

BE EXTRA CAUTIOUS WITH SENSITIVE INFO

Passwords...Be Creative

These days it is hard to find someone who does not have a plethora of online accounts. It is common for members of the Kingsborough community to manage multiple personal and work related accounts. CUNY Portal, CUNYfirst, e-mail, banking, social networking, shopping, travel and credit card web services are all accessed daily by many of us – with a user name and a password. While these online services do make life easier, if their passwords are not managed properly it can lead to an unauthorized access and in extreme cases the theft of your personal identity. Imagine the nightmare this may cause.

Passwords are important because they help protect your personal information and identity. Remember that online activity conducted under your user name and password is attributable to you. It is therefore important to use only well thought out password to mitigate these risks. To avoid the pain associated with the password management please follow some simple tips for creating and managing your password in this brochure.



PROTECT YOUR DATA ON THE GO

INSTALL ANTIVIRUS SOFTWARE

Cyber Security Starts with YOU!

Do Your Part...Educate Yourself, Educate Others

Be Safe Than Sorry!

Kingsborough Community College

Office of Information Technology Services
2001 Orient Boulevard
Brooklyn, New York 11235

Phone: 718-368-6679
Fax: 212-237-8015
E-mail: helpdesk@kbcc.cuny.edu

KINGSBOROUGH



COMMUNITY COLLEGE

PROTECT YOURSELF FROM EMAIL SCAMS

THINK BEFORE YOU CLICK

Common Sense Guide for Creating Passwords

Kingsborough Community College

Office of Information Technology Services

Tel: 718-368-6679

USE STRONG PASSWORDS



Think Password As Your House Key...Password Locks Data

1. Choose a **Complicated** Password.

Don't use most common words in the English language and basic character arrangements, such as "87654321" and "123abc". Aim for at least eight characters or more with combination of letters (lower and upper case) and numbers. However, don't make your passwords so complicated or impersonal that you may have to write it down.

2. Try to be **Creative** with Spellings.

Use punctuation marks and other symbols in place of letters. Try substituting a "@" for an "a" or a "\$" for a "S." Take a normal word or name and then alter it by putting symbols, numbers and punctuation marks into it somewhere. For example, if you want to use the word "moonlight" as your password, use a "0" (zero) instead of an "o," and a "!" instead of an "i."

Think Password As Your Tooth Brush...Should You Share Either?

3. Make your Passwords **Personal**.

To remember easily create your passwords with personal information. You can arrange a combination of some of your personal information backwards. Assuming you remember your mom's birthday, you can reverse it in the password. Similarly you can use a personal name as the basis for a number of online passwords. For example, if your father's name is William, you could use "MAILLIW1" for CUNY Portal account and "MAILLIW2" for Kingsborough email account.

4. Use an **Acronym** of Favorite Quotes, Personal Names, etc.

If you remember a favorite phrase or words, you can use them to create a password. Take a phrase and turn it into an acronym and add extra numbers or characters to the beginning or end to change it for different accounts. For example, say you remember "To be or not to be" then "TBONTB11" could be your Facebook® password, "TBONTB12" could be your shopping site password and so on.

5. **Keep all your Passwords to Yourself**.

Don't leave your password on a post-it note next to your computer or lying around anywhere or give it to anybody over the phone or through e-mail. Many hackers are able to get into your account not through technological means but through getting on the phone and impersonating as an official. Be suspicious if someone calls you and asks for your password or your personal information over the phone or if your bank asks you to send it over an e-mail. Most reputable institutions don't ask people for passwords or personal information by e-mail anymore.

Be Suspicious...Be Vigilant

6. **Change your Passwords Regularly**.

Don't use the same username and password for all your online accounts. Be sure to change your passwords when prompted by the application or proactively every 3 months.

7. **Set up Passwords for All the Devices You Own**.

Remember to password-protect your cell phone, smart phone, iPod, e-Reader, etc. Also, make sure to change the factory default administrative password on your home wireless router and other devices to something more "complicated". Disable "guest access" from your home wireless router as well.



Use the Right Tools...Follow the Right Behavior