NSF Office of Polar Programs, Arctic Sciences Program

Information Security 101

October 2012

Volume 1, Issue 2

Special points of interest:

- Who to contact for IT support
- Planning for IT before remote research events
- When to encrypt a file
- How to protect your PC or Mac

Inside this issue:

Arctic IT Service Providers

As connectivity to the Internet and IT services serves as a critical link to what we do; be it scientific research, educational outreach, performing our jobs, or personal communications, it's important to know:

- Who provides IT services at Arctic research facilities?
- How do I reach IT technical support when I need it?
- How do I know what IT policies apply to me while using IT resources at a research location?

CH2M Hill Polar Services

The CH2M HILL Polar Services (CPS) Team is an integrated group of organizations that provide research support for the Arctic Sciences Program. CPS is comprised of CH2M HILL, the prime contract holder, and it's team subcontractors, Polar Field Services (PFS), SRI International, and UMIAQ. Each CPS team organization has their own areas of expertise.

Barrow, Alaska

IT technical support for research in Barrow Alaska is currently provided under the CPS subcontract by University of Alaska Fairbanks (UAF) Office of Information Technology (OIT).

For IT assistance before and during your on-site research, contact Richard Machida at 907 852-0901 (Barrow), 907-474-7102 (UAF), or by email at rm@alaska.edu.

In addition to NSF requirements, UAF OIT policies apply to users and systems connecting to the network in Barrow. UAF OIT policies can be found at http://www.alaska.edu/bor/policy-regulations.

UMIAQ also provides assistance in local computer workstation and IT peripheral maintenance support to include the Barrow wireless network, video teleconferencing, handheld radio and GPS support to researchers. For more information contact Ken Robbins at 907-852-8212.

Summit Station and the Greenland Ice Sheet

IT technical support for research at Summit Station, based out of Kangerlussuaq, and throughout Greenland is provided by SRI International. For IT assistance while on-site, contact SRI IT support at cps@sri.com.

NSF requirements apply to users and systems connecting to the network at Summit Station and Kangerlussuaq.

Toolik Field Station

IT technical support for research on site at Toolik Field Station is provided through the UAF Institute of Arctic Biology (IAB), which is serviced by the UAF OIT. For IT assistance before and during your on-site research, contact UAF IT Help Desk at helpdesk@alaska.edu or 1-800-478-8226. In addition to NSF requirements, UAF OIT policies apply to users and systems connecting to the network at Toolik. UAF OIT policies can be found at http://www.alaska.edu/bor/policy-regulations.

Remote Alaska

IT support at Imnavait Creek and other remote Alaska sites is provided by SRI International (cps@sri.com).

Research Vessels

IT technical support for research performed on the US Coast Guard (USCG) Healy is provided by the Scripps Institution of Oceanography and the USCG Information Technology Division Polar IT Branch. For IT assistance when performing research on vessels, contact Scott Hiller (shiller@ucsd.edu) or Dave Forcucci (dforcucci@ucsd.edu).

Arctic IT Service Providers

ARSLS Program Applications

CH2M Hill Polar Services (CPS) subcontracts support of Arctic Research Support and Logistics Services (ARSLS) Program applications to Critigen for IT hosting, technical support, and software development services. Some of the ARSLS applications used to disseminate information to personnel supporting funded research projects, the science community, and the general public include:

Cargo Tracking System (CTS) – Tracks cargo to destinations in the Arctic, and to return equipment and samples back to institutions at the end of the research season.

Arctic Research Logistics Support Service (ARLSS) – Used to support funded research projects and to disseminate science information to the science community and the general public.

www.armap.org – A public website for access to the Arctic Research Mapping Application (ARMAP) application. ARMAP is the GIS interactive mapping application hosted by the Systems Ecology Lab at the University of Texas El Paso (UTEP).

www.polar.ch2m.com – A public website for information about services provided by operational personnel supporting the Arctic Sciences Program. For IT support please contact mike.dover@critigen.com.

Instrumentation and Field Support

UNAVCO is a non-profit national facility providing expertise and instrument support for high-accuracy earth science applications using the Global Positioning System (GPS) and complimentary equipment, including terrestrial LiDAR and related power and communications systems. Funded by the NSF, the range of services provided to the Office of Polar Programs Arctic Sciences Section (NSF-OPP/ARC) includes equipment, training, project planning, field support, proposal assistance, technical consultation, data processing, and data archiving on a year-round basis. Permanent station network support services are also provided, from the initial engineering and installations through operations, maintenance, and data archival and distribution.

For more information contact: Joe Pettit. UNAVCO Polar Project Manager, 303-381-7615, pettit@unavco.org.

Did you know?

The US based Internet Crime Complaints Centre (IC3), warns those travelling outside the US about malware which attempts to infect computers by installing itself through Wi-Fi connections in hotels. The warning states "*Recent analysis from the FBI and other government agencies demonstrates that malicious actors are targeting travelers abroad through pop-up windows while establishing an internet connection in their hotel rooms.*" The attack targets a "a widely-used software product" and the IC3 recommends that travelers update all software on their PCs before their journey and to be extra cautious before updating software from a public WiFi connection.

Information Source: http://www.theregister.co.uk/2012/05/09/hotel_wi_fi_malware_warning/ http://www.v3.co.uk/v3-uk/news/2173458/fbi-warns-business-travellers-hotel-wi-malware-scam

Researchers—Planning for IT

Often times IT needs can be an after thought in planning for projects & deployments, as we are used to having high speed wireless connections, printing, and scanning, at our fingertips. Since Arctic Science Program sites are in remote locations with limited IT services, it is important to include your projects IT needs in proposal and planning stages. This allows the program to confirm services you need will be provided where you will be working from, or work with you to find available alternatives. Some IT considerations for science planning:

⇒ IT services required for scientific research: Internet access, printing, large format plotter, kiosk computer, data storage, data/system backup, data transfer, remote connectivity, use of specific internet protocols, technical support needed, audio and video streaming, live webcast, video teleconferencing, or Podcasts.

⇒ When services will be required: temporarily while on site, year-round or seasonal data transmission, remote connection to on site systems.

Maintaining the confidentiality, integrity, and availability of the data captured by scientific research is of the utmost importance to the Arctic Sciences Program. For assistance when proposing new fieldwork and before on-site research at locations, not otherwise mentioned in this newsletter, contact your CH2M Hill Polar Services (CPS) Science Planner by email at planning@polarfield.com to identify the best set of services for protecting your science.

Protect Sensitive Data When Emailing

Protecting sensitive information is your responsibility. Emailing personal information, research data, and job sensitive documents is a standard business practice. Unfortunately it's not uncommon to email the wrong person, or send sensitive emails in clear text. Using free commercial email services (e.g. Gmail, Yahoo) and sending sensitive data without appropriate protections also poses a significant risk of unwanted access and capture of your email data. These risks can be avoided by securing (encrypting) sensitive attachments using free trial & inexpensive to purchase WinZip software., downloadable at: Mac http://www.winzip.com/mac/en/index.htm, PC http://www.winzip.com/trialpay.htm

Choosing a strong password to encrypt the file is also important. Use the following best practices when developing a password:

- Minimum of 8 characters
- Contains at least 1 number, 1 lowercase character and 1 uppercase character
- Examples include: "GreenL@nd#" "P0l@rBe@r$"

Communicate the chosen password to the recipient separate from the email with the sensitive encrypted attachment. It would defeat the purpose of encrypting the attachments if the password is provided with the file. Remember:

⇒ It is your responsibility to protect sensitive information

⇒ Encrypt attachments sent via email, especially if the attachment is sensitive information

⇒ Use WinZip to encrypt the files before attaching

⇒ Choose a strong password when encrypting

⇒ Communicate the password to the recipient separate from the email with the attachment.

By taking an extra 30 seconds to encrypt sensitive attachments, accidental disclosure of research or personal data, data breaches and embarrassing security incidents can easily be avoided.

Real World PII Incident

March 14, 2012 Humboldt State University, Arcata, California, 5,700 records affected

The personal information of students was accidentally sent in an email attachment as a response to a request for data. The mistake was noticed immediately and all copies of the file were removed from the system of the party requesting data. Student names, addresses, and Social Security numbers were exposed. Humboldt State University warned students to be vigilant about phishing, but stated that it is unlikely the data was misused.

Information Source: http://humboldt.edu/notices/

Tutorial: Encrypting Files using WinZip

To create an encrypted Zip file

WinZip Ribbon Interface

1. Check the *Encrypt* box in the Home tab.
2. Set your encryption level in the Settings tab. AES Encryption is recommended.
3. Create a new Zip file.
4. Enter a password when Encrypt dialog displays.

Legacy Menus/Toolbar

1. Open WinZip and create a new Zip file.
2. In Add dialog, check the *Encrypt added files* box.
3. When the Encrypt dialog displays specify an Encryption method: AES Encryption is recommended.
4. Enter a password and click OK.

To encrypt an existing Zip file

1. Open the Zip file.
2. In WinZip ribbon interface, click *Encrypt Zip File* on Tools tab. For legacy menus/toolbar, click *Encrypt* on the Actions menu., or right click on the Zip file in a folder window.
3. Choose WinZip.
4. Click *Encrypt.*
5. WinZip will require a password (and encryption method if you are using the Classic interface) before encrypting documents within the Zip file.

Laptop Health, Maintenance & Security: At Home & In The Field

Below are strongly recommended laptop maintenance activities to keep your PC or Mac working smooth and safe from security exploits both at work and while deployed in the field.

Weekly PC

Anti-Virus Updates: Whether using a free or paid anti-virus program, you must keep that program up-to-date with the latest virus definitions to be effective. Pick a time each week to routinely update anti-virus software, or better yet enable your software to allow for automatic updates.

Install a host based firewall: For best protection of your data, install and maintain a host-based firewall. Firewall software should be updated weekly in order to be effective.

Back Up Data and Email: Backing-up your data and email at least once a week ensures that if your laptop is lost or crashes, your hard work, research, personal data, and files are maintained.

Weekly Mac

Anti-Virus Updates: Avast is a widely accepted Anti-virus solution that is available for Macs. The A/V component is free and can be configured to auto-download vulnerability definitions and run scheduled scans. It is a common misconception that Macs are *not* susceptible to viruses. Macs used to be less susceptible to viruses because the market share was small, and malicious individuals were less interested in developing exploits. Now that Macs have taken a significant share, exploitation is becoming increasingly common. Avast Anti-virus http://www.avast.com/free-antivirus-download

Monthly PC & Mac

Software Updates: Keep software programs running on your laptop up-to-date with the latest vendor released software versions and patches, perform monthly checks or consider enabling auto update options. Maintaining software ensures that vulnerabilities in software are not exploited putting your data and system at risk.

Full Back-Up: Complete a full back-up of your system each month, and keep the back-ups in a safe location There are many commercial inexpensive back-up solutions available, so do some research on what works best for your needs.

Quarterly PC & Mac

Clean Your Hard Drive: Examine files on your hard drive and determine what can be discarded, what needs to remain local, and what can be moved to a data repository, archive, or external hard drive for future reference. Review programs and executable files on your system and be sure to properly un-install programs when no longer needed.

Defrag Your Hard Drive: Defragging your hard drive allows programs to run more quickly and make better use of the space on your hard drive. After defragging, software crashes/freeze ups decrease and programs run better.

Macs with OSX 10.2 and later automatically defrag files as the need arises; eight or more fragments for a file.

Additional Mac Security Tips

OS Updates: OS X can be configured much like MS Windows, to automatically download and install Operating System levels updates.

Defragging: Macs with OSX 10.2 and later automatically defrag files as the need arises; eight or more fragments for a file.

Hardening Mac: Apple has released *Security Configuration Guides* for **hardening Macs.** http://www.apple.com/support/security/guides/ The guides are designed to give instructions and recommendations for securing Mac OS X and for maintaining a secure computer.

"Keep all software programs up-to-date with vendor released software versions, patches, and updates."

Arctic Sciences Program Information Security Support is provided by SPAWAR Office of Polar Programs

Jack Buchanan Program Manager, SPAWAR Office of Polar Programs (SOPP)
843.218.5583
jack.buchanan@navy.mil

Sarah Wolfe OPP Program Manager
843.529.4847
wolfe_sarah@bah.com

Heather Fiebing Arctic Information Security Lead
303.221.0396
fiebing_heather@bah.com

SPAWAR
Systems Center ATLANTIC