

Know IT



Volume 8, Issue 1

Information Technology Newsletter

February 2009



ShoreTEL VoIP Training Wrap-up and Support Materials Reminder

Training sessions were successfully held for the new ShoreTel VoIP phones in December and January with approximately 250 faculty and staff members attending sessions. Many thanks to Kathy Moore,

Debbie Cox, and Chris

Cameron of Accent for assisting in the planning efforts and conducting the training sessions!

Now that the new ShoreTel VoIP phone system is in place and operational, and classroom training sessions are complete, Information Technology Services would like to remind users about other support materials for the system.

For additional support, you also view online training videos for the new system. You can access the videos at:

http://our.sinclair.edu/sites/its/itswebsite/it_policies/procedures/its/voice/voiptrng.html.

Click on the individual links on the page to view each video. Many thanks to Jai Rezy, Rob McNally, and Greg Deye of Learning Technology Production for working with us to create these videos!

An online manual for the VoIP system is also available at:

http://our.sinclair.edu/sites/its/itswebsite/it_policies/procedures/its/voip/voip/voice.htm

A quick guide for using your new phone is found at: http://our.sinclair.edu/sites/its/itswebsite/it_policies/procedures/its/voice/230%20IP%20Phone%20Quick%20Guide.pdf

A quick guide for using your voice mail is found at: http://our.sinclair.edu/sites/its/itswebsite/it_policies/procedures/its/voice/Voice%20Mail%20Quick%20Guide.pdf.

In this issue...

- ShoreTEL VoIP Training Wrap-up
- Cell Phones are Attack Targets
- PC and Gadget Recycling
- Prevent Eclutter Before It Happens
- What is a Webinar?
- You Want Your Application Where?
- Happy 25th Anniversary to the Original Macintosh!
- A Short History of the @ Sign

A pocket guide for the new phones and a card for voice mail access numbers can be picked up in room 13000. Many thanks to Kelly Vogelsong in Publications for working with us to create these resources!

Cheryl Stewart



Information Security Corner

Cell Phones are Attack Targets

Everyone is mobile today. People's lives—business and personal—are meshed via the always-on connectivity provided by our cell phones. Many of these devices have advanced well beyond “phones” and are in reality very powerful mini-computers that are complete with office applications and Internet connectivity. Unfortunately, as our phones become more technologically advanced, capable, and valuable, they are also increasingly attracting the attention of criminals and other attackers who are continually looking for—and finding—new ways to target victims. Cell phones pose some unique risks, mainly due to the typical user's perception. Nearly everyone is aware that their desktop/laptop computer is subject to connectivity-based attacks—but almost no one thinks of their phone as a computer that is subject to the same attacks!

Most cell phones have the ability to send and receive text messages (which essentially are the phone equivalent of email), and many smart phones have full email and Internet capability. Some typical cell phone attacker goals include:

- Abuse of Service - Most cell phone plans limit the number minutes you can use and text messages you can send and receive without extra charge. Some attackers spam text messages simply to harass their victims and force them to pay additional fees. A more advanced type of attack involves the attacker infecting your phone with malicious code that allows them to access and use your service. Because the contract is in your name, you will likely be held responsible for the charges.
- Phishing Attacks- Phones that provide email are targets for standard phishing attacks, and attackers are using text messages for phishing as well. The attacker spoofs messages that appear to originate from the service provider or other legitimate business in an attempt to get you to provide sensitive information such as account numbers and passwords. A sub-set of this attack uses text/email to lure the cell phone user to a malicious site to install malware.
- Harvest or “own” your phone – Similar to the botnet attacks a standard computer is subject to, cell phones are also now subject to being compromised and controlled by attackers. The attacker gains control over your phone, then uses it to harvest additional phones by contacting those in your phone's address book. The phone can also be used for other attacks such as phishing.

Continued from Page 2

As our phones continue to increase in capability, the attackers will likely escalate their attacks. Cell phone users, and particularly “smart phone” users, need to take effective measures to protect their devices. The most important protective measure is changing the way you think—your perception—of your phone. Your phone is no longer a device that simply connects two points together to permit voice communication, it is a device that can connect to and be connected to by multiple points, often simultaneously, and sometimes unknown to the user. It is also capable of storing much information—some of it confidential. Follow similar rules with your cell phone as you should for your computer, including:

- Be careful about posting your cell phone number and/or email address on the Internet, especially on social network sites such as MySpace and FaceBook. Attackers use software that crawls Web sites harvesting telephone numbers and email addresses.
- Do not follow links sent in email or text messages. Be particularly suspicious of any URLs sent in unsolicited email or text messages. Never respond to the sender!
- Be wary of downloadable software. There are many sites that offer games, ringtones, music, and other software you can load on your cell phone. Many of these are legitimate, but there are many that are malicious. Avoid downloading files from sites if you cannot verify it is a reputable site that guarantees its software is free from malware
- Evaluate your device’s security settings - Make sure that you take advantage of appropriate the security features offered on your device. Some basic features include password protection at startup, encryption of stored information, clearing of memory/cache, and securing Bluetooth. One of the best security measures is disabling unused or unneeded services. If you do not use Bluetooth—turn it off!

Cell phones and other portable devices have certainly elevated our connectivity and ability to communicate conveniently while on the go. As we increasingly use and rely on this rapidly changing technology, we need to ensure we do so safely and securely!

Dan O’Callaghan, CISO





PC and Gadget Recycling

Today's technology allows us to continually upgrade our computers and electronic gadgets so we can have the latest and the fastest. Because the prices of items such as calculators, laser pointers, mp3 players, USB drives, and CD and DVD discs have fallen so drastically, many times these items are seen as disposable.

Buying new has become easier and provides increased performance but this flexibility comes at a high price. Landfills are filling up with old PCs, cellphones, media players etc. Just tossing your old computers and electronic gadgetry is not only irresponsible but also ecologically dangerous. Some older electronics may be valued by nonprofit organizations or by individuals in developing nations while many of the materials used in electronics are toxic and dangerous when dumped into our ecosystems. In addition, recycling electronics can recover valuable materials and save energy. Carelessly tossing your gadgets can also endanger your personal information and privacy!

The Environmental Protection Agency has valuable information on donating or recycling electronics at their web site. Some useful EPA links are:

- Where Can I Donate or Recycle My Old Computer and Other Electronic Products?- includes information about manufacturer, retailer, and government-supported programs <http://www.epa.gov/waste/consERVE/materials/ecycling/donate.htm#local>
- Where You Live – includes an interactive map to find information about regional and State electronics recycling programs <http://www.epa.gov/waste/consERVE/materials/ecycling/live.htm>
- Basic information on reducing and reusing <http://www.epa.gov/waste/consERVE/materials/ecycling/basic.htm>
- Recycle Your Cell Phone. It's an Easy Call <http://www.epa.gov/waste/partnerships/plugin/cellphone/index.htm>

Numerous nonprofit organizations will take donations of electronics. Organizations such as the Goodwill will take these items and repurpose them or sell them in the organization's stores. Another example is Cellphones for Soldiers (www.cellphonesforsoldiers.com) which turns old cellphones into minutes of prepaid calling cards for U.S. troops by sending the phones to ReCellular which pays the organization for each donated phone—enough to provide an hour of talk time.

Continued on Page 5

Continued from Page 4

You should also remember to properly dispose of the batteries used in electronics as they also contains toxic materials! Laptop, alkaline, titanium, NiCad, NiMH, 6V, and 9V batteries all contain harmful chemicals. Don't just toss old batteries into your weekly trash but instead contact your local waste disposal facility on available procedures to dispose of old batteries. Another tip is to buy rechargeable batteries and a charger. They cost more to purchase initially but save money and resources in the long run due to their ability to be recharged. In addition, a device called REZAP that can charge both throwaway and rechargeable batteries of almost any kind is available for purchase. Always carefully follow any instructions that come with a battery recharging device!

Before donating, recycling, or disposing of any PC or other electronics such as smartphones, external hard drives, or USB drives that can contain personal information, you should be sure to use software or other utility to either wipe data from the devices or make them inoperable. Identity thieves target these items!

NOTE: You do not have to worry about recycling or donating Sinclair-owned electronics such as PCs, monitors, printers, and scanners as these materials are surplused at the end of their useful lives. Data is also wiped from these electronics before they are surplused.

For additional information about the surplus process, go to

http://our.sinclair.edu/sites/its/itswebsite/it_policies/procedures/its/srpls/srpls.htm.

Cheryl Stewart



Prevent Eclutter Before It Happens

In a previous issue, we published information about dealing with Eclutter on a PC. This article will talk about ways to stop digital debris before it happens and help you not to become a digital packrat. As Ben Franklin wrote, an ounce of prevention is worth a pound of cure!

1. **Keep things simple.** Before you save or download something to your PC, ask yourself if you can just delete it instead. Instead of purchasing or asking for more storage, see if you can purge or delete files that are not required instead. Use a simple filing system using simple file and folder names. Only bookmark essential and frequently accessed websites. Don't create unnecessary shortcuts on your PC's desktop.
2. **Create purging routines.** Just as it is important to purge your home of unwanted or unnecessary item, you should also clean your PC of data that is no longer required. Put purging reminders in your calendar.
3. **Stop saving junk.** Choose to save only required or important items and then trash the rest. Every time you are about to save or download something, ask yourself twice if it is really valuable or just junk. Make this a regular practice. If you absolutely can't decide on an item, create a Junk folder and save it to that folder. Review your Junk folder once a month and you will probably wonder why you saved a lot of the items in the first place!
4. **Create archives.** For older items that you do not access on a regular basis, create an archive folder or area. You can do this for data files and for email. Archiving will put older items in storage and allow you easier access to current and frequently used items.
5. **Follow records retentions schedules for College records.** Some items access or created on your College-owned PC or laptop may fall under records laws and requirements. Become familiar with your department's records retention schedule. Contact Records Management & Archives at X2113 for additional information.

For additional information on handling digital debris, go to:

http://our.sinclair.edu/sites/its/itswebsite/it_policies/procedures/its/Digital%20Debris.pdf



Cheryl Stewart

What is a Webinar and where can I participate in one?

What is a Webinar?

The term Webinar is short for Web-based-seminar. It is generally a presentation, lecture, workshop, or seminar that is transmitted over the Internet. Because using this technology saves travel time and expense, Webinars are becoming a popular way of presenting and attending seminars.

Webinars involve synchronous communication which means these sessions are live and must be viewed at the time of the presentation. Though it is possible to transmit both audio and video over the Internet, typically webinar's provide one way video over the internet and use a speaker phone to both transmit and receive audio communication.

Where can I participate in a Webinar?

Since Webinar's often involve the use of a telephone for the two-way conversation portion and sometimes for the audio for the webinar itself, an office or meeting room equipped with a speaker telephone, a computer with Internet access, and a projector or other viewing equipment is usually required.

Webinars viewed by a smaller audience (generally one to five people) can be viewed right from your desk. If you choose to participate from your office you may wish to purchase a headset so that you can hear the audio without disturbing others in your office.

For larger groups there are meeting rooms and classrooms well suited for the receipt of a webinar. Contact Registration to find out available locations for your Webinar session.

For more information on Webinars and their viewing requirements, contact Suzanna Smith, Manager, Multimedia Services at 937-512-4264.

Suzanna Smith



You Want Your Application Where?

ITS maintains the Windows “Images” in over 200 campus computer classrooms, which contain over 700 different applications in approximately 70 combinations. In the past the installation of any new application into an image required the creation of an installation script which had to be run on the computers that the software was made available on. The amount of time required to install the applications in an image and the testing required due to the possibility of conflicts between the applications has caused our response time for changes to images to be longer than we would like.

In an attempt to improve our response time for image changes and to promote the flexibility of computer classroom use ITS has begun using an “application virtualization” program from Microsoft called App-V (formerly SoftGrid – see FY09 IT Master Plan). Using App-V, application installation modules are created once and re-used without the current testing for conflicts because each application runs within its own virtualized environment. This will also allow completely new combinations of applications to be created dynamically.

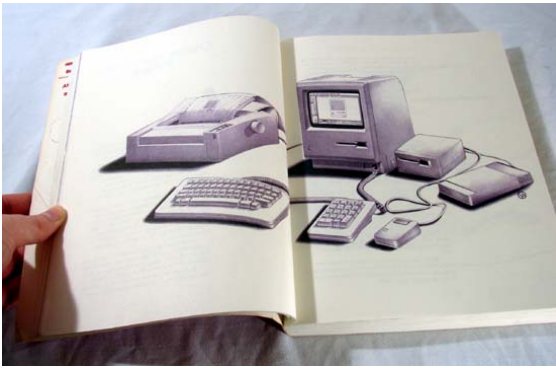
Because of the way that App-V allows applications to be assigned to users and dynamically installed when they are used, the possibility of using applications in any space on campus becomes possible. This has great benefits over the way that full application installs are done within physical spaces. ITS is already using App-V to deploy applications to campus computers and we are re-building whole images that are used in academic classrooms and labs.

Our goal, by Fall 2009, is to allow a student to login with their own ID and access the applications that are used for the specific classes that they are registered for. ITS has already converted about half of the 700 applications in the classroom images to App-V. We also have created procedures that automatically assign these App-V applications to student logins based on the classes that the student is registered for.

In addition to allowing students to login anywhere on campus and receive these applications, we have recently begun testing the capability of providing these same applications remotely via the Internet using an additional capability of App-V called “App-V for Terminal Services”. The HIM department is currently using this system to provide remote access to software that previously was only available in a campus classroom.

Using this new capability Sinclair will be able to increase regional access through the promotion of on-line learning and off-campus instruction. Also, the college will be able to offer increased opportunities for students to learn on their own schedule and without traveling to campus. We will be providing more information about App-V’s capabilities over the next several months.

Scott McCollum



Happy 25th Anniversary to the Original Macintosh!

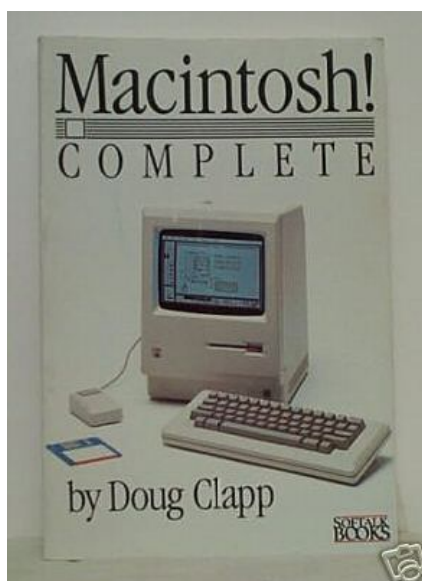
The original Macintosh personal computer celebrated its 25th anniversary on Saturday, January 24, 2009. It was the first personal computer to appeal to the masses, introduce a mouse pointing device, and use a graphical user interface instead of text. This personal

computer was the first to appeal to millions of people and to change the view of computers as toys for playing simple games or as tools reserved for engineers and scientists. Its popularity eventually resulted in it being given the nickname, the Mac.

The Macintosh first gained notoriety with its \$1.5 million commercial directed by Ridley Scott and shown during Super Bowl XVIII on January 24, 1984. Its '1984' Orwellian theme warned against conformity. I remember watching it with my Dad during that game. After the commercial was over, he turned to me and said, 'Why would anybody ever want one of those in their office or home?' Well, times change!



The Macintosh project began in the late 1970s with Apple employee Jef Raskin's vision of an easy-to-use, low cost computer for the average consumer. He wanted to name the computer after his favorite type of apple, the McIntosh, but the spelling had to be changed slightly for legal reasons. Raskin assembled a large development team, and its work caught the attention of Steve Jobs, co-founder of Apple, who felt that the Macintosh had more commercial appeal than another Apple product, the Lisa computer. Raskin left the project in 1981 over conflicts with Jobs, and the final product is said by some to be closer to Jobs' concepts than Raskin's. Jobs also left Apple in 1985 but returned to the company in 1996.



The original Macintosh came bundled with only two applications, MacWrite and MacPaint. Eventually, existing text-mode and command-driven applications were redesigned around the Mac's graphical interface with Microsoft Word being the most famous. Original system specs included 128k of RAM, an internal floppy drive (no hard drive), 9 inch screen, keyboard, and single-button mouse.

Continued on Page 9

Continued from Page 8



The Macintosh was also one of the first 'mobile' computers in that a carrying case was available for purchase to assist with 'easy' transport of the machine. Case, computer, and peripherals weighed approximately 30 pounds!

The original Macintosh still inspires devotion among computer users. Collectors trade the computer enthusiastically on Ebay, and several Macintosh museums are in operation. Owners have also come up with some creative uses for their Macs including custom paint jobs and Macquarium conversions!



COURTESY MIKE TUOHY



COURTESY AVNER RESEHF

Science fiction author Douglas Adams was one of the first owners of the original Macintosh.

The Macintosh or Mac name still has a faithful following with current products such as the MacBook, the Mac Pro, and the Mac Mini. Happy 25th!

Cheryl Stewart

A Short History of the @ Sign

It is so ubiquitous today that most people wouldn't even give a second thought to that little symbol in the middle of their email addresses but, yes, the lowly @ (at) sign actually has a history.

One of the most widely used symbols in English doesn't even have its own special name like the ampersand, semicolon, or period symbols have. It is simply called the 'at' sign because it symbolizes the word 'at' in price quotes or rates such as to buy three pounds of potatoes @ (at) \$2 a pound.

However, elsewhere in the world, this symbol has taken on some very interesting names. The Dutch call it an apestaart which means monkey's tail while the Germans call it a Klammeraffe which means spider monkey. Russians see a dog somewhere in the @ symbol as they use the word, sobachka or little dog. The feline population is also represented as Finns call it kissanhäntä or cat's tail. Swedes call it a snabel or elephant's trunk while the French see snails in @ and call it an escargot!

The origin of the symbol @ is the French preposition à meaning 'to' or 'at' in expressions like: dix pommes à Euro (ten apples a Euro). In English, the accent over the 'a' eventually disappeared and the use of 'a' meaning at or per developed in English expressions like 'five dollars a pound' and 'twenty miles an hour' before we transformed it into @.

Today @ is most widely used as an indicator of an e-mail address, e.g. joe.schmoe@sinclair.edu, separating the account name from the domain name. Loosely interpreted that would be Joe Schmoe's account at the Sinclair domain.



Cheryl Stewart

ShoreTel VoIP Phone Tip: Forwarding Your Extension

If you are going to be out of the office and want to forward your extension to another extension, follow the steps below:

1. Press the Options button
2. Enter your Voice Mail password
3. Press the OK soft key
4. Use the scroll button to put the arrow next to Call Handling
5. Press the Edit soft key
6. Use the scroll button to put the arrow next to Out of Office
7. Press the Edit soft key
8. 1101 is displayed under CallFwd Dest: Press the Back soft key four times to delete it. Use the key pad to type the extension you wish to forward your calls to.
9. Press the OK soft key.
10. Press the OK soft key.
11. Press the Done soft key and you will be returned to the main display.
12. When you are going to be out of office and wish to forward your calls, press the Mode soft key.
13. Use the scroll bar to select the Out of Office mode and press the OK soft key.
14. Remember to put your phone back into Standard mode when you return to the office.
15. If you wish to change the number that you want your calls forwarded to when you are out of office, repeat steps 1-12 above.

NOTE: Per phone etiquette, always notify the party associated with the extension that you are forwarding your extension to that you have forwarded it.