Fall 2014 Newsletter

Internet Safety – Same old thing with a few new twists

Seems like every newsletter there is some new set of malware infections or "innovative" phishing scams that we want you to know about. This fall is no different, so here they are.

1) **"Drive-by-download"** This one has been around for some time but it is getting more common and can be even more dangerous than before.

a. **So what is it?** It is a malware delivery system that is activated when you visit a hijacked website. All you have to do is go to the site. No clicking, no downloading required. The bad guys have inserted a very small piece of code into what might otherwise be a legitimate website. Once your browser "sees the page" the code is silently downloaded and starts working.

b. **What does it do?** That depends on the specific code that was downloaded. It might start stealing your private data and passing it back to the hacker. It might make your browser more vulnerable to other malware and you will soon be buried in a sea of popups, or you may receive a message that your files will be encrypted and no longer usable unless you pay them money – YES they can do that.

c. **What can you do?**

- Make sure to keep all of your programs up to date. Restart your computer at least once a week. This will allow the Windows updates to run.
- Make sure to keep your web browser up to date.
- If you are prompted to update software when you are on the web, don't update. Things like Adobe Flash, Adobe Reader, Java etc. update alerts may be fake and the "update" just a disguise for malware. It is sometimes very hard to tell the difference between a legitimate update or a hacked update. To be safe go directly to the company to check for updates. (adobe.com, java.com)
- Make sure your files are backed up. The J and K drives are backed up every night. Those files can still be infected, but we have a backup. Saving your often used and important documents on the J drive is a good idea. (See a later article for how to access those files from off campus.) If you store files on your computer, make sure you have a way to back up those files and run the back up regularly.

2) **Infecting yourself at illegal websites.**

Many of our students are victims of this method of infecting computers. Many – maybe even most students do their TV and movie viewing on the internet now. Sites like Netfilx and Amazon Prime are fine and don't pose a threat. Here is where the problem starts…. The new episode of the latest MUST SEE program isn't available on legitimate sites yet. So, if you want to see the latest "Walking Dead" episode (or insert your favorite show here) just "Google it" and you will easily find foreign sites where it can be downloaded for free. What is being downloaded is an illegal copy and usually full of malware. Don't be tempted by this. One student brought their badly infected laptop down for us to clean up. They told us they were infected by going to a website to watch a movie that had been assigned for a class. That website was serving up illegal copies of movies. If you find a site that is offering free access to movies that you normally need to pay for or episodes of TV shows that are not yet available to purchase, you can be pretty sure you are at an illegal site that will serve a large portion of malware with your movie.

3) **Have a Mac and think you are safe**…..well…don't get too comfortable. The same illegal websites mentioned above can also infect your Mac. We have had several student bring their Mac laptops in because they were buried in pop up ads. How did this happen? If you are using a Mac and you go to one of these sites, you will be asked to download and install a program to play the video. If you agree and put in your password, you will be downloading malware. Just remember – If a website

asks for the password to your computer you should be very suspicious. Make very sure you are at a reputable site and you really do want that site to install software on your computer and you trust the site. If you are not sure – don't do it.

For more information, see the ITS webpage on internet saftety. *http://www.augie.edu/information-technology/documentation-help/internet-safety*

Traveling Outside the US – Please let us know.

For several years our system has been set up to monitor where login attempts are coming from and it has made a big difference in the number of faculty/staff email accounts that get compromised. When an account is compromised the attacker can send hundreds of spam and/or maIware messages from that account. This very quickly gets Augustana on worldwide blacklists. That means that mail coming from augie.edu addresses goes either into spam filters or worse, it is blocked and never delivered to the intended recipient at all.

If you notify us of your travel plans, we can exempt your account from this auto checking. If you are not exempted, we get a text message **every time** you check your email from outside the US. (Some of you check your messages a lot when you travel!) Remember – it may be the middle of the day where you are – but it may be the middle of the night here. This is EXTREMELY important if you are traveling in a country that is known as a safe haven for hackers. If we see your account being accessed from a place like Nigeria, China or Russia (and others) and we don't know that you are really there, it is VERY LIKELY that we will disable your account until we can confirm that it is really you checking mail. Please let me know your plans.

Invite ITS to your Department Meeting

Interested in having ITS attend one of your department meetings? We would love to come and talk about the technology challenges you have and your technology wish lists. Sometimes we can solve your problems on the spot, and with other things we will need to do a little research or setup. We can't solve every problem, but we would like to try.

If your department would like to get on the schedule, please email Cheryl to set up a time.

Software in Computer Labs

Faculty – if you have new software you would like to have installed in the computer labs for Interim or Spring semester, please get that to us ASAP. We have a short window of time to change the lab between semesters, so the more advance notice you can give us the better.

Office Phone System Refresher - and the DND button.

It's been over a year since we installed the new phone system and it may be time for a refresher on features and buttons that may benefit you. An office phone system overview and a voice mail overview are available at *www.augie.edu/phone-services*

Note that one "feature" that a few people have accidentally enabled is DND (Do Not Disturb). Most phones have a button closer to the top of the LCD screen labeled DND. DND stands for Do Not Disturb, and it does just that. If it is pushed and lit, no calls or beeps will come through to your phone, all will go directly to voice mail. This feature allows you to hold serious meetings with students, clients, and others in your office without being disturbed. The only way to know that DND is on is to look at the button next to DND on your phone, if it is lit red, it's on. Otherwise it's off and you will receive calls.

Technology needs for the 2015/2016 year

Time to start thinking about your technology needs for next year….I know..it seems early but the due date always comes faster than we expect. Requests forms will need to be submitted to the committee in mid January. Watch for the official announcement from Dan Drenkow in early December. Procedure and Guidelines can be found at *http://augie.edu/information-technology/policies/its-budget-request-procedure-and-guidelines*

Technology Purchases

Just a reminder that all information technology purchases must go through ITS to be fully supported. Here is a link to the current policy for Information Technology purchases.
http://www.augie.edu/information-technology/policies/policy-information-technology-purchases

Getting to the J and K drive from home or mobile devices.

If you would like to get to the J or K drives from off campus or from your smart phone or tablet, these instructions will help you connect.

If you are setting this up on a phone or tablet, search your App Store for the free Novell Filr app. When it asks for the server name use*https://mariner.augie.edu:8443.* User your regular Augustana username and password.

Apple Devices – *https://itunes.apple.com/us/app/novell-filr/id575729298?mt=8*
Android Devices - *https://play.google.com/store/apps/details?id=com.novell.filr.android&hl=en*

If you want to use your computer to access the drives, just type *https://mariner.augie.edu:8443* into the browser address window and then login with your normal Augustana information.

Once you are logged in with either method, you will see your J Drive. If you would like to get to a K drive folder, click on the Net Folders icon at the top.

Email on Smart Phones and other Mobile Devices

If you have recently purchased a smart phone or other mobile device and would like an easy way to read your Augustana email, stop down to the Help Desk and we will be happy to get that set up for you. If you would like to try setting it up yourself, instructions can be found on the ITS website. *http://www.augie.edu/information-technology/email* If you do the set up yourself, you will need to contact the Help Desk so we can authorize your account for mobile access. Just give us a call or send an email to helpdesk@augie.edu