CYBERSECURITY DIGEST

Spring 2018

IN THIS EDITION

Data Privacy Tips from SANS
Storing & Securing Your Data
Recent Security Vulnerabilities
How & Why to Update Your OS
And More!

DUQUESNE UNIVERSITY
Computing and Technology Services

Letter From Director of Information Security

As October comes to a close, we can reflect on the 2017 National Cyber Security Awareness Month's (NCSAM) activities. During NCSAM, CTS campaigned using social media, events, and activities to promote cyber security awareness in our community. These activities included information on identifying phishing emails, protecting yourself from identity theft, owning your online presence, and keeping a clean machine. We also hosted an event open to all Duquesne University community members and local community members on the theme "Workplace Security is Everyone's business," which highlighted the challenges we face in this interconnected world. To see cyber security tips and news, please visit our CTS Twitter account @DuqCTS or the CTS website at http://duq.edu/cts , where you can get up-to-date news and tweets about cyber security events and activities.

Duquesne University's commitment as 2-time National Cyber Security Awareness Month Champion (NCSAM) is to promote and educate our community on ways to defend against cyber criminals.

While CTS has invested in our cyber security infrastructure, personnel, and skills to protect our campus community - it is not enough. We need you to remain vigilant in the fight to protect our community as well. Criminals will continue to become more sophisticated and persistent in their attacks. Please report any suspicious activity, emails, websites, or potential loss of sensitive data or equipment to CTS at help@duq.edu and 412.396.4357. With your help we can continue the fight against cyber criminals and protect our colleagues and friends as well.

-Tom Dugas, *Director of Information Security and New Initiatives*

Staying Safe Online

Major News Events

When a major news event happens, cyber criminals will take advantage of the incident and send phishing emails with a subject line related to the event. These phishing emails often include a link to malicious websites, an infected attachment, or a scam designed to trick you out of your money.

Kids and Family Members

If you have children visiting or staying with family members (such as grandparents), make sure the family members know your rules concerning technology that your kids must follow. Just because your kids leave the house does not mean the rules about what they can do online change.

Ransomware

Ransomware is a special type of malware. Once it infects your computer, it encrypts all of your files and demands you pay a ransom if you want your files back. Be suspicious of any emails trying to trick you into opening infected attachments or click on malicious links. In addition, backups are often the only way you can recover from ransomware.

Never Give Your Password Over the Phone

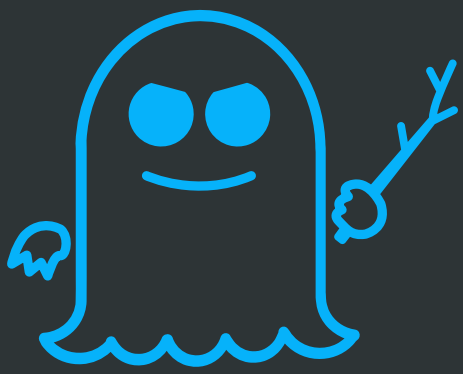
Never give your password to someone over the phone. If someone calls you and asks for your password while saying they are from the Help Desk or Tech Support team, it is an attacker attempting to gain access to your account.

Trust Your Instincts

Ultimately, common sense is your best protection. If an email, phone call or online message seems odd, suspicious or too good to be true, it may be an attack.

For more information on staying secure online, please visit **duq.edu/safe-computing.**

MELTDOWN



SPECTRE

New security vulnerabilities were announced on January 3rd, 2018 that affect computer processors on virtually all modern computers and mobile devices. They are referred to as Meltdown and Spectre.

What Do They Affect?

These hardware bugs allow programs to steal data which is currently processed on the computer. This includes secrets stored in memory such as passwords, encryption keys, photos, emails, and business-critical documents.

Meltdown is a flaw affecting laptops, desktop computers and internet servers with Intel chips, and allows hackers to steal data, including passwords that have been saved in Web browsers.

```
meltdown:
mov al, byte [rcx]
shl rax, 0xc
jz meltdown
mov rbx, qword [rbx + rax]
```

Sample code from Meltdown

Spectre is a bug affecting chips in smartphones and tablets, as well as computer chips from Intel and Advanced Micro Devices Inc. and allows hackers to manipulate apps into leaking sensitive information. While Spectre has been branded less dangerous than Meltdown, it is expected to be more difficult to patch.

```
if (x < array1_size)
   y = array2[array1[x] * 256];
```

Sample code from Spectre

What Can I Do?

As always, CTS recommends that you remain up-to-date on all patches and hotfixes for any computer hardware and software, as vendor patches are meant to help combat common exploits and reduce the likelihood of future cyber-security incidents.

For assistance with updating your Operating Systems, please visit the following links below:

Windows OS:

https://support.microsoft.com/en-us/help/311047/how-to-keep-your-windows-computer-up-to-date

Mac OS:

https://support.apple.com/en-us/HT201541

iOS device (iPad, iPhone, iPod):

https://support.apple.com/en-us/HT204204

Android OS:

http://www.ubergizmo.com/how-to/update-android-os/

For more information on Meltdown and Spectre, please visit **https://meltdownattack.com/**

Windows Updates

at Duquesne University

Each year Microsoft typically deploys 2 version updates to Windows 10 machines in order to keep them secure against cyber-threats and add new features. Computing and Technology Services usually installs these updates on Duquesne-owned machines during the night at the end of each semester so as not to affect faculty and staff members' productivity during the workday. However, if you'd like to install them at your own convenience, you have that option as well.

Please note: Updates will take approximately 45 minutes to install and you will not be able to work on your machine once you start the update. Before you install the update, be sure you close all open applications and save any work as the update will restart your computer.

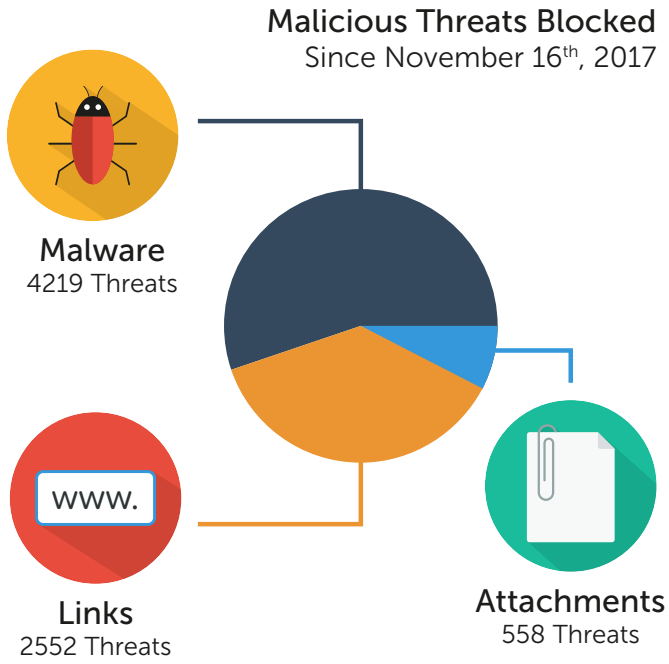
Remember, it is *extremely* important that you keep your Operating System up-to-date so that it possesses all of the recent fixes for any recently-discovered security vulnerabilities. Hackers are always finding new ways to attack systems. Most malicious malware is aimed at exploiting weaknesses caused by users not updating their systems. Your vendor's IT experts fight the good fight against hackers by sending you security patches, but they are no good unless you install them.

For assistance with installing Windows 10 updates on your Duquesne-owned machine, please visit **duq.edu/assets/Documents/cts/pdfs/Windows_10_update_instructions.pdf.**

Threats Thwarted By ATP

Last August, Computing and Technology Services implemented Advanced Threat Protection (ATP) as an extra layer of security against various cyber threats. Since November of last year, ATP has blocked 4219 malware threats, 2552 phishing links, and 558 unsafe attachments.

While tools such as ATP effectively reduce the number of cyber threats that enter Duquesne's technology environment, you are the best defense against these threats. Be sure to continue to follow safe-computing best practices and remain vigilant of suspicious emails. For more information, please visit **duq.edu/safe-computing.**



Keeping Your Information Stored & Secured

Duquesne University has many different storage options available to the campus community. The best storage option for your needs will depend heavily on the type and amount of data that you wish to store. With regards to Duquesne University's data, we have put together a helpful guide that can assist you in determining the sensitivity of your University data and where it should be stored. This guide can be found at **duq.edu/data-governance.**

Best Practices

A common best practice for backing up and storing your data is the 3-2-1 Rule which says you should keep 3 copies of your data on 2 types of storage media and 1 copy should be offsite.

- Having 1 copy offsite protects your data from local risks like theft, lab fires, flooding, or natural disasters.
- Using 2 different types of storage media improves the likelihood that at least one version will be readable in the future should one media type become obsolete or degrade unexpectedly.
- Having 3 copies helps ensure that your data will exist somewhere without being overly redundant.

Local Storage

While working on your data, you'll likely be using and saving your files on your desktop computer or laptop. Make sure to save often but also keep master copies in another location in case your computer crashes, is stolen, or falls victim to other unfortunate events.

Examples: local hard drive, USB drive, external hard drive

Pros	Cons
Data can be accessed easily and quickly	Not backed up unless you configure a back up drive
Data can be accessed without a network connection	The user is responsible for the safety of the data

Networked Drives

Networked drives are a good place for one copy of your data. They're managed by your school, department, or the university so they're quite stable. Talk to your department or Computing and Technology Services about the storage available on your networked drives.

Examples: CIFS and Einstein shares

Pros	Cons
Managed and regularly backed up by CTS	Off-campus access requires VPN
Offers an additional layer of security to protect your data	Data is only shared with Duquesne users

Cloud Storage

Storing your data in the Cloud is an easy way to meet the "1 copy offsite" piece of the 3-2-1 Rule. Cloud storage often allows you to sync your files from your computer, making backing up your data a simple process. However, most cloud storage solutions are owned by private companies, so your data may not be entirely private and the cloud storage company may possess the right to look at the data and do what it pleases with it. Additionally, some of these companies may go out of business or become obsolete.

Examples: Microsoft OneDrive for Business, BOX, Google Drive, Dropbox

Pros	Cons
Allows for synchronization of local storage, such as your computer's hard drive	Network connection required to access files
Ability to share folders and files with internal or external users	Storing data on a public cloud provider poses security and privacy concerns
Ability to customize permissions on files/folders	Data recovery options and customer support can be limited

Cloud Storage at Duquesne University

Faculty, students, and staff at Duquesne have access to a BOX account and a Microsoft OneDrive for Business account (through their Duquesne email). Microsoft OneDrive for Business is better for personal use, and contains 1TB of storage. BOX has been reviewed by Duquesne University's Information Security team and has been approved for storing internal and public data. It also contains unlimited storage. For more information on storage services available at Duquesne University, please visit **duq.edu/storage-services.**

Flash Drives

Flash drives are very convenient places to store data. However, flash drives, like all storage media, degrade over time. They are also very small and easily lost or broken. For this second reason especially, it is not recommended that one of your 3 copies of your data be stored on a flash drive.

Pros	Cons
Easily save and access data	Unreliable hardware
Easy to transport	Drives can become corrupt and result in data loss
Can access data on the move without a network connection	Small size makes them easy to misplace/lose

NEED HELP? Contact Us!

help@duq.edu

412.396.4357 (HELP)

206 Union
Hours:
Monday-Friday: 7 AM-5 PM
Saturday: 9 AM-4 PM
Sunday: 12 PM-4 PM

@DuqCTS