The summer is a very important time here at Duquesne University. Our students are preparing for another academic year, our administration is closing out the fiscal year, and our faculty are preparing their upcoming courses. It is also an important time for the Computing and Technology Services (CTS) team. The summer for us means getting all of our systems and services upgraded, patched, and ready for students and faculty to arrive in the fall. These upgrades and patches are critical not only to provide the necessary IT services to our community but also to protect our University. Unpatched systems accounted for 85% of malicious exploits in 2016 according to the 2016 Verizon Breach Report.

While we at CTS hope you all enjoy a relaxing and refreshing summer break, we would also like for you to ensure that your devices are patched, updated, and protected with an endpoint security software before returning to campus. Applying patches as soon as they become available and turning on automatic updates for critical patches will help you protect yourself and others at Duquesne University.

We look forward to another great academic year with you at Duquesne University.

-Tom Dugas, Director of Information Security and New Initiatives

Computer Lab and Classroom Podium Login Changes Enables Use of MultiPass Accounts

Over the past several months, Computing and Technology Services (CTS) has been making improvements in our computer labs to enable the use of MultiPass to log into the computers. This improvement will provide additional security to your sessions while you work in the labs and ensure that
only authorized users are using Duquesne’s resources. In addition, logging in with your MultiPass credentials will create a temporary user profile for your account, which will grant an extra layer of privacy to your data.

Employee Windows Machines Receive LogMeIn Rescue Desktop Icon!

Employees will notice that Computing and Technology Services (CTS) has recently deployed a LogMeIn Rescue DU Help Desk icon to all Windows domain-bound computers. This icon will allow customers to easily connect with a Duquesne Help Desk Support Representative, or Educational Technology Support Representative for remote assistance.

When a Support Representative asks for your permission to establish a remote session, you will be able to click the LogMeIn Rescue DU Help Desk icon on your Windows Desktop and enter the 6-digit pin code provided by the representative to receive remote support. This icon will negate the need for customers to go to logmein123.com and download plugins to allow for remote assistance. However, the ability to go to logmein123.com will still be available in circumstances that require it.

Below is an image of the LogMeIn Rescue DU Help Desk Icon:

![DU Help Desk Icon]

Here are some key factors to know when using the LogMeIn Rescue DU Help Desk icon:

- Computing and Technology Services (CTS) will never initiate a remote session without first getting a support request from an employee. If you receive an invitation to a remote session and you have not sent a support request, please contact the Help Desk immediately.
- A Duquesne Support representative must provide customers with a 6-digit pin code in order for the remote session to begin.
- A Duquesne Support Representative cannot gain remote access to a customer’s computer without the consent of a customer. Customers will need to grant permissions to the consultant.
- The customer can end the remote session at any time via the LogMeIn interface.
- Your desktop background will turn black once the remote session is underway and will revert back to normal once the Duquesne support representative or customer has ended the session.
- The LogMeIn Rescue DU Help Desk icon is not available on Apple devices.
- Duquesne Support Representatives will need to continue to access the LogMeIn Rescue Technician Console in order to provide remote support.

If you have any questions or feedback regarding the LogMeIn Rescue DU Help Desk icon, please contact the CTS Help Desk by calling 412.396.4357 or emailing help@duq.edu and referencing ticket #331260.
Updated Office 365 Duquesne Email Web Login Page

Computing and Technology Services (CTS) will be implementing a new login page for Duquesne Office 365 Email.

This new web login page will feature an image of Duquesne’s Administration building as well as the important login information that is common to most other Duquesne applications.

All information regarding Duquesne’s authentication services can be found on our CTS website, here: http://duq.edu/about/campus/computing-and-technology/safe-computing/authentication

An image of the new Email web login screen can be seen below:
Are You Practicing Safe Social Networking?

Millions of Internet users engage in some type of social networking, and many of them assume they’re in a safe, controlled environment. However, social networking presents unique security challenges and risks.

Who Else Is Online?

When you use social media, do you think about who might be using it besides your friends and connections? Following are some of the other users you may encounter.

- **Identity thieves.** Cybercriminals need only a few pieces of information to gain access to your financial resources. Phone numbers, addresses, names, and other personal information can be harvested easily from social networking sites and used for identity theft. Cybercrime attacks have moved to social media, because that’s where cybercriminals get their greatest return on investment.

- **Online predators.** Are your friends interested in seeing your class schedule online? Well, sex offenders or other criminals could be as well. Knowing your schedule and your whereabouts can make it very easy for someone to victimize you, whether it’s breaking in while you’re gone or attacking you while you’re out.

- **Employers.** Most employers investigate applicants and current employees through social networking sites and/or search engines. What you post online could put you in a negative light to prospective or current employers, especially if your profile picture features you doing something questionable or “less than clever.” Think before you post a compromising picture or inflammatory status.

How Do I Protect My Information?

Although there are no guaranteed ways to keep your online information secure, following are some tips to help keep your private information private.

- **Don’t post personal or private information online!** The easiest way to keep your information private is to NOT post it. Don’t post your full birthdate, address, or phone numbers online. Don’t hesitate to ask friends to remove embarrassing or sensitive information about you from their posts, either. You can NEVER assume the information you post online is private.

- **Use privacy settings.** Most social networking sites provide settings that let you restrict public access to your profile, such as allowing only your friends to view it. (Of course, this works only if you allow *people you actually know* to see your postings — if you have 10,000 “friends,” your privacy won’t be very well protected.)

- **Review privacy settings regularly.** It’s important to review your privacy settings for each social networking site; they change over time, and you may find that you’ve unknowingly exposed information you intended to keep private.

- **Be wary of others.** Many social networking sites do not have a rigorous process to verify the identity of their users. Always be cautious when dealing with unfamiliar people online. Also, you might receive a friend request from someone masquerading as a friend. Here’s a cool hint — if you use Google Chrome, right-click on the photo in a LinkedIn profile and choose Google image
search. If you find that there are multiple accounts using the same image, all but one is probably fraudulent.

- **Search for yourself.** Do you know what information is readily available about you online? Find out what other people can easily access by doing a search. Also, set up an automatic search alert to notify you when your name appears online. (You may want to set alerts for your nicknames, phone numbers, and addresses as well; you may very well be surprised at what you find.)

- **Understand the role of hashtags.** Hashtags (#) are a popular way to provide clever commentary or to tag specific pictures or posts. Many people restrict access to their Instagram accounts so that only their friends can see their pictures. However, when someone applies a hashtag to a picture that is otherwise private, anyone who searches for that hashtag can see it.

**My Information Won’t Be Available Forever, Will It?**

Well, maybe not forever, but it will remain online for a lot longer than you think.

- **Before posting anything online, remember the maxim “what happens on the web, stays on the web.”** Information on the Internet is public and available for anyone to see, and security is never perfect. With browser caching and server backups, there is a good chance that what you post will circulate on the web for years to come. So: be safe and think twice about anything you post online.

- **Share only the information you are comfortable sharing.** Don’t supply information that’s not required. **Remember:** You have to play a role in protecting your information and staying safe online. No one will do it for you.

---

**Information Security Office Schedule of Events**

**Cyber Security Training Available July 1st**

Starting **July 1st, 2017,** Computing and Technology Services (CTS) will be offering online cyber-security training to all Duquesne employees as part of a partnership with the SANS institute.

This training will consist of a number of short videos that have been curated by CTS to answer the specific challenges faced by Duquesne. The videos can be viewed at your leisure and will take approximately 15 minutes to complete.

Employees will be notified of your training account information via your Duquesne email address. The message will come from the CTS Help Desk but the email address will reflect noreply@securingthehuman.org with information on how to login since the training is coming through our partner the SANS institute.

**Please note:** The login information for the Cyber Security Training is NOT your MultiPass account, but instead your full DU email address and a separate password that you will receive. If you have trouble logging in, simply click the “forgot your password? Click Here” option to have the password reset.
All employees who complete the training by September 29th, 2017 will be entered into a drawing for prizes!

For more information on the Cyber Security Summer Awareness training please visit www.duq.edu/cyberaware.

Be sure to start the summer off strong by educating yourself on current trends in safe-computing and cyber-security!