DUQUESNE UNIVERSITY
Computing and Technology Services

Spring 2020

# CYBERSECURITY DIGEST

In This Edition



# TABLE OF CONTENTS



# Letter From the Chief Information Security Officer

Every January, we celebrate National Data Privacy Day on Jan. 28. This internationally recognized day is an educational initiative designed to raise awareness among businesses and individuals about the importance of protecting the privacy of personal information. This year, we turn our attention towards protecting our online accounts.

At Duquesne, Computing and Technology Services (CTS) invested in Duo multi-factor authentication (MFA). Duo MFA enables students and employees to add an extra layer of security to their MultiPass account. This added layer requires you to have two things to access your MultiPass account: something you know, like your login credentials, and something you have, like a phone or hardware token. Requiring two factors instead of just one to gain access to an account increases the security of your MultiPass.

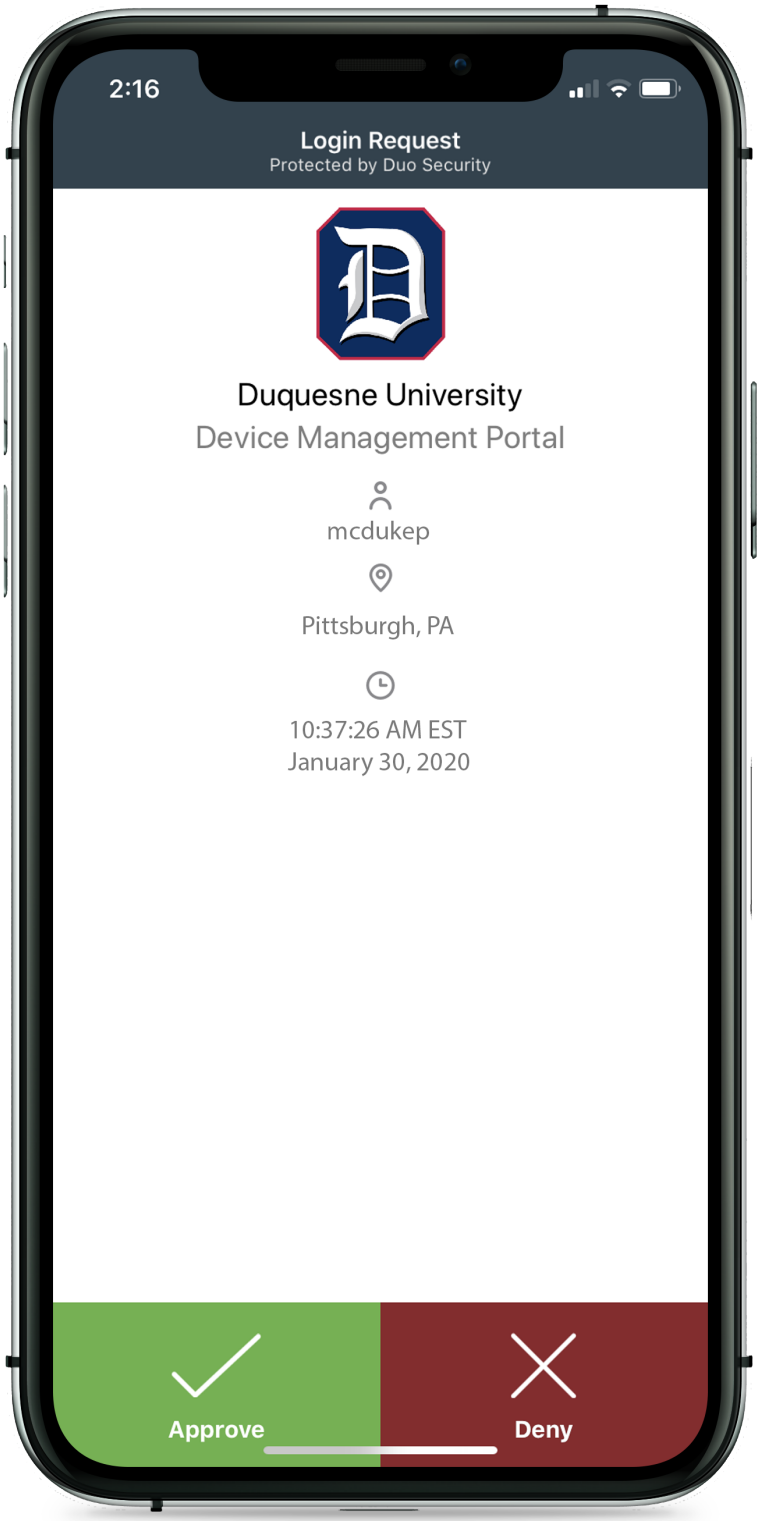
However, MFA isn't just for your MultiPass account; it's an essential security tool for your email, financial, social and entertainment accounts. With so many accounts in our everyday lives, people commonly re-use the same password or create a similar password for many accounts. While this may make it easier to remember your password, it also makes it easier for multiple accounts to get hacked if your password is ever stolen. Adding MFA to your accounts helps prevent cybercriminals from accessing your personal information, even with a stolen password.

I encourage you to take a few moments to enable MFA on your online accounts, particularly your banking accounts or accounts linked with a credit or debit card. Many online accounts offer MFA options in the account's privacy and security settings. Visit **duq.edu/duo** to learn more about Duquesne's MFA efforts.

**Tom Dugas**
*AVP, Chief Information Security Officer (CISO)*

"MFA isn't just for your MultiPass account; it's an essential security tool for your email, financial, social and entertainment accounts."

# Making the **Push** For MFA




Over a year ago, Computing and Technology Services (CTS) began shifting Duquesne to a multi-factored campus. Multi-factor authentication (MFA) is a security mindset of using two factors to authenticate your identity when signing in to a website, application or other online service.

These factors include something you know, like a username and password, and something you have, such as a smartphone or security key.

MFA protects against cyberattacks such as phishing, social engineering and brute-force login attempts. If a cybercriminal steals your login credentials, they could not access your account because they only have one of two authentication factors. Like the saying goes, "Sometimes two is better than one."

CTS uses Duo to manage the second factor of MFA: something you have. Duo MFA allows you to authenticate into Duquesne online services through a variety of ways, including:

- Approving a Duo Push sent to your smartphone through the Duo Mobile app
- Generating a one-time passcode with a Duo hardware token or in the Duo Mobile app
- Answering a call to your mobile or landline phone
- Tapping a YubiKey USB security key plugged into your computer.

So which method is right for you?

## DUO PUSH

If you download the Duo Mobile app on your tablet or smartphone, you can take advantage of Duo Push. This feature allows you to approve an MFA request sent to your mobile device with the tap of a finger.

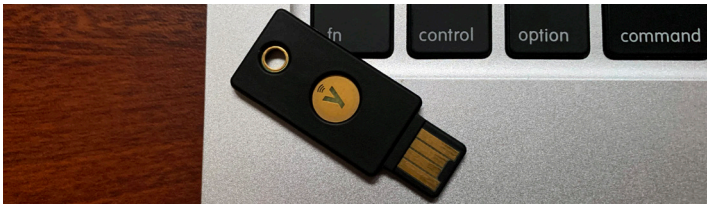
After signing into a Duquesne online service with your MultiPass credentials, select **Send Me a Push** on the Duo authentication prompt. After a few seconds, a Duo Push notification will pop up on your mobile device. Simply tap **Approve** on the notification to gain access to the online service.

## DUO HARDWARE TOKEN

If you don't want to use a mobile device for MFA, an alternative is a Duo hardware token, which allows you to generate a one-time six-digit passcode when prompted to sign in with Duo. After signing into a Duquesne online service, select **Enter a Passcode** on the Duo authentication prompt and tap the button on the hardware token to generate a passcode.


## YUBIKEY

YubiKeys are USB devices that function similarly to a hardware token, but feature a more streamlined login experience. After signing into a Duquesne online service, select **Enter a Passcode** and tap your finger on the YubiKey to gain access to the online service.




Duo hardware tokens and YubiKeys are available for purchase at the Duquesne Computer Store on the second floor of the Union. After purchasing your device, contact the CTS Help Desk at 412.396.4357 or help@duq.edu to register it with your Duo account.

## EMPLOYEES REQUIRED TO ENROLL IN DUO BY MARCH 31, 2020

As we turn the calendar to a new year, a new batch of cyberattacks and exploits are expected to soon be popping up across the world. While these attacks typically target large companies and organizations, Duquesne is susceptible to being a target. With an increasing number of cyberattacks against universities and growing regulatory compliance obligations, the need for additional account security rises.

To better protect the University from cybersecurity threats and exploits, such as phishing and ransomware, all University employees are required to enroll in Duo by **Tuesday, March 31.** Employees are encouraged to enroll at least two devices in Duo, including a smartphone with the Duo Mobile app installed.

Visit **duq.edu/duo** or contact the CTS Help Desk to learn more about Duo, MFA and device enrollment.

# be aware

## OF WHAT YOU SHARE

Social media makes staying in touch with friends and family a breeze. Whether you share pictures from a recent vacation, check in at your favorite coffee shop or post about getting a new job, your followers are easily kept in the loop with everything happening in your life. However, sharing personal information online opens up a door to serious privacy concerns.

Many people are not aware of the information that they share with each post on social media. When you share a photo of the cute puppy you adopted, you may also be sharing a possible password or security answer for one of your online accounts. If your social media account isn't private, this information could be shared with anyone in the world.

Location is another piece of information that is commonly overshared. Snapchat features a global map where people can see your exact location. Left unrestricted, you could be sharing your location with strangers. If you plan to use an app that requests your location, make sure you restrict it to friends or disable it.

Before creating your next post or sending a selfie to your best friend, review the privacy settings on your social accounts and make sure you're aware of what you're sharing.

### FACEBOOK

1. Sign into your Facebook account.
2. Click **Settings.**
3. Select **Privacy.**

More information: **https://www.facebook.com/help/325807937506242**

### INSTAGRAM

1. Go to your Instagram profile.
2. Tap the **menu icon.**
3. Tap **Settings.**
4. Tap **Privacy.**

More information: **https://help.instagram.com/196883487377501**

### TWITTER

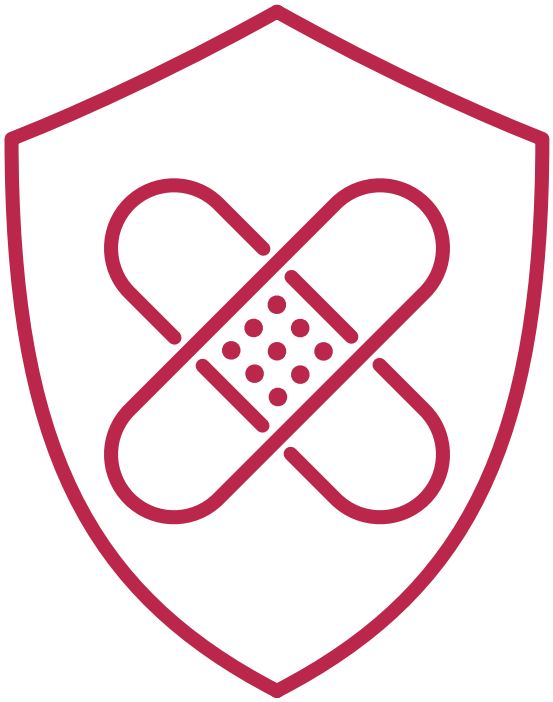
1. Sign into your Twitter account.
2. Click **More.**
3. Select **Settings and privacy.**
4. Select **Privacy and safety.**

More information: **https://help.twitter.com/en/safety-and-security**

### SNAPCHAT

1. Go to your Snapchat profile.
2. Tap the **gear icon** to open Settings.
3. Scroll down to the **"Who Can…"** section.

More information: **https://support.snapchat.com/en-US/a/privacy-settings2**



# PATCH UP YOUR PC

One of the strongest components under the hood of a computer is its operating system. This software supports a computer's basic functionality, from opening and closing applications to adjusting the brightness of the screen. Without an operating system, computers could not function properly.

To keep your computer operating at peak performance, an up-to-date and secure operating system is necessary. Left unsecured, bugs and security vulnerabilities can make your device an easy target for a cybercriminal. Installing recent security patches, updates and drivers can prevent your computer from becoming slow, unresponsive and compromised.

Computing and Technology Services (CTS) manages all operating system and third-party app updates on university-managed computers. Follow the steps to the right to install updates and software patches on your personal computer.

## WINDOWS 10

1. Click the **search icon** in the bottom left and type "settings" in the search box.
2. Open the **Settings** app.
3. Select **Update & Security.**
4. Click the **Check for Updates** button.
5. Install and apply recommended updates.

## MAC OS (MOJAVE OR LATER)

1. Open **System Preferences.**
2. Select **Software Update.** Your device will automatically check for updates.
3. If an update is available, click the **Update Now** button.

## THIRD-PARTY APPS

Third-party apps are pieces of software made by a developer who is not the device's manufacturer. Some of the most commonly used third-party apps include Google Chrome, Mozilla Firefox and Adobe Reader DC.

These pieces of software also need frequent updates to ensure your computer remains secure. Third-party apps typically offer built-in updating options that can be set to install updates automatically or check for updates each time the software is opened.

## DO YOUR RESEARCH

While updates are supposed to improve an operating system or application, they can sometimes cause unexpected issues, like slow performance or depleted battery life. Before installing a new update, do your homework to learn more about it and any potential pitfalls to installing it.

Visit third-party app developer's websites to learn more about recently released updates. For major operating system updates, research the manufacturer's website and major tech news outlets, like CNET.


# Take a Road Trip with Eduroam

Connect to free, secure Wi-Fi in over 100 countries worldwide with your Duquesne email address and password.

**duq.edu/eduroam**

eduroam

# TECH BYTES

## MICROSOFT WINDOWS 7 REACHES END OF SUPPORT

Please note that Windows 7, released by Microsoft in October 2009, is no longer supported by as of Jan. 14, 2020. Computing and Technology Services (CTS) started informing the campus community early in 2019 to upgrade from Windows 7 to 10. If you still use a university-managed computer with Windows 7 installed, contact the CTS Help Desk at 412.396.4357 or help@duq.edu to request a Windows 10 upgrade.

## MAC OS CATALINA COMING TO CAMPUS

This spring, CTS will make Apple's latest operating system, macOS Catalina (10.15), available to the campus community. MacOS Catalina improves the functionality and stability of previous macOS versions. However, it achieves this by eliminating support for 32-bit applications.

Before upgrading to macOS Catalina, a list of 32-bit applications installed on your macOS device will be shown. Check with the application developers or your CTS technician to determine if your applications are compatible with macOS Catalina.

## WINDOWS 10 UPDATES: FEATURE VS. QUALITY

After releasing Windows 10, Microsoft introduced a new servicing model under the label "**feature updates.**" Under this model, Microsoft releases and integrates new features to Windows 10 twice a 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 computers. Quality updates are released every month in accordance with Microsoft. To learn more about updates and patches for university-managed computers, visit **duq.edu/software-updates**.

## HELP YOURSELF TO DU SOFTWARE

University-managed Windows and macOS devices each feature a tool to help employees install popular applications, such as Microsoft Office, SPSS and GlobalProtect VPN. This helps ensure your university-managed computer is up to date and running compatible software. It also removes the risk of downloading unwanted programs or malware commonly bundled with internet downloads.

On macOS devices, open Finder and then navigate to the Applications folder to locate **Self-Service.**

Windows users can access **Software Center** by:

- Double-clicking the Software Center shortcut located on the desktop
- Clicking the magnifying glass icon located in the bottom left corner and typing "software center" in the search box.

# WHAT THE HACK

## RANSOMWARE

No one wants to find themselves being held hostage by a computer, but that's exactly what happens when a computer becomes infected with ransom malware, also known as ransomware.

Once ransomware infects your computer, it locks your files and demands a ransom payment to regain access. Often, you have a limited amount of time to make the payment before losing access to your files forever. However, paying the ransom does not guarantee that you will recover access to your files.

Due to the nature of ransomware attacks, almost anyone can be a target. The most common targets are individuals or organizations that can afford a large ransom payment, including:

- Healthcare systems
- Government agencies
- Law firms holding sensitive data
- Universities.

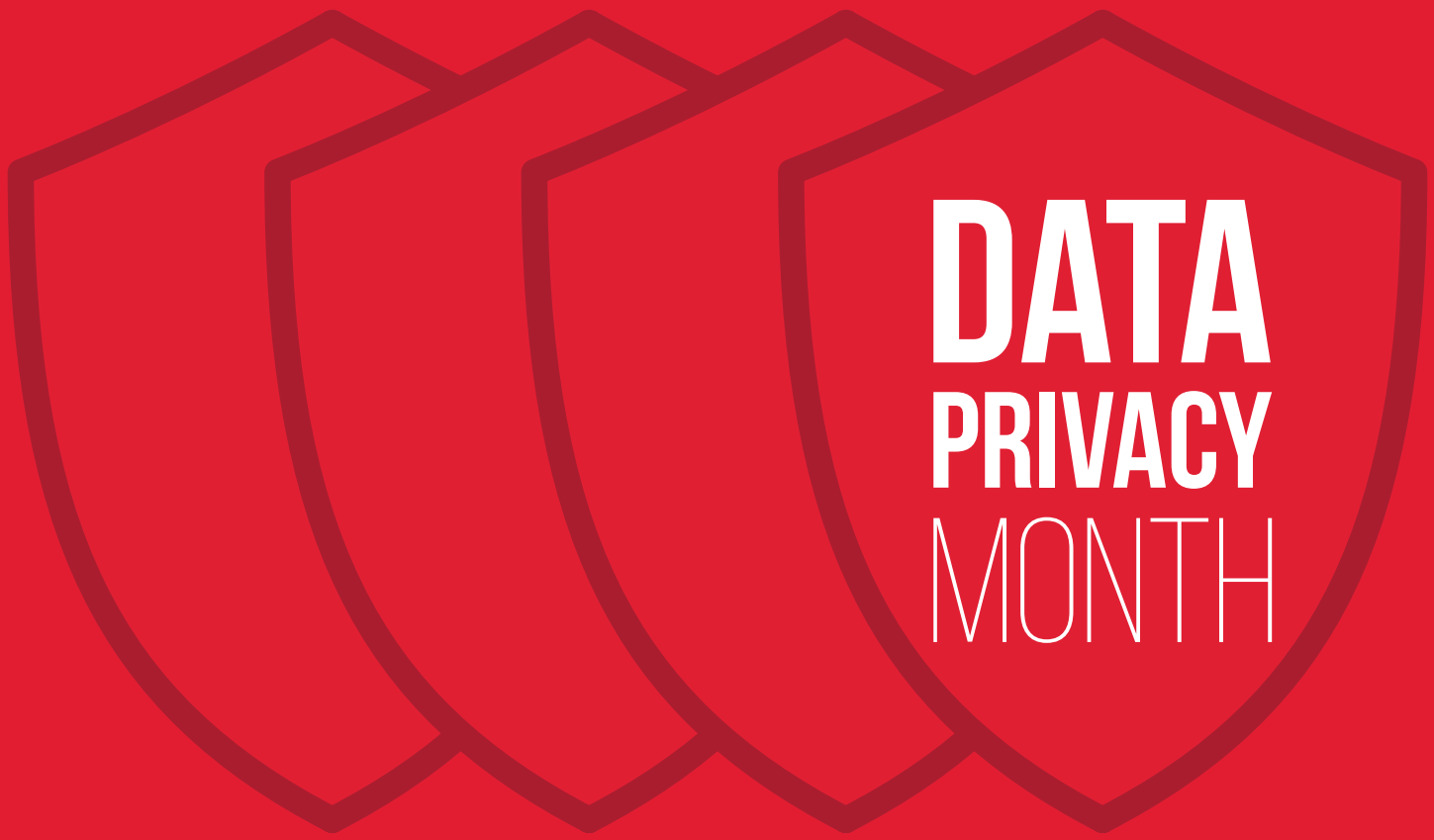
Ransomware is often spread through phishing emails that contain malicious attachments or links. Computing and Technology Services (CTS) recommends following these safe practices to avoid being a victim of ransomware:

- Update software and operating systems with the latest patches and security updates.
- Never click on links or open attachments in suspicious emails.
- Back up important files and data.
- Be cyber aware while browsing the internet.

### RANSOMWARE SPOTLIGHT: WANNACRY

WannaCry is a ransomware worm that spread through outdated Windows computers in May 2017. Once a computer was infected with WannaCry, a user's files were encrypted. Cybercriminals then demanded a bitcoin payment in exchange for the decryption key.

According to the United States Department of Homeland Security, WannaCry infected approximately 200,000 computers globally. The largest target of this attack was National Health Service (NHS) hospitals in England. An estimated 70,000 NHS devices— including computers, MRI scanners and blood-storage units—were infected with WannaCry.



# DATA PRIVACY MONTH

> Data Privacy Month is an opportunity to remind us that we are responsible for the privacy of our data, whether it be at work, home, or elsewhere.

As snow begins to fall throughout the Pittsburgh region, millions of people are falling for phishing scams asking them to do a "quick favor" or upgrade their mailbox "quota." Falling victim to these types of cyberattacks can result in the loss of personally identifiable information, such as a bank account number, email address or Social Security number.

Each year, Data Privacy Month takes place from Jan. 28–Feb. 28, kicking off with Data Privacy Day. This month-long event aims to raise awareness about the importance of protecting your personal data and information online. Between email, social media and other online services, many people forget to "share with care" when it comes to their data.

Some apps and services include vague terms in their privacy settings, making it hard to determine what information is being shared when using them. Even worse, once personal information is shared, many people are unaware of how it is being used by companies or organizations.

"We cannot assume that someone else is securing our data or keeping it private," says Tom Dugas, Chief Information Security Officer. "We need to be emphatic about our need to keep our personal information private and out of the wrong hands. Data Privacy Month is an opportunity to remind us that we are responsible for the privacy of our data, whether it be at work, home or elsewhere."

Follow CTS on Twitter and Instagram (@duqcts) all month long for data privacy tips and information about this year's data privacy contest.

DUQUESNE UNIVERSITY
Computing and Technology Services

www.duq.edu/cts

@DuqCTS

@duqcts

@CTSduq