ESSENTIAL CYBERSECURITY PRACTICES FOR EVERYONE

Recently at UH, attackers have been using “spear phishing” techniques to try to convince the recipients of malware-infected emails to open the attachment or click on an included link to infect the victim’s computer. These emails can be sent from compromised UH email accounts or a trusted colleague whose account was compromised, and are well-crafted and specially designed to convince the intended victim to open the email attachment and/or click on the malicious link. If the attacker is able to compromise an email account, existing email threads can be hijacked, infected with malware, and sent out to other potential victims.

Other common tactics used by attackers to acquire your personal information and compromise your computers are:

- Brute force password cracking ( automated attempts to guess your password);
- Looking for computers with outdated operating systems (such as Windows XP and Windows Server 2003) and exploiting vulnerabilities to break into the system – then capturing any usernames/passwords found on the system or network; and
- Malicious software (including ransomware and viruses) usually acquired by visiting infected websites or via phishing emails.

The best ways to protect yourself are to:

- Update your computer’s software and applications regularly;
- Use strong passwords (and use UH’s multi-factor authentication to protect your UH credentials – see the article below about UH multi-factor authentication);
- Use anti-virus software and update it regularly; and
- Be suspicious of any unusual/suspicious communications (emails, phone calls, text messages, etc.)

For additional tips on protecting yourself and your systems, please visit: http://www.hawaii.edu/infosec or email infosec@hawaii.edu with any questions.
MULTI-FACTOR AUTHENTICATION IS HERE!

University of Hawaii faculty, staff and students can now add a second level of verification to their UH Usernames by registering for Multi-factor Authentication (MFA). This feature greatly increases the security of your UH Username by requiring that you possess not only the right password to log in, but also access to the appropriate hardware device. UH Information Technology Services strongly encourages everyone in the UH community to register for MFA.

MFA uses a registered mobile phone or landline to provide an added level of protection. When enabled, UH Login would require signing in with your UH Username and password, then authentication through a smartphone or landline to log in. Using these multiple factors provides increased security to your UH login information.

More information and FAQs on MFA may be found at: https://www.hawaii.edu/its/uhlogin/. If you have any questions, please contact the ITS Help Desk at (808) 956-8883, (800) 558-2669 from neighbor islands, or help@hawaii.edu.

2018 FEDERAL DEMONSTRATION PARTNERSHIP (FDP) FACULTY BURDEN SURVEY

The FDP will be administering its third Faculty Workload Survey in early 2018. The purpose of the survey is to estimate how much time a researcher involved in federally funded research spends on administrative tasks relative to the research and where that administrative time is spent. The last survey in 2012 received over 12,000 responses from active faculty and found that 42% of their research time was spent on administrative tasks. This correlated with the first survey in 2005, which also estimated the 42% of time spent on administrative tasks.

UH submitted a list of email addresses for all faculty with active federal awards during fiscal year 2017 (July 1, 2016 to June 30, 2017). If you receive an email request to participate in the survey, we highly encourage you to take the time to complete it.

For additional information regarding the upcoming and previous surveys, please refer to the FDP site at http://sites.nationalacademies.org/PGA/fdp/PGA_181909.
On December 31, 2017, legacy downloadable forms packages will no longer be available for proposal submissions through Grants.gov, although Grants.gov and the National Institutes of Health (NIH) systems will continue to process previously downloadable application packages through March 2018. If you plan to submit a downloaded application package after December 31, 2017, NIH recommends that you download an extra copy of the forms package for the opportunity before the end of the year in case you run into a technical difficulty with the original.

In addition, starting January 1, 2018, it is recommended that you submit NIH proposals through NIH's ASSIST, as it is optimized for NIH applications. More information about ASSIST may be found here. In the alternative, you may also submit NIH applications through the Grants.gov WORKSPACE application portal. As a note, you must register as a user at Grants.gov with an affiliation to the University of Hawaii in order to use WORKSPACE.

If you have any questions or need assistance, please contact your assigned ORS specialist, or the ORS Helpline at orshelp@hawaii.edu.

In addition, starting January 1, 2018, it is recommended that you submit NIH proposals through NIH's ASSIST, as it is optimized for NIH applications. More information about ASSIST may be found here. In the alternative, you may also submit NIH applications through the Grants.gov WORKSPACE application portal. As a note, you must register as a user at Grants.gov with an affiliation to the University of Hawaii in order to use WORKSPACE.

If you have any questions or need assistance, please contact your assigned ORS specialist, or the ORS Helpline at orshelp@hawaii.edu.