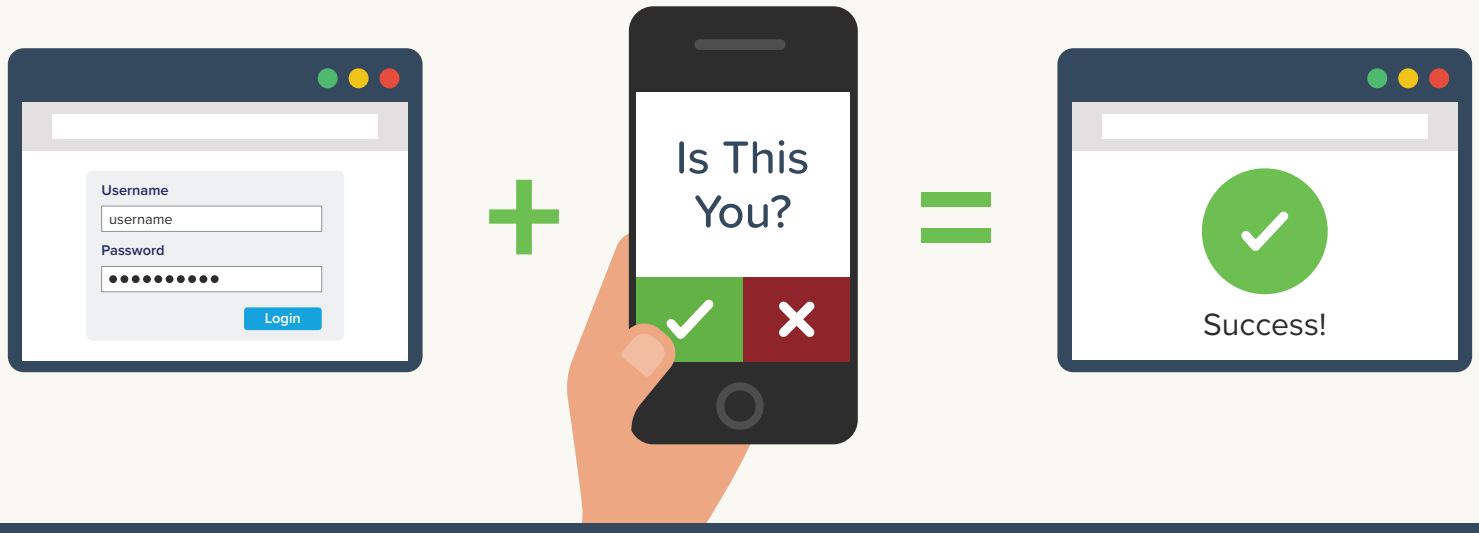
CYBERSECURITY DIGEST

Spring 2019, Vol. VIII

IN THIS EDITION

- Multi-Factor Authentication with Duo
- Safe Computing Tips for Working Remotely
- Spotting a Spoofed Email
- Cybersecurity Training Highlights
- And More!



DUO

DUQUESNE UNIVERSITY
Computing and Technology Services

Letter From Director of Information Security

Every January, we celebrate Data Privacy Day on January 28. This internationally recognized day is an educational initiative focused on raising awareness among businesses and individuals about the importance of protecting the privacy of personal information. As the creation and distribution of information being collected by companies, websites, and social media grows, so does the importance of protecting personal information.

At Duquesne University, Computing and Technology Services (CTS) devotes several resources to the protection of restricted data and, in particular, **personally identifiable information (PII)** in our environment. PII is any combination of data points that can lead to the identification of a specific individual, such as yourself. Most often, people think of PII as social security numbers, driver's license numbers, passport information, and financial account numbers. However, PII can also be data such as your birthdate, medical information, and account passwords.

While Duquesne University takes great responsibility to protect the privacy of your PII, it is also your responsibility. Social media users are especially prone to concerns about PII, as they voluntarily share large quantities of their information, as well as information belonging to friends and family, online. For example, I once read a social media post that asked: "if you were as old as your social security number, how old would you be?" Surprisingly, hundreds of individuals replied to that post with their social security number.

With the spring semester in full swing, take time to protect your PII and PII of others. Keep PII and other forms of restricted data protected and secured electronically using security tools such as encryption, password protection, secure file sharing, and locked hard drives. In addition, enable multi-factor authentication (MFA) for any third-party application that offers it, particularly financial institutions and others with access to your PII.

Protecting data is a shared responsibility between you and institutions that have access to it. Be aware of how you can compromise your own privacy and confirm that organizations you engage with handle your data appropriately. Information on how Duquesne University categorizes and protects data can be found in the CTS Data Governance Service Requirements at **duq.edu/data-governance**.

Tom Dugas
Chief Information Security Officer (CISO)

MULTI-FACTOR AUTHENTICATION WITH DUO

With new security vulnerabilities and breaches occurring more frequently, a strong password is not enough to keep your personal information secure. If the credentials for an account you own are stolen, there is no extra layer of defense between your information and a cybercriminal. Even worse, if you use the same or a similar password for more than one account, a cybercriminal can infiltrate multiple accounts by cracking a single password. So how can you better secure your accounts and personal information? By doing what many companies, including Google, Apple, and Microsoft, are doing: doubling up on security with **multi-factor authentication (MFA).**

What is MFA?

MFA, sometimes referred to as two-factor authentication or 2FA, adds an additional layer of security on your accounts by requiring two forms of verification before granting access to an account. These forms of verification, referred to as factors, can include:

1. Something you know (ex. account password or banking PIN)
2. Something you have (ex. a mobile phone or ATM card)
3. Something you are (ex. a fingerprint)

A common example of MFA in action is withdrawing money from an ATM. When you arrive at the ATM, you insert your bank card (something you have) and then enter your PIN (something you know). After these two factors of authentication are accepted, you gain access to your account and can withdraw money.

Multi-Factor Authentication Example

Withdrawing Money From an ATM

1. Insert your bank card **(Something you have)**

2. Enter your PIN **(Something you know)**

3. Receive your money **(Gain access)**

Securing Your Accounts with MFA

If you use your mobile device to access email, bank accounts, and other services, you are already using your mobile device as one factor of authentication. Adding tools such as Google Authenticator, LastPass Authenticator, and Duo Security to your mobile device can add the additional layer of security that MFA offers. These MFA apps can link to many other accounts such as Google, GitHub, Facebook, and Twitter by scanning a QR code generated under the account's settings. Once MFA is enabled, you can conveniently use the mobile app to generate a one-time passcode when signing in to your account. For a list of services that support MFA, visit **https://twofactorauth.org.**

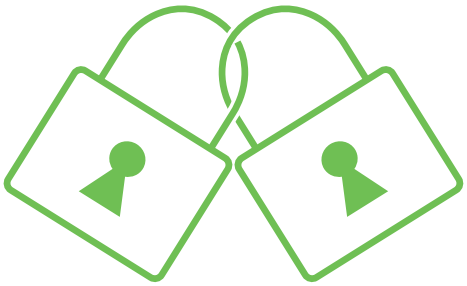
Duo at Duquesne

Computing and Technology Services (CTS) will begin rolling out MFA and Duo Security tools to campus this year. Initially, Duo will be available to faculty, staff, and students for a select set of Duquesne University applications. The use of MFA with Duo will be required when accessing these applications.

Additional information about the Duo and MFA rollout to campus will be available as this feature becomes available. To learn more about Duo Security tools at Duquesne University, visit **duq.edu/duo.**

Enabling Duo on 3rd Party Accounts

In addition to securing your MultiPass account, Duo can add an extra layer of security to your personal accounts. For assistance with enabling MFA on a third-party account with Duo Security, visit **https://guide.duo.com/third-party-accounts.**



ISO SPOTLIGHT

This past October, members of Computing and Technology Services' (CTS) Information Security Office hosted their annual cybersecurity event. The event, **Don't Take the Bait,** focused on sharing different methods individuals can use to identify phishing messages. Some of the methods highlighted include:

- **Click Reply But Don't Send**

  If the Reply To field is not an @duq.edu email address, the message is not legitimate.

- **Mouse Over Clickable Links**

  If you hover over a clickable link and the link is for a non-duq.edu site, it is not legitimate.

- **Grammatical and Spelling Errors**

  If the message has numerous grammatical or spelling errors, it is probably fake.

In addition to learning cybersecurity tips, visitors received cybersecurity-themed stickers, RFID card holders, and Swedish Fish® flavored ice (courtesy of Rita's Italian Ice).

AVOID FALLING FOR SPOOFED EMAILS

Email messages have been circulating across campus recently in which the sender pretends to be someone the recipient knows asking them to purchase gift cards or perform wire transfers. In some cases, the sender pretends to be a supervisor or colleague to make the message appear legitimate. These types of messages are known as "spoofed emails."

What is Email Spoofing?

Email spoofing occurs when a message appears to be sent from someone you know but is actually sent from a malicious attacker. Some of the most common spoofing emails come from someone you know asking you to perform some financial transaction for them. These transactions can include:

- Changing banking information
- Buying gift cards
- Mailing checks.

Spoofing is very easy to do and almost impossible to prevent. For example, spoofing is as simple as placing a false return address on an envelope when you mail something via the U.S Postal Service. In this example, the letter would appear to be sent from the spoofed return address printed on the envelope.

When someone spoofs an email address, the email account remains secure in most cases. However, you may begin to see undeliverable messages and unusual emails in your inbox. This is because the hackers are routing messages to your email address. The best course of action is to delete these messages and notify the CTS Help Desk at 412.396.4357 or help@duq.edu.

How Can I Tell If an Email is Spoofed?

Vigilance in identifying suspicious messages is the most effective protection against these types of attacks. A primary indicator of a spoofed message is when the known sending email address is different than the email address in the "reply to" field. This "reply to" address is most often a non-@duq.edu address created by the attacker. To learn more about identifying characteristics of phishing and spoofing emails, visit **duq.edu/phishing.**

What If I Responded to a Spoofed Email Message?

Faculty, staff, and students who have received or responded to one of these messages are asked to report it immediately to the CTS Help Desk at help@duq.edu.

For more information about spoofed messages, visit **duq.edu/safe-computing** and click on the *News and Alerts* icon.

Working remotely is a growing trend in the American workplace. While working from home offers many benefits for employees, it can also open more security risks for companies. If you find yourself working remotely, follow these tips to ensure your information, as well as your company's, remains secure.

Password Protect Your Home Router

Your home router acts as a "turnstile" all the network traffic in your house travels through. Still, many people forget to secure this important device, leaving it susceptible to hackers. At the very least, you should change the default username and password required to edit your router's settings. In addition, it is good practice to change your Wi-Fi password from time to time to block individuals or devices that may have gained access to your home network without your knowledge.

Avoid Allowing Family Members to Use Your Computer

Some companies provide a computer for employees to use when working from home. It is easy to forget that computer should only be used for work purposes. While it is tempting to allow a family member to borrow your computer to look up a recipe or complete a homework assignment, avoid doing so. If important work documents are accidentally deleted or accessed, or a drink is spilled on the keyboard, you are putting both yourself and the company at risk.

Do Not Store Personal Data on Your Work Computer

Personal data can include a myriad of items such as pictures, tax documents, and resumes. Since these types of files include information about your personal life, you should avoid saving them to a company-owned computer. If you access personal files on a work computer that you need to save, consider saving them to a personal cloud account or USB stick.

Avoid Connecting to Free WiFi

Whether you are working from home at a coffee shop, securing your network connection is essential. Using virtual private network (VPN) services when sending and receiving data across a public network helps ensure any network traffic remains secure and encrypted. To learn more about VPN services offered for Duquesne University employees, visit **duq.edu/globalprotect.**

SANS Cybersecurity Training Highlights

Last July, as part of a partnership with the SANS Institute, Computing and Technology Services (CTS) launched a cybersecurity training campaign for all Duquesne employees. This campaign aimed to raise awareness about common trends in cybersecurity and, most importantly, help teach you how to keep your information and identity secure. While CTS continues to stress the importance of current potential risks and safer online behavior, this information is never enough. An effective defense strategy requires a thoughtful combination of hands-on training, education, employee buy-in, and innovative technology that can identify risks before they become real threats.

A vast majority of data breaches are purely accidental, with no ill intent. From falling for a spear phishing campaign to mishandling confidential information, even a seemingly small mistake can open the door to a massive cyberattack. However, educating yourself and staying cyber aware can help minimize these risks.

CTS is always evaluating new methods and solutions to strengthen the effectiveness of our cybersecurity awareness training campaigns. We strive to help employees protect themselves, their families, and their organization in today's online world. Our recent campaign concluded at the end of October, which is national cybersecurity awareness month. The campaign was a huge success, with 713 employees completing the 10 modules and supplementary assessments.

1/3 DUQUESNE EMPLOYEES **COMPLETED TRAINING**

Four lucky winners were randomly selected and were awarded gift cards. We look forward to this year's upcoming cybersecurity training campaign and thank you for your contributions on making this prior year's campaign a success!

SECURING YOUR COMPUTER WITH SOPHOS

This past December, Computing and Technology Services (CTS) completed the deployment of **Sophos Intercept X** to university-managed Windows and Mac computers for malware and virus protection.

Sophos Intercept X employs a comprehensive defense-in-depth approach to endpoint protection rather than simply relying on one primary security technique. Some of these approaches include deep learning malware detection, anti-ransomware specific features, behavioral analysis, malicious traffic detection, and application control. These features allow for more scalability and higher performance than endpoint security solutions that use traditional machine learning signature-based detection alone.

Sophos For Personal Devices

Employees and students can download and install Sophos Home on personally owned computers and devices for free by visiting **home.sophos.com.** As part of the download process, users will be required to create a Sophos account. CTS recommends that users sign up with a non-@duq.edu email address for this step.

Sophos Home provides advanced, real-time protection from malware, ransomware, and hacking attempts. To learn more about Sophos Home, visit **duq.edu/sophos.**