Technology Options for Workplace Communication

Effective communication is important for all work environments. In the not so distant past, workplace interaction was accomplished with face-to-face meetings, memos, and telephone calls. In today's fast-paced business environment, technology has facilitated alternatives to achieve interaction and foster communication. Communication can be instantaneous and interactions immediate by using multimedia software. At TTU, e-mail, instant messaging, web conferencing, and Internet voice calls are some of the most widely used multimedia communication tools. At one time, multimedia communications required a variety of programs and applications. With the implementation of Microsoft's Office Communications Server (OCS), these multimedia tools and other powerful options are integrated into one program—Office Communicator.

This summer, the TTU IT Division will make these multimedia tools available through the latest version of Microsoft Office Communicator. For those of you that already use the current version of Microsoft Communicator, you will update your version to take advantage of the new integrated tools. To upload the software or upgrade your current version, please visit the eRaider website (eraider.ttu.edu). Watch TechAnnounce for web-based instructions that will guide you through the simple 5-10 minute software installation.

To download Communicator or upgrade your current version, please visit the eRaider software download website (eraider.ttu.edu). In addition to the current software functionality, the new Communicator software has the following features:

Real-time communications—Office Communicator is an ideal companion to e-mail for real-time communications and information. You can find TTU individuals by using the built-in search or by adding them to your personal contacts list. All of your chat conversations may be automatically archived in your Outlook Inbox (by each individual user). Collaborating with others with voice and desktop sharing can increase your efficiency dramatically. Note that drag and drop file transfers are scanned by OCS anti-virus software to ensure your system's security.

Conferencing—You will be able to schedule multi-party phone and computer conferences directly from Outlook using meeting requests. (Conferences can be totally spontaneous, too.) As a result, audio conferencing will be much simpler to schedule and use. Participants can use either a desk phone, mobile phone, or their computer with Communicator to join the audio conference. Office Communicator clients will be able to add video and/or desktop sharing among participants, along with instant messaging (IM) chats.

Public Internet Connector—Do you need to chat with people using Yahoo, MSN or AOL clients? No problem! Just add their IM addresses to your Communicator contact list and you will be able to get their presence information and chat with them over secure communications links.

Streamlined desktop sharing—Office Communicator has been enhanced to simplify desktop sharing. Any conversation or multi-person conference can quickly add desktop sharing without having to launch any other programs. Viewing information together can streamline computer support, facilitate discussion, and enable real-time collaboration.

Online “webinars” and meetings—Live Meeting provides the means to have online meetings with anyone on the Internet. Participation in a Live Meeting can be with anyone inside or outside of Texas Tech University, provided they have the appropriate software. Setting up a Live Meeting is no harder than scheduling a meeting through Outlook. Combined with the new conferencing capabilities of OCS, you can have Live Meetings that allow attendees to dial-in from their telephones or use voice/video over the Internet with the new Communicator software. Unlike hosted services, TTU's OCS environment hosts Live Meeting on-premise; therefore there are no fees for the service.

If you are new to the Texas Tech University OCS environment or want to learn more, there are self-paced tutorials on both the Microsoft Office Communicator and Microsoft Live Meeting home pages. In addition, Technology Support will offer classroom ShortCourses this fall. To assist departments and areas that are interested in how Office Communicator and Live Meeting work, Telecommunications Services will be happy to demonstrate the software and answer questions. If you are interested, please contact Audrey Pekowski at (806)742-8000.

Botnets

The terms virus, Trojan horse, and worm have become synonymous with the on-going struggle users face to maintain a secure and fully operational computer system. As malicious software continues to become more sophisticated, a new type of threat has quickly become a primary weapon for cyber criminals—botnets.

Botnets, short for robot networks, are comprised of multiple computer systems infected with a virus, Trojan horse, or worm with the intent to later pass on further instructions, turning the infected computers into relay tools for hackers. After multiple computers have been infected by the same source, the network of infected computers simultaneously receives instructions from the attacker for further action. Botnets are not always used for data and system destruction, some have been found to collect user information such as Internet browsing history that is later sold to solicitors or spammers. Without your knowledge, your computer may fall victim to a botnet attack and be used to cause harm to Web sites, spread viruses, or commit identity theft against individuals.
Botnets often do not disable a computer entirely since Internet access is needed for the botnet to receive instructions and to work maliciously against other computer systems, which can make detection difficult. Botnet infected computers often run more slowly than usual, display unexpected messages, and work in a manner other than what the system owner intends. Some of the common identifiable symptoms of a botnet-infected computer include:

- You are unable to run programs that have previously run without difficulty;
- Your computer responds to commands and access the Internet more slowly than usual; and
- Your hard drive spins (constant whirring noise) when computer is not in use.

**Suggestions to avoid botnets and other infections:**

- Keep your computer updated with the latest version of operating system and software;
- Keep antivirus and antispyware software updated and make sure both are set to scan regularly;
- Do not click on links contained in an email message unless you are certain of the sender’s identity;
- Only open email attachments which you are expecting and can verify the sender and content; and
- Use a personal firewall for your personal systems and networks; many botnets are designed to avoid detection by antivirus clients and a firewall serves as a strong second line of defense.

For assistance with an infected TTU computer system, you may contact IT Help Central at (806) 742-HELP (4357).

**The Flutter about Twitter: Tweets “On-the-Go”**

Twitter is an online interactivity tool that allows you to send short messages, called “tweets,” to groups of people that subscribe to your twitter, called “followers.” Tweets must be less than 140 characters, facilitating brief communications from one to many on mobile devices or computers. In the recent presidential election, campaigns used the technology to update constituents and volunteers, heightening public awareness of the tool. Businesses, schools, social organizations, and political coalitions are using the tool to deliver timely updates to those interested. According to Nielsen, visits to Twitter have increased from 475,000 unique visitors in February 2008 to 7 million by February 2009. Adults between the ages of 35 and 49 comprise almost 42% of the site’s audience; 62% of them are accessing the site from work.

**Recommended Practices:**

The TTU IT Division recommends the following safe computing practices:

- If you are going to create a Twitter account, don’t use your primary email account; you may see an increase in SPAM if you use Twitter;
- Do not respond to any tweet from an unknown follower and delete the tweet immediately; because email accounts aren’t verified, spammers can use bogus email accounts to establish a twitter account to gather follower lists for the purposes of spamming;
- When using third party products that enhance Twitter functionality (audio, multimedia, integration with electronic mail, etc.), be mindful of what information they collect as part of the service;
- Make sure your anti-virus software on your device is current because tweets can contain abbreviated links to websites designed to install malicious code on your devices or to collect your personal data;
- Do not include any personal information in your tweets; and
- Consider setting up a protected profile where you must approve requests to follow you.

The value of Twitter is staying connected, providing timely updates, and fostering a sense of community within a group. Twitter has created a new fast-paced communication channel to distribute all kinds of information. You can view the Texas Tech Twitter at [http://twitter.com/TexasTech](http://twitter.com/TexasTech). Just remember as you use Twitter, we encourage you to practice safe computing! If you have technical questions, please contact IT Help Central at ithelpcentral@ttu.edu or (806)742-HELP (4357).

**Don’t Let Identity Theft Spoil Your Vacation**

Summer is a time for much-needed vacations and relaxation. Follow these simple tips to protect your identity while you are away to ensure your life and your identity are waiting for you when you get home:

- Ask a trusted neighbor to pick up your mail and newspaper or stop their delivery. Identity thieves are often on the lookout for signs of people on vacation in order to steal mail and, ultimately, personally identifiable information.
- Don’t travel with all your credit cards. Carrying limited credit cards, reduces the chance that they will be lost or stolen; you also minimize your loss should you fall victim.
- Be aware of leaving personal and financial information in your hotel room. Remember that many people have access to your room. Carry your wallet, your passport, and other information with you or store them in the hotel safe.
- Avoid accessing personal information from public computers. Internet cafes and hotel business centers are convenient, but you cannot assume that those servers are secure. Adept identity thieves can easily steal your information. Most public wireless connections are not generally encrypted, so avoid using them for secure transactions.

For additional safe computing information, please visit [http://safecomputing.ttu.edu](http://safecomputing.ttu.edu).

**Contributions by:** Katherine Austin, Ph.D., Darrell Bateman, Shannon Cepica, Fisayo Delano, Paco Diaz, Mark Holwerda, Alvin Mills, Yung Ng, J Stalcup, and Britta Tye.

**Safe Computing Practices Committee:** Sam Segran, Katherine Austin, Ph.D., Darrell Bateman, Pulin Bhatt, Shannon Cepica, Paco Diaz, Scott Hall, Mark Holwerda, Michael Horton, Danny Mar, Alvin Mills, Yung Ng, Mike Simmons, J Stalcup, Britta Tye, John Vandygriff, Allen Young, and assistance from IT Division leadership and staff.