The Twist: by Ron McCarville

Touchscreen technology is component of a significant portion of the laptop market, at least on Windows side of things. Recently, there has been an influx of touchscreen laptops purchased in AHS. These laptops are extremely light but have significant computing power.

Recently, Associate Dean, Ron McCarville purchased a Lenovo Twist from the Campus Tech shop right here on campus. Ron was so pleased with his purchase, we asked him to give a review, from the perspective of a user. In his words,

“I want to begin with an admission. I have not a clue about technology. I have been asked to review the Twist Ultrabook and I have no knowledge of its inner workings. It’s like being a passenger in a 747. I don’t know a thing about why or how it flies. I know only how satisfied I am with that flight. The same holds true for the Twist. I don’t understand its technological specifications but I do know how well it works. And it works very well. I love this computer. It has a typical laptop configuration but the “twist” capacity lets it operate as a tablet as well as a traditional laptop. It is the first of a dozen or more personal computers and tablets I have owned that seems to do everything I ask it to do. It is light and portable, it is fast with lots of memory, and best of all, it is functional. I can edit, create, browse, and display wherever and whenever I desire. The touch feature is particularly useful. I love how it eases navigation and movement from one screen to the next. Once you become accustomed to the touch screen you may begin to consider the mouse & touch pad as antiquated relics of years gone by.”

Imagine if You Lost Everything!!!

Imagine if you lost everything?
What if you lost all of your music?
What about the years of digital photos you’ve taken?
Or even worse your research data!

The image to the left is making the rounds on Facebook and it looks to be a legitimate story.

Do you have a backup strategy? You should have a backup in multiple places, make sure it is encrypted, stored on various types of media (USB, DVD etc) and that you can read/restore the backup.

The best way to avoid a scenario like this at work? Save all of your files to your N: drive!
AHSCO Summer Update

Sometimes people think the Computing Office sits around all day surfing the web and drinking coffee. That’s not true... Craig doesn’t drink coffee. All joking aside, the spring term is a time to do development, implement new projects and to upgrade systems.

With the Campus IT Strategic Plan soon to be released and the AHS Strategic Plan and the Waterloo Strategic Plan 2013-2017, there will be a plethora of initiatives and projects. In response, AHS Computing will soon be holding its annual planning session to address areas covered in each of these plans.

Two of the major initiatives spawning from the strategizing will be an investigation into Virtual Desktops for students (so they can access course software like SPSS and SAS from offsite locations) and shared data space for AHS researchers (in an effort to consolidate vulnerable NAS drives).

We will also be implementing a campus wide asset management system and investigating a request tracker (RT) system.

Currently we are working on getting an instance of Windows 2012 implemented. This will be a replacement for our current ahcoserv which is providing IP addresses to the student computing lab, acts as the faculty print server and is our software repository. Old hardware will be repurposed as a replacement for ahssstore (our archiving repository).

Windows 8 is on our horizon as well. We are working on building images for deployment. Large scale distribution of Windows 8 in AHS is not likely, however, we like to be prepared. That being said, Office 2013 is ready to be distributed. If you would like it to be installed on your PC, please let a member of AHS Computing know.

Green IT initiatives are being considered as well. We are working on collecting data to demonstrate the electrical savings of smart power bars (where a master device, most likely your PC, controls the outlets in the power bar based on whether it is turned on or not).

Finally, our summer seminar series is under way, for details on booked sessions please visit our Events Page. There are lots of interesting topics for everyone in our faculty. If you have a suggestion for a topic, please pass it along to a member of AHS Computing.

10 Security Mistakes That Are Easy to Avoid

Computer security is about being vigilant. Whether you are working on a PC, Mac or even running Red Hat (we doubt you are but one never knows) security is about protecting your computer and your identity.

1. Using poorly chosen passwords—Don’t create passwords that are easy to retrieve by someone looking at your Facebook page (i.e. DOB, Anniversary Year or middle name). Mix things up. Pass phrases are even better. For more info on passwords check out the archive of an AHSCO Seminar

2. Never changing passwords—People who keep the same password forever and use the same password on multiple sites are more likely to suffer a breach. There are people in AHS who still have the old ‘callixxxx’ password (ask someone who’s been in AHS 10+ years what that means)

3. Not installing antivirus/anti-malware—If your PC is joined to the NEX-US domain, we take care of that! However, if you have a laptop or are running a Mac make sure to install Symantec Endpoint Protection or Microsoft Security Essentials

4. Never patching machines—Same as with Anti-Virus, we take care of all PCs joined to NEXUS. Outside of that it is your responsibility to keep your computer up to date. Why? Operating system and application vendors release software patches for a reason. While many updates add new functionality, many correct security flaws in products.

5. Insecurely storing data—How many of you have stored sensitive data on a USB drive? Do you ever take drive with you out in public? Un-protected data is a big deal. A single lost USB drive, laptop, iPad, or tape with the wrong information can land an organization in a mess financially, legally, and from a public relations perspective. Our recommendation, store files to your N: drive, encrypt all laptops and USB Devices. See a member of AHS Computing for assistance.

6. Never testing backups—if you make a backup, make sure that it has everything that you need it to. Also make sure that it is stored in a different location that the device that it is backing up.

7. Never run as an administrator—Have the account that you primarily use be a simple User account. Why? If your computer is compromised while you are logged on as a User the chances of anything terrible happening are reduced because as a User you don’t have access to break any operating system files.

8. Forwarding chain email without checking it first at Snopes or some such place— Be smart and courteous. Not everything you read is true!

9. Printing— As soon as you print something, it is not secure and might end up in the wrong hands, plus it isn’t very green.

10. Leaving your keys laying around or leaving your office open when you are not there—this may not sound computer related but once someone has your keys they have access to everything in your office, your computer, credit cards and your identity.

AHS Computing has a YouTube channel!

The AHS Computing Office recently opened a YouTube channel for the purpose of sharing informational videos with the faculty, staff and students of Applied Health Sciences. The first video posted was a recording of a recent Excel tips seminar. The Computing Office will continue recording seminars and will also be creating tutorial videos for topics such as getting onto Eduroam, connecting using the VPN and using remote desktop. The YouTube Channel is the latest addition to the AHS Computing Office social media suite, currently including Facebook and Twitter. Be sure to check us out on each of our social media accounts for up to date information on the state of computing at Waterloo as well as tips for web and computer use.