

## CYBER SECURITY AWARENESS ISSUE

Volume 2, Issue 3

October 2009

### INSIDE THIS ISSUE:

<i>Cyber Security Tips</i>	1
<i>Mobile Devices</i>	2
<i>Horror Stories</i>	3
<i>MyAACC Security Questions</i>	3
<i>System Downtime</i>	3
<i>Cyber Security at AACC</i>	4



### IS Organization

Media & Web Services

Customer Support Services

Instructional Support

Institutional Technologies

Network Services

## Cyber Security Awareness Month



Welcome to this special edition of infoTech to recognize Cyber Security Awareness Month! It's important to us that you're aware of the best cyber security practices to protect your identity and personal information. What you'll find in this edition is a list of helpful online tips, personal testimonials of security gone bad, where to find Cyber Security Awareness Month on campus, and more! We hope you enjoy this issue and learn new ways to be safe online!

*Nancy Jones*

Nancy Jones, Network Services Manager

## Cyber Security Tips

Think you're secure? Check out these cyber security tips below to see if you measure up to these best practices.

- Make backups a regular habit. Set a regular time (weekly, biweekly, monthly) to make your backups. If possible, store your computer backups in a different place than where you keep your computer.
- Use your computer's built in backup tools, as most operating systems now provide backup software designed to make the process easier. Keep your important files in one place on your computer for easier backups.
- Passwords should have at least eight characters and include upper case and lowercase letters, numerals and symbols.
- Avoid common words in your passwords as some hackers use programs that try every word in the dictionary.
- Don't use personal information that someone might already know or could easily obtain in your passwords.
- Change passwords regularly, at least every 90 days or any time you believe your system has been compromised.
- Use different passwords for each online account you access.
- If you must write down passwords, do not store them in a document on your computer. Keep them in a secure location away from your computer.
- Change your default passwords on your computer and router. Many wireless devices come pre-configured with simple administrator passwords to help in setup.
- Make sure your computer's firewall is running. Your firewall is your first line of defense against wireless and wired intrusions.
- Keep a careful eye on your laptop just as you would any valuable item. No matter where you are in public, avoid putting your laptop or any mobile device on the floor or unattended.

*(continued on back)*

## Mobile Devices

Devices such as RIM's BlackBerry, Apple's iPhone and iPod, and various Windows Mobile devices are increasingly popular - so popular that it's easy to forget these devices are actually powerful mini-computers storing large amounts of information. These devices have similar capabilities to a laptop, but fit in the palm of your hand and therefore require similar security precautions. It's important to secure your device so that you and the college are protected. Since the location and use of these devices is not confined to a specific area, the security risks are different.

**Areas where the owner of the device and the college could be at risk:**

**Loss of information** – College or personal data and files. These devices can have large amounts of memory used to store vast amounts of college or personal data in the form of e-mail, contacts, documents, and saved passwords.

**Loss of productivity** – The employee's time to recover from information and work lost on the device, which could be a few hours or days.

**Introduction of viruses and malware into the company's installed computer base, usually when synchronizing PC and hand-set in the office and on a home PC**– A few simple steps will help ensure you don't lose data, allow attackers to control your accounts, or inadvertently provide access to personal or confidential information.

**Here are 12 recommendations that can reduce the risk of using one of these very capable devices.**

**1. Set a password or PIN** Setting a password or PIN on your device is an excellent way to prevent someone else from using it or accessing the information you've stored on it. Pick a password that's hard to guess (don't use something simple such as aaa or 12345) but easy to type on your device's keyboard or screen. Consider a password with at least six characters, and use a few special characters.

**2. Enable the screen's auto-lock function** Most handhelds can be set to require a password that disables operation if they are inactive for a while. For example, once your device has been idle 10 minutes, you must enter a password before you can use it again. This prevents someone from picking it up and using it without your knowledge.

**3. Encrypt the contents** Protect your data from being stolen and viewed by attackers by encrypting the contents of your handheld. Encryption prevents someone from reading the contents of files, even if he or she finds a way to download the files without your knowledge.

**4. Don't use password remembering features** Use software with devices that remember your passwords very cautiously. If the device is lost or stolen, then an individual may have access to those accounts as they now also have the passwords.

**5. Delete unnecessary information** You can minimize your risk of losing important data by deleting information you no longer need on your handheld, which includes e-mail attachments, downloads from Web sites, and files you transported between computers via your handheld.

**6. Only download applications you trust** Be very careful downloading programs to your device. Only use applications from trusted vendors and be skeptical of free programs on the Internet. Some free programs can harm your device, steal your data, or even infect your device. Only certified applications from a trusted source should be used.

**7. Secure transfer of confidential or private information** If your device allows the ability to sync with various e-mail accounts using wireless or Bluetooth technology, then use settings that support encryption such as SSL. This will ensure the communication between your device and the application servers or your workstation is kept private.

**8. Keep your software up to date** You should check for updates for your device regularly. Your device may have a software updater application, or you may need to download the software to your computer and install it via USB to your handheld. By doing this, you not only get the newest applications for your device, you also get the latest security updates to better protect your information. Consult your manufacturer or provider's Web site for update instructions and downloads.

**9. Be careful where you connect** If your device can be used on wireless networks, be careful of unsecured wireless access points. Treat your handheld just as you would a laptop. If you are using an unsecured wireless network, your wireless signals can be intercepted and inspected. This includes any unencrypted passwords sent through the air. If you use Bluetooth for any reason, then remember to disable it when it is not needed. This is a communications protocol that can be used to gain unauthorized access to your device.

**10. Report stolen or lost devices to AACC.** If you have lost or someone has stolen your device with stored AACC information, please notify [Information Services](#). There are many compliance regulations we must follow if certain data is lost.

**11. Wipe contents before disposal, donation, or transferring the device to another** If you are donating or transferring your device to another, then carefully wipe the contents of the device and any memory cards in the device. Most devices today have the ability to use removable memory cards that are stored within the device.

If your device has stopped functioning and you are going to dispose of it you should remove all memory cards and physically destroy the device and additional memory cards. If your new device can use the old memory card, you may be able to transfer it to your new device.

**12. Restrict the users of the device** These devices should not be loaned or shared with others as this would potentially give others access to any information stored on the device.

*NOTE: These recommendations may not be applicable to all devices. For assistance please contact the device manufacturer.*

# Horror Stories

## Phishing Hell

I began receiving e-mails asking for my password from the college's IS department for an account upgrade. Unbeknownst to me, these were phishing e-mails that appeared legit because of the AACC return address and language of the e-mail. Unfortunately, after I replied with my password, the phishing scammers used my e-mail to send out thousands of inappropriate e-mails over the next two weeks. I started receiving hundreds of angry and humiliating responses to e-mails I never sent. I had to immediately change my password and spent the next two weeks deleting these e-mails. Moral of the story? Don't provide your password or user ID to anyone! The college will never ask for your user ID or password through an e-mail. *Arvid Amos*



## A Horror Poem

It was a dark and stormy semester day at AACC;  
And Sherri just broke up with her beloved,  
Johnny Lee.  
He was mad, mad, mad, you see;  
Sherri, he cried, "come back to me!"  
But his cries fell on deaf ears  
(yes, we know; that's from Shakespeare, my dear)  
And Johnny Lee did what any broken-hearted soul  
would do through his tears;  
(First, he went to Starbucks in the rain...)  
Then sipping his Caramel Mach  
and enjoying The Fray,  
He logged into her account and plotted his way,  
Hissing and growling with anger and glee  
(it was the sugar he had ingested, you see)  
With the press of a button; he deleted her work;  
Her essay on Whitman; her photos of Turkey;  
Even her presentation on the history of beef jerky!  
And, finally, one last sip and a sinister grin;  
That'll teach you, my Sherri, he whispered within,  
To never, never share your password again.

*Anonymous*



## The Dark Side of Downloading

Don't download any software unless you are 100% sure of the package you are getting. I downloaded a free worm remover program which infected my machine until it eventually died. When I tried to remove the program from my machine, the infections became worse and wreaked havoc on my machine.

*Ghoulish Gary*

## MyAACC Security Questions

Last spring, we enabled users to reset their own password on MyAACC after first answering a set of seven security questions compiled by members of our Information Services team. The user, upon the next password reset, is required to answer three out of the seven questions correctly in order to successfully reset their password.

To protect your information, you can change these security answers anytime by logging into MyAACC and selecting the "My Account" link which is located to the left of the welcome message in the upper left-hand corner. Then select "Change Security Questions and Answers" under Configure Secrets.

You can also change your MyAACC password anytime by selecting the same "My Account" link and filling out the appropriate information.

[Login to MyAACC](#)

## System Downtime

AACC is committed to providing current and progressive technology to enhance and support the college mission. AACC provides students with access to proven state-of-the-art hardware and software, current classroom technology, Web applications, and efficient management systems to support the student experience while attending the institution. For a complete list of available technologies and services, visit the [Technology Web site](#).

In order to provide superior service to the college community, regular maintenance is required.

Scheduled maintenance occurs on Friday evenings from 9:30 p.m. (EST) to 1:30 a.m. (EST). All college systems will be unavailable to students, faculty and staff during this timeframe. This includes access to e-mail, ANGEL (online, hybrid and Web-based courses), MyAACC, STARS and [www.aacc.edu](http://www.aacc.edu).

On the second Friday of every month the Self Services tab in MyAACC and STARS will be unavailable from 6:30 p.m. (EST) to 1:30 a.m. (EST).

## Cyber Security Tips (continued)

(continued from front)

- Use startup passwords on your laptop to prevent thieves from easily accessing your data.
- Back up important data before traveling. A few minutes spent backing up your files will protect you later.
- Every computer should have at least these three forms of protection installed: an anti-virus program, firewall, and anti-spyware program. Make sure they're up to date and running on a schedule.
- Visit [www.staysafeonline.org](http://www.staysafeonline.org) for more helpful suggestions and tips for increasing your Cybersecurity knowledge.
- Be careful what you post on social networking sites like Facebook or MySpace. Criminals use these sites to build information about their victims.
- Be careful about meeting social networking 'friends' in person. Do so in a public place and have a friend go with you.
- Be careful about what files you download. Any software can contain malicious code. Most browsers will alert you that a file is being downloaded. If you did not ask to download something, refuse to download it.
- No e-mail filter is perfect, so treat every message you get with caution, even if it appears to be from friends, coworkers, or relatives.
- Phishing scams are e-mail attacks that attempt to get personal or financial information from you. Avoid phishing attacks by never responding to e-mails when you do not recognize the source, or feel that the information they are requesting is sensitive. Remember that no organization will request your credit card information, bank account information, social security number, or passwords via e-mail.
- Be cautious when making online purchases. You should never assume everything on the Internet is safe.
- Avoid online credit card purchases using wireless networks in public places.
- Before providing personal information to an online retailer, make sure the site is secure such as an https address or a padlock in the browser.

Source: [www.staysafeonline.org](http://www.staysafeonline.org)

### Cyber Security at AACC

#### How is AACC participating in cyber security awareness?

- Visit <http://my.aacc.edu>'s Cyber Security tab for daily tips and resources for making a difference in your workplace.
- Check out our Cyber Security posters in labs across campus.
- View our window display in the Careers Center Building on the second floor in front of room 215.
- Visit [www.staysafe.org](http://www.staysafe.org) for more tips and information!

Thanks to our Cyber Security team:

Jamie Carter  
Stacey Gustavson  
Nancy Jones  
Scott Kramer  
Kathy Long

Special thanks to Editor Kimi Raspa.

Please direct any questions or comments to Shirin Goodarzi,  
Chief Technology Officer  
[smgoodarzi@aacc.edu](mailto:smgoodarzi@aacc.edu)

#### Notice of Nondiscrimination

AACC is an equal opportunity, affirmative action, Title IX, ADA Title 504 compliant institution. Call Disability Support Services, 410-777-2306 or Maryland Relay 711, 72 hours in advance to request most accommodations. Requests for sign language interpreters, alternative format books or assistive technology require 30-day notice. For information on AACC's compliance and complaints concerning discrimination or harassment, contact Karen L. Cook, Esq., federal compliance manager, at 410-777-7370 or Maryland Relay 711.