What is High Risk Confidential Information (HRCI)?

A person's name in conjunction with that person's:

- Social Security Number
- Credit or debit card account number
- Individual financial account number
- Driver's license number
- State ID number
- Passport number
- Biometric information
- Personally identifiable human subject and medical information

Steps to take now

- Choose strong passwords
- Use a unique password for each account
- Password protect all mobile devices
- Use strong account security questions
- Password protect your screensaver
- Check your credit report
- Be aware

Safe Handling of HRCI

- Store hard copy high risk or confidential information in a locked area.
- Only use a Harvard computer to work with HRCI - at work and at home (adhere to your remote access policy when working remotely).
- Never store HRCI on your computer, an external device, or portable media.
- When transferring confidential information, use Secure File Transfer (contact service desk for further information)
- Obtain approval from the School and/or University CIO prior to collecting or working with HRCI or contracting with a vendor to process HRCI,

Disposing of HRCI

- Dispose of hard copy HRCI in an approved, locked shred-bin.
- Contact the service desk for the appropriate disposal of CDs/DVDs/Blu-Ray discs, hard drives and all other media containing HRCI.
- When a computer or a mobile device is repurposed, its hard/flash drive must be completely "sanitized," not just reformatted. Contact the service desk for this service.
Passwords
- Passwords must be strong and never be shared with anyone or written down.
- IT support will never ask for your password.
- If you think your password has been compromised, change it immediately and contact your IT support department.

Strong passwords should:
- Be a minimum length of 8 characters.
- Be changed at least once annually.
- Be a combination of upper and lower case letters, including at least one numeric and/or special character.
- Contain at least 5 different characters
- NOT contain a string of characters that match previous passwords.
- NOT be names, words, or anything else easily guessed by those who know you.
- NOT contain more than two consecutive characters that are the same.
- NOT be based on a single word, or consist of two words separated by a space, hyphen, or underscore character.

HUIT IT Security
ithelp@harvard.edu

Top Ten Desktop Security Tips
1. Set automatic updates for your computer.
2. Regularly update and run your anti-virus software.
3. Set strong and regularly change your passwords.
4. Do not store any personally identifiable information on your computer.
5. Secure your workstation with a password protected screensaver.
6. Transfer sensitive files in a secure manner.
7. Delete unsolicited e-mails.
8. Limit Web browsing to reputable sites.
10. Backup your data to the encrypted media.

Top Ten Security Tips for Mobile Devices
1. Set a strong passcode and wipe data option after 10 failed passcode attempts.
2. Download and apply software updates for your mobile device.
3. Avoid keeping sensitive data on mobile devices.
4. Use discretion when downloading apps.
5. On public Wi-Fi, limit email, social networking and online shopping/banking. Use VPN where possible.
6. Use Bluetooth safely - Disable or use hidden mode.
7. Download mobile malware protection software for your mobile device.
8. Do not jailbreak or root your mobile device.
9. Ensure remote wipe capabilities are enabled.
10. Regularly back up your device

Public Places
- Do not leave your computer unattended.
- Turn on the screensaver feature and require a password to resume.
- Do not disable security features on your computer.
- Beware of your surroundings and people looking over your shoulder.

Social Networking:
- Consider what you place online.
- Information posted remains the property of the social network site.
- Posted information/messages may never be deleted.
- Check with public affairs or student affairs dean prior to posting on behalf of Harvard.
- Use two factor authentication where possible.
- Limit access to your profile (do not grant access to acquaintances).

You should contact the service desk or Information Security Office in the event:
- You need to immediately report any loss or breach of high risk or confidential data.
- You are working on a project that needs a security input or assessment.
- You believe you encounter a phishing attempt or your computer has been infected with malware.
- Your computer or mobile device is lost or stolen.
- You have any security questions or concerns.