

Information Security 101



October/November 2014

How BYOD Affects You

Inside this issue:

Bring Your Own Device (BYOD)

Protect yourself against Phishing

Heartbleed Prompts DHS Scans

ARC Awareness & Training: Contingency Planning

ARC IT Spotlight: Nagruk Harcharek

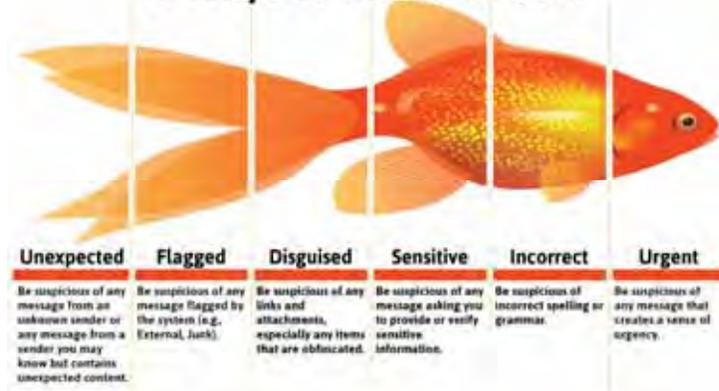
Most workers utilize a personal device (laptop, smart phone, tablet) to conduct business to some extent. This includes checking work email, sharing documents, or accessing work-related sites and information. Most workers have the option to use some government or corporate furnished equipment, yet choose to Bring Your Own Device (BYOD) because of convenience and familiarity in using one device for both personal and professional use. The problem is that mobile malware is on the rise, and users aren't necessarily looking at their devices as intelligent computers and protecting them accordingly. Researchers and staff who BYOD in the ARC Program should ensure any device utilized to access and transmit ARC information is suited for the job, and understand their responsibility in recognizing and safeguarding sensitive information that is within their control.

- Keep Device OS patches up to date: The latest OS updates often contain important security patches.
- Maintain up to date antivirus from a quality source such as [McAfee](#) or [Norton](#).
- Understand the Arctic Program Rules of Behavior, published on the NSF ARC RSL Webpage:
 - http://www.nsf.gov/geo/plr/arctic/info_security/arctic_rules_of_behavior.pdf
- To protect against the threat of malware, on mobile devices, install up-to-date anti-malware applications on the device with current definitions loaded. Android is particularly susceptible to malware, Approx. 60% of infected devices are Android Phones. Consider installing one of several available Anti-Malware Apps, available for free download directly to your device: <http://www.av-test.org/en/compare-manufacturer-results/>
- For questions or help ensuring your device is compliant, contact:
 - ARC IT Security Team—Sarah Wolfe (wolfe_sarah@bah.com) or Maria Petrie (Petrie_maria@bah.com)
 - CPS IT—Michael Lilly (Michael.lilly@ch2m.com) or Barrow IT Support Nagruk Harcharek (Nagruk.Harcharek@UmiqScience.com)
 - Your institution's IT Department

Don't Get Hooked! Phishing on the Rise

Phishing emails are targeted hacking attempts in the form of authentic looking emails that contain malware or viruses in attachments, pictures, links, or executable files. While occasionally simply opening a message can compromise your machine, viruses or malware generally require further action to execute, such as clicking a link, picture or attachment. There are many different types of malware, but the important takeaway is that these malicious files change the inherent security settings of your machine by executing code that gives the attacker control of the machine or creates a hole where data can easily be mined. There may be a delay between the execution of the malware and any negative symptoms in computer's operation, so prevention is key in protecting against malware phishing attacks. If you receive a suspicious email, do not open or click any links or attachments. Send the email as an attachment to your organization's security POC. This can include abuse@nsf.gov, ARC Security contacts Maria Petrie and Sarah Wolfe, and/or your institution's IT support team. The United States Computer Emergency Readiness Team ([US-CERT](#)) provides great information on phishing attacks and is an ideal resource for up to date, dependable information on understanding and preventing phishing attacks.

6 Ways to Catch A Phish



Security Learning Corner: Heartbleed Prompts DHS Scans

The massive reach of the Heartbleed vulnerability this summer prompted federal policy makers to take a more proactive stance with regard to cybersecurity as a national concern, particularly in light of the failure of congress to pass sweeping FISMA reform.

Building on authorities established in a 2010 memorandum, the Office of Management and Budget announced in mid-October plans to initiate proactive scanning of public facing federal networks. Compliance and participation are required on a quick turnaround, with agencies expected to provide necessary IP address infor-

mation to DHS by mid-November. The rapid response time reflects OMBs interest in providing the federal government with a more agile method for responding to cybersecurity threats, a defense capability DHS feels is lacking in current national security measures.

OMB M-15-01 also reinforces and updates the reporting requirements of agencies in the event of a breach. Again building on authorities established in older memoranda, M-15-01 requires federal agencies to report cyber or paper incidents to the US Computer Emergency Response Team

(US CERT) within one hour of breach discovery.

Learn more about new DHS Scans and OMB policies:

www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-01.pdf

www.govinfosecurity.com-dhs-to-scan-agencies-for-vulnerabilities-a-7398/p-2



in safeguarding program resources and information.

Learn more about the tactics, origin, and results of the year's most recent data breach attempts by reading the DSS report.

More Information

www.dss.mil/documents/ci/2014UnclassTrends.pdf

Helpful Tips:

If your computer's performance changes and/or you suspect you may have a virus or malware, take steps to prevent further damage:

- ⇒ Notify your security POC immediately
- ⇒ Ensure you have the latest software updates & antivirus for your machine
- ⇒ Run a scan with the updated antivirus tool
- ⇒ Quarantine or delete detected malicious files
- ⇒ Forward suspicious emails (without opening attachments) to your security POC

collection by foreign actors, methods used, and tips for prevention.

The 2014 report was recently released and provides a useful addendum to general information security training and awareness material because it records actual attempts to obtain national security data as well as the methods which were most commonly exploited to overcome network security measures or exploit user weaknesses.

According to the 2014 report, the most common attempts to obtain information were conducted by government sources in the East Asia & Pacific region and were directed against electronic devices in the US via suspicious network activity. Of note,

Data Breach in Disguise:

Every year, the Defense Security Service (DSS) publishes a classified and an unclassified report detailing attempts at data

however, is that while suspicious network activity remained the top collection method, academic solicitation increased significantly as a popular method of attack/ attempted exploitation.

Many of the ARC program human and material resources are of an academic nature, making the increase of phishing attempts disguised as academic pursuit particularly dangerous to ARC network security. While sharing information is a treasured value of the academic community, ARC program users must be vigilant in guarding the sensitive information entrusted to them as members of a government program. Add an extra layer of scrutiny to any requests for information from potential colleagues that are not personally known. Remember that no amount of network security protections can ensure the safety of program data without the vigilance of each user

ARC Awareness & Training: Contingency Planning

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

Robert Myer, Program
Manager, SPAWAR Office of
Polar Programs (SOPP)
843.345.0800
robert.l.myer.civ@mail.mil

Sarah Wolfe
Polar Program Manager
843.364.3350
wolfe_sarah@bah.com

Maria Petrie
Arctic Information Security
706.414.1412
Petrie_maria@bah.com



Did you know?

An early 2000s report by the GAO revealed that only 2% of federal agencies develop and regularly test IT Contingency Plans for all of their networks and systems. The ARC Information Security team is committed to positioning the ARC program for success in the event of an outage. Our recent activities include:

- Utilizing details from the recent Summit Station visit to prepare a detailed Contingency Plan for the Summit Station Firewall Server
- Conducting a Vulnerability Assessment and Table Top Exercise of the ARSLS Program Applications System for use in developing and testing a formal ARSLS Contingency Plan

What is Contingency Planning?

Contingency Plans provide specific instructions to restore critical systems in the event of an outage or incident. Contingency Plans identify the order in which resources should be restored, and include step by step instructions for informing the user community about resources affected by an outage. Documented Contingency Plans and regular tests of those plans are required for federal systems by the National Institute of Standards and Technology.

Contingency Planning for Your Workday

Do policies and procedures exist to restore normal operations if the systems you use on a daily basis were no longer available? Do you know the steps to take if you en-

counter an outage and how long you can expect to be without the resource? If your daily job functions rely on the use of an IT and communications resource provided by the Arctic program, you may request a copy of the IT Contingency Plan for that resource or could help develop a plan for the system if one does not already exist.

Effective Contingency Planning is a critical piece of the ARC information security program. Robust documentation and an appropriate annual test schedule not only keep the ARC program compliant with federal requirements, but ensure timely restoration of IT services critical to mission success.

ARC IT Spotlight: Nagruk Harcharek, Science Logistics Project Manager, UMIAQ Science

Each addition of the ARC IT Spotlight newsletter will introduce a member of the ARC IT team and feature the unique services they support in dedication to ARC IT. For the fall spotlight we had the privilege of interviewing Nagruk Harcharek, Science Logistics Project Manager at UMIAQ Science.

Q: Nagruk, what is your favorite part of the job?

A: The constant and sometimes last minute challenges with working in such a harsh environment. No two days are ever the same. Also, coming to work with such a great team everyday makes work enjoyable.

Q: What is your professional background?

A: When I first began my career, I pursued education in small vessel fabrication and repair and later aeronautical science. I pursued my dream of flying and worked with Ryan Air out of Kotzebue for three years, but returned to Barrow when the

long hours away began to limit the time I could spend with my family. Not long after I returned to Barrow I learned of the opportunity at UMIAQ and have been here ever since!

Q: From a personal standpoint, what are you excited about these days?

A: My family always comes first in my life. I have two daughters ages 7 and 5, and a son who is 8 months old. I have an opportunity to pass on traditional Inuit values to my children and I take full advantage of each of those opportunities. I grew up learning these values from my parents while out subsistence hunting so we try and get out as much as possible so I can pass them on to the next generation as well. It helps that the kids love being outdoors and participating. We are planning on purchasing an airplane so we can get out more during the spring, summer, and fall seasons.

Thanks, Nagruk, for your time for this interview and your dedication to the Arctic Program!



Photo: Nagruk and his family appreciating time spent outdoors on a family hunting trip