Cyber Security Starts with

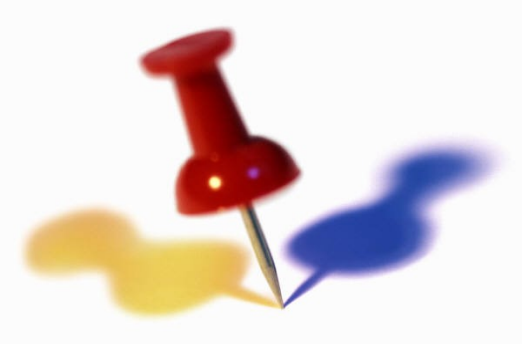
YOU!

- Is your computer up-to-date…Patch it to protect it!
- Did you lock your computer…Lock it when you leave it!
- Are you cyber secure…Be more secure!
- Is your password "strong"…Create strong passwords and don't share it!

Use the Right Tools…
…Follow the Right Behavior

Be Safe than Sorry!

Defend Your Computer



Do Your Part…
…Educate Yourself, Educate Others

Kingsborough Community College
Office of Information Technology Services
2001 Oriental Boulevard
Brooklyn, New York 11235

Phone: 718-368-6679
Fax: 718-368-6601
E-mail: helpdesk@kbcc.cuny.edu

KINGSBOROUGH COMMUNITY COLLEGE

Use Strong Passwords

Tips for Protecting Personal Information. Yours and Other's

KINGSBOROUGH COMMUNITY COLLEGE

Office of Information Technology Services
Tel: 718-368-6679

Protect Your Data On The Go

What to Do if Security Problems Occur?

1. When using e-mail or other web services, you may encounter spam, phishing scams, obscene material, aggressive behavior or theft of your account or identity. When this occurs:
   - Report immediately to the service (e.g. look for *Report Abuse* link or email *abuse@domain.edu*, etc.)
   - Report immediately to the Office of Information Technology Services
2. If any sensitive non-public data has been compromised because of theft or loss of a computer or a laptop, portable device, breach of network security or through any other means try your best to minimize the damage and:
   - Report it immediately to the Office of Information Technology Services
   - Change all passwords immediately for network accesses and devices after they have been found
   - For smartphones and PDAs, contact the service provider for help in wiping the data from the device. For college owned devices contact Office of Information Technology Services

More Resources...

CUNY's Office of Information Security
http://security.cuny.edu
Office of Inspector General
www.ed.gov/about/offices/list/oig/misused/idtheft.html
Federal Trade Commission – Identity Theft
www.consumer.gov/idtheft/
US Department of Justice – Identity Theft & Fraud
www.usdoj.gov/criminal/fraud/websites/idtheft.html
Identity Theft Prevention and Survival
www.identitytheft.org/
Privacy Rights Clearinghouse - Identity Theft Resources
www.privacyrights.org/identity.htm
FTC -When Bad Things Happen to Your Good Name
http://www.ftc.gov/bcp/menus/consumers/data/idt.shtm
CERT Coordination Center – Home Computer Security
www.cert.org/homeusers/HomeComputerSecurity/
National Cyber Security Alliance Guide
www.staysafeonline.org/for-higher-education
Security Tools & Resources and Free Security Check Ups
www.staysafeonline.org/toold-resources
Microsoft – Maintain Your Privacy
www.microsoft.com/athome/security/privacy/
EFF's - Top 12 Ways to Protect Your Online Privacy
www.eff.org/Privacy/eff_privacy_top_12.html
CDT's – Top 10 Ways to Protect Privacy Online
www.cdt.org/privacy/guide/
BBB Online (Better Business Bureau) - Privacy Tips
www.bbbonline.org/UnderstandingPrivacy/toolbox/tips.asp
Microsoft – Chat and Messaging Safety
www.microsoft.com/athome/security/chat/

Protect Yourself From E-Mail Scams

Basic Security Tips

1. Choose a strong password and protect it. Use a different password for each online account.
2. Backup your computer files regularly.
3. Be careful which sites or services you access when using a public wireless network.
4. Change default password on your home wireless router to a long complex password.
5. Be sure your computer or laptop has security software tools (e.g. Symantec Antivirus, etc.) and is updated with security patches.
6. Do not leave laptop unattended in public areas.
7. Use caution when using public computers.
8. Turn your computer off when not in use.

Online Shopping and Banking

1. Limit online shopping to merchants you know and trust.
2. Pay your online purchases with a credit card or an online payment service.
3. Keep a paper trail of purchases and check your bank and credit card statements regularly.
4. Look for "https" or "shttp" at the beginning of a web address (URL) and a closed padlock beside it.
5. Don't provide financial information or social security numbers through email.
6. Before you share personal information, ask
   - Who's going to see it?
   - What is the value of it?
   - Why do they need to see it?

Downloads & File Sharing

1. Be wary of installing free downloadable software.
2. Practice caution when using free file-sharing programs.
3. Be alert to phishing scams in email, Web or social networking sites.
4. Don't follow email links or pop-up ads that claim your computer is infected and offer anti-virus software ("scareware") with fake security warnings.
5. Don't download pirated software, music and movies.

Data Security at Kingsborough

1. Encrypt all sensitive data on your computer using encryption software such as PGP.
2. Lock your computer every time you leave your desk. Set up a screen saver with preset time out and password protection.
3. Allow access to systems and sensitive non-public data to only those who need it.
4. Backup your data regularly.
5. Be cautious when you print or copy sensitive non-public information — do not leave it in an open area and shred it when not in use.
6. Strictly follow CUNY security policies, procedures and advisories (http://security.cuny.edu), and report violations and issues when they occur to the IT department.
7. Don't give out your social security number to any college department unless it is absolutely necessary.

Social Networking

1. Be cautious how much personal information you provide.
2. Learn and use privacy settings on social networks.
3. Protect your reputation on social networks.
4. Limit your social network to "real" friends.

Protect Data on Portable Devices

(Smartphones, e-Readers, PDAs, Flash Drives, Memory Sticks, etc.)

1. If it is not necessary, don't copy the information on the portable device.
2. Encrypt files or the entire disk on the device.
3. Use a strong password on all the devices and lock the keypad when not in use.
4. Turn off Bluetooth and Wi-Fi when not using it.
5. Be sure to backup all the critical information.
6. Avoid unsecured Wi-Fi networks.
7. Before discarding wipe the device clean.
8. Store your devices securely when not in use.

FOR ALL KINGSBORUGH RELATED SECURITY PROBLEMS AND ISSUES CONTACT THE OFFICE OF INFORMATION TECHNOLOGY SERVICES IMMEDIATELY AT 718-368-6679 OR E-MAIL HELPDESK@KBCC.CUNY.EDU

Think Before You Click...Think Before You Share Personal Information