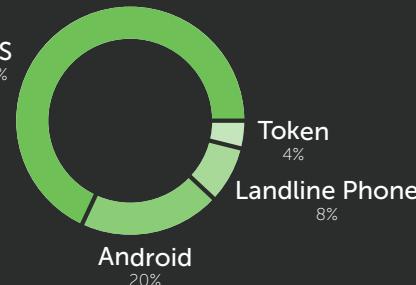
Enrolled Users



2432

Enrolled Devices

Device Types



Successful Authentications

in August 2019

74K+

Total Authentications

2400+

Daily Authentications



Duo Push

73%



Phone Call

15%

Passcode

12%

Enrolling in Duo

Duo enrollment is open to all students, faculty and staff at Duquesne. Enroll in Duo using the Duo Device Management portal in MultiPass and DORI.

There is no limit to the number of devices you can enroll in Duo. CTS recommends registering at least two different devices in case you lose one or leave it at home. For example, you can enroll your mobile phone and a hardware token in Duo. If you leave your mobile phone at home, you can still log in to MFA-enabled services by generating a passcode with your hardware token.

Duo hardware tokens and YubiKeys are available for purchase at the Duquesne University Computer Store. Visit duq.edu/duo for instructions and a video on enrolling in Duo.

Enrolling Third-Party Accounts in Duo

Did you know that downloading the Duo Mobile app on your mobile device enables you to secure third-party accounts such as Facebook, Twitter and Google with Duo. Visit guide.duo.com/third-party-accounts for details about securing third-party accounts with Duo.

NEED HELP? CONTACT US!

The CTS Help Desk is happy to assist students, faculty and staff with any technical issues or questions. Contact the CTS Help Desk at:



412.396.4357 (HELP)



help@duq.edu



206 Union



Monday–Friday: 7 AM–5 PM
Saturday: 9 AM–4 PM
Sunday: 12 PM–4 PM

CYBERSECURITY AWARENESS TRAINING



FOR FACULTY & STAFF

Computing and Technology Services (CTS) offers online cybersecurity awareness training to all Duquesne employees as part of a new partnership with KnowBe4, one of the world's top security awareness training platforms.

This year's training features videos, activities and assessments on social engineering, a primary cybersecurity challenge at Duquesne University. Employees will learn strategies for keeping their personal information secure, including:

- Hints on how to identify and avoid potential threats
- Seven email red flags that can alert you to a possible cyberattack
- Strategies for staying safe on computers, mobile devices and in modern office environments.

Employees who complete the training can practice their cybersecurity skills in the "Danger Zone" game. Complete the training by **January 10, 2020**, to be entered into a drawing for a chance to win great prizes!

For more information about cybersecurity awareness training, visit duq.edu/cybersecurity-training.

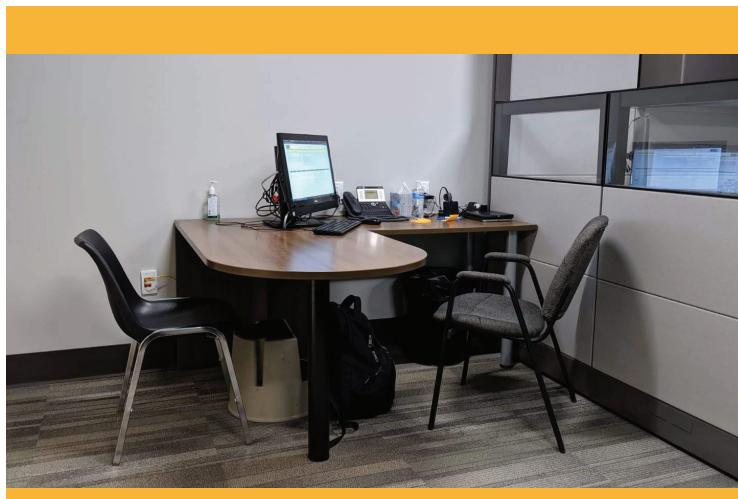
HELP DESK SERVICE CENTER SUMMER UPGRADE



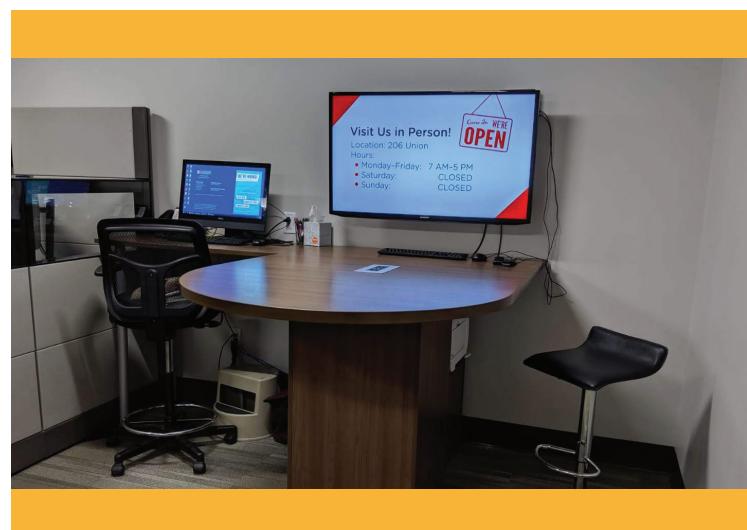
Providing campus with top-notch customer service is one of the Computing and Technology Services (CTS) Help Desk's primary goals.

In 2012, CTS opened the Help Desk Service Center on the second floor of the Union to offer in-person assistance at a central location on campus. With new technology initiatives over the last few years, the service center's previous setup began to show its limitations.

To continue to offer the best customer service and accommodate new technology initiatives, CTS upgraded the Help Desk Service Center space over the summer. "We love the Duquesne community and strive to provide the best possible experience when they are faced with technology challenges," Melissa Jackman, Help Desk Manager, says. "The upgrade to the Help Desk provides a more service-oriented layout which allows us to assist customers much more efficiently."

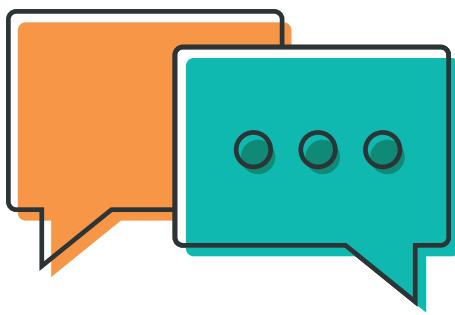


The Help Desk Service Center now features service stations on each side of the space staffed with a Help Desk consultant. It also offers a larger space for customers and Help Desk staff to work together in the troubleshooting process.



In 2017, CTS introduced DuqNet Internet of Things (IoT), a wireless network designed for streaming and gaming devices. With resident students connecting devices such as Roku, Apple TV and PlayStation to the campus network, a new challenge arose: how to troubleshoot connection issues with IoT devices. The upgraded space provides Help Desk staff with new tools to better assist students trying to connect gaming and streaming devices to the IoT network.

The Help Desk service center is open Monday through Friday from 7 a.m. to 5 p.m., Saturday from 9 a.m. to 4 p.m. and Sunday from 12 p.m. to 4 p.m. Information and answers to frequently asked questions is available at duq.edu/cts.



NEED HELP? CHAT WITH CTS!

As technology continues to evolve, so does communication between people and organizations. Telephone and email have been the dominant methods to contact an organization for customer support. Today, however, online chat is a popular choice for interacting with an organization when support is needed. With emerging technologies such as artificial intelligence (AI) and chatbots, the future is bright for online chat in the customer support world.

The Computing and Technology Services (CTS) Help Desk now offers online chat as an additional way to receive customer support. LiveChat offers many benefits such as quick resolution time and strong customer satisfaction.

Visit duq.edu/cts and click the “Need Help?” button located in the bottom right corner of your browser window to use LiveChat. After submitting your name, email address and phone number, a CTS Help Desk consultant will initiate a chat session with you.

Need Help?



LiveChat is available Monday through Friday from 9 a.m. to 3 p.m. Otherwise, contact the CTS Help Desk at 412.396.4357, help@duq.edu or in-person on the second floor of the Union for assistance.

zoom

Meet Whenever, Wherever

Zoom Meetings is a video conferencing tool that allows you to collaborate with your friends, family and classmates. University students and employees can sign into Zoom with their MultiPass credentials at duq.zoom.us. Once signed in, you can join, host or schedule a meeting. If you need to invite a non-Duquesne University individual, email them a link to so they can join.

Want to get more out of Zoom? Download the Zoom Meetings app on your mobile device’s app store and the Zoom for Microsoft Outlook plugin. Visit duq.edu/zoom for more information on Zoom and training materials.

Wireless Lab Printing



Print From Your Own Device!

Visit one of more than 40 campus computer labs and print files from one of the lab computers or your own computer using Web Print.

Students receive an annual print quota of 3,000 pages with the option to purchase additional pages at the Computer Store. Visit duq.edu/wifi-printing for more information on using Web Print.



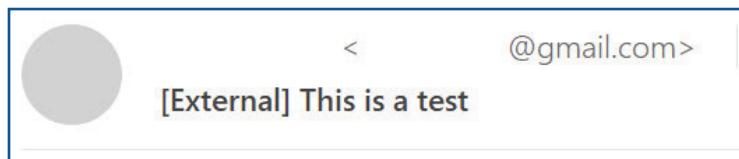
New Security Features On The Bluff

Over the summer, Computing and Technology Services (CTS) implemented two new changes to help keep personally identifiable information (PII) secure—external email tags and an updated login experience for DORI and Office 365 email.

External Email Tags

Most phishing emails are sent from an external email address and include malicious attachments or links designed to steal PII. External email tags will notify you when an email has been sent from someone outside of Duquesne University.

The text **[External]** now appears in the subject line of all emails from non-@duq.edu addresses.



This External tag appears when viewing your Duquesne University email in the Outlook Web App (OWA), email clients and mobile devices. If you receive an email from an unrecognized sender, be aware of the risks of clicking on links or opening attachments.

New DORI & Email Login Experience

DORI and Office 365 email offer access to personal and financial information, making them prime targets for a cybercriminal looking to steal PII. The new login experience for DORI and email provides additional security with the use of multi-factor authentication.

When accessing DORI and Office 365 email, you are now redirected to the standard Duquesne University web application login page. If you are accessing DORI, click the **Login to DORI** button to be redirected to the login page. Anyone enrolled in multi-factor authentication (MFA) with Duo will be required to complete an MFA login to gain access to DORI and Office 365 email.

Tech Tip

If you use a bookmark to access DORI, you may be redirected to the standard Duquesne University web application login page instead of the DORI dashboard. To access the DORI dashboard containing upcoming maintenance notices and articles, visit duq.edu/dori and create a new bookmark.

BEWARE BEWARE BEWARE

OF PHISHING

duq.edu/phishing

WHAT IS PHISHING?

Phishing is a form of **fraud** where a cybercriminal attempts to steal your confidential information. This is typically accomplished by sending an email that directs you to a false website where you are asked to provide personally identifiable information (PII), such as a password, credit card or bank account numbers.

TYPES OF PHISHING

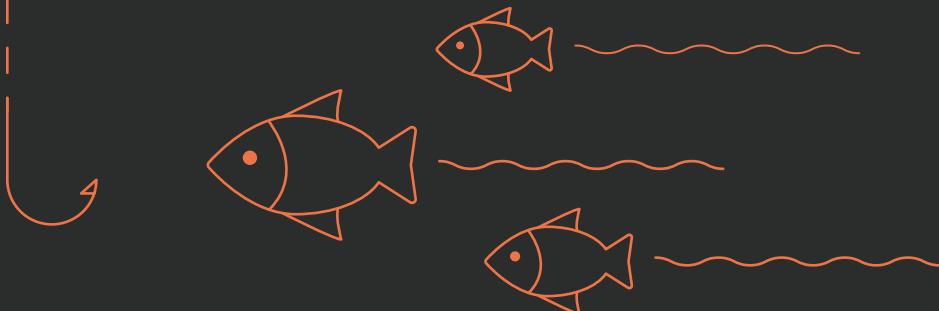
Email spoofing occurs when a message appears to be sent from someone you know but is actually sent from a cybercriminal.

Spear phishing attacks are targeted toward a specific individual, organization or business to increase the chances that the recipient takes action.

Vishing is a phone-based phishing attack whereas **smishing** uses SMS or text messages to target you. Both of these attacks aim to steal your PII through the use of links and by creating a sense of urgency.

COMMON SIGNS OF A PHISHING EMAIL

- Misspellings in the subject line or body of the email
- A link or attachment that you are directed to open
- A sense of urgency to take action or respond
- The signature in the email does not look legitimate



DuqNet IoT



DuqNet Internet of Things (IoT) allows resident students to connect a wide range of streaming and gaming devices to the campus network. Devices such as Apple TV, Xbox, PlayStation and Roku can connect to DuqNet IoT. Any streaming devices connected to DuqNet IoT must be controlled with their respective remote control.

The DuqNet IoT network is strictly designed for recreational purposes—it is not meant for connecting computers or mobile devices. Students can register up to four non-WPA2 Enterprise-capable devices on DuqNet IoT by visiting duq.edu/iot.

XFINITY On Campus

Stream Live TV On Laptop, Desktop & Mobile Devices



XFINITY On Campus provides resident students access to more than 90 TV Everywhere apps. Students living on campus can experience the full features of XFINITY On Campus, including live TV, On Demand shows and movies, on their laptop, desktop and mobile devices.

To access XFINITY On Campus, visit xfinityoncampus.com from your desktop or laptop computer or download the XFINITY Streaming App on your mobile device. Students can sign in using their MultiPass credentials. More information about XFINITY ON Campus is available at duq.edu/xoc.

BUY YOUR NEXT COMPUTER AT A REDUCED PRICE!

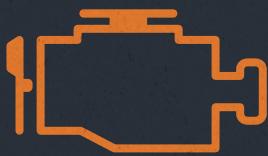
On the third Thursday of each month, the Duquesne University Computer Store hosts a used computer sale. Students, faculty and staff can purchase a wide range of secondhand technology equipment, such as laptops, desktops and iPads, at a discounted price. Visit duq.edu/used-computer-sale the week of the sale to check available inventory.

Note: This sale is first come, first served. A valid Duquesne University ID is required to complete your purchase. Limit one item per customer while supplies last.

Join Us for Our Next Sale!



Thursday, Sept. 19



MAINTAINING A WELL-OILED COMPUTER

Just like you change the oil on your car every 3,000 miles, you should perform routine maintenance on your computing devices. Computers consist of several hardware and software components working together to power your device. However, viruses and unmanaged files can add wear and tear on a computer. Computing and Technology Services (CTS) recommends routinely performing the following actions to keep your device operating at peak performance.

Keep Software Updated

Operating systems (OS) and third-party applications live on every computer. These tools work with a computer's hardware to provide functionality to a device. However, bugs and security vulnerabilities can leave a hole in a computer's defense.

While most operating systems and third-party applications automatically install updates, it is a good practice to manually check for updates. Do this by navigating to the **Settings** menu in the device or application and then to **Check for Updates**.

Install Antivirus Software

An antivirus program adds an extra layer of security to your computer's defense. When you download third-party applications from the Internet, unwanted programs or viruses can also be downloaded if the website is unsafe. Antivirus software helps fight off viruses trying to infect your computer.

CTS recommends employees and students secure their personal computers with Sophos Home antivirus. Visit duq.edu/sophos for instructions on installing Sophos Home on your device.

Organize and Back Up Your Data

Before backing up important data on your computer, it's helpful to organize your files and folders. This allows you to easily back up important files and locate them in the backup.

Back up your data using an external hard drive or cloud storage service, such as Google Drive or Box. Follow the 3-2-1 rule: keep **3** copies of your data on **2** types of storage media with **1** copy offsite.

box + Office

Take Your Productivity to the Next Level

Looking for an easy way to access your Box files in Microsoft Office? Check out Box for Office! This add-in allows you to easily open, edit, save and share files in Box directly from Microsoft Office. Box for Office is only available for Windows devices.

If you visit duq.edu/box to access your Box files, you can view and edit your files using Microsoft Office Online. Sign in using your Duquesne University email and begin making changes to your files.

About

Tech Talk is published each fall semester for Duquesne University students and employees. Content in Tech Talk may be printed without permission, but it is required to credit the source.

CTS Mission Statement

Computing and Technology Services (CTS) provides a critical set of services enabling Duquesne University's teaching, learning, research, business, image and campus life. CTS partners with the entire campus community to meet our common and strategic goals through the University's Spiritan Mission of Service.



Upcoming Events

Join CTS at the following campus events!



Tech Life: World Tech Tour
Sept. 23 from 10 AM—1 PM
Union Atrium



Center for Student Involvement Safety Fair
Sept. 25 from 10 AM—2 PM
Academic Walk