definitions

Social Engineering–the practice of obtaining confidential information by manipulation of legitimate users. A social engineer will commonly use the phone or internet to trick people into revealing sensitive information or getting them to do something that is again typical policies or actions. By this method, social engineers exploit the natural tendency of a person to trust his or her word, rather than exploiting computer security "holes". It is generally agreed upon that "users are the weak link" in security and this principle is what makes social engineering possible.

Phishing–Mail or electronic messages (text/im) that pretend to be financial institutions or companies that attempt to get you to reveal your personal information or that of others.

Dumpster Diving–rummaging through trash looking for paper with personal information on it.

Old fashioned stealing–taking of information from wallets/purses, rummaging through office files, unattended computing devices, or asking employees who have access to private information to disclose it.

Executive Office of
Housing & Economic
Development

1 Ashburton Place
21st floor
Boston, MA 02108

www.mass.gov/hed

Executive Office of
Housing & Economic Development

Privacy & Information Security

Pri—va—cy n.
the right to be free of unnecessary public scrutiny or to be left alone.
the quality or state of being apart from observation

Se—cu—ri—ty n.
the state or feeling of being safe or protected.
precautions taken to keep somebody or something safe from crime, attack or danger.

EOHED–Privacy and Information Security Brochure

Confidential Information is:

Social Security numbers

User ID's and Passwords

Bank Account numbers

Credit Card numbers

Birth information

Medical data

EOHED is legally required to keep our business information secure. This brochure is a reminder to you of your responsibilities as an employee of the Secretariat. Breaches of confidential information can put you and the agency at risk.

Ask yourself this - would you want your privacy compromised due to someone else's carelessness? Do you want to be liable for a breach of private information?

It is easy to become complacent in your day to day work. You think you are helping others by just "sending something along" to them in an email....or just forwarding on some information...or you are in a hurry so you leave that spreadsheet on your desk in full view....or you make too many copies and drop the extras into the trash.....

Actions such as those above may very well have serious consequences. If you are in possession of sensitive data then you must take measures to protect that data.
YOU ARE RESPONSIBLE!

Questions to ask yourself

- What information do I really need?
- What data should I be collecting?
- Is SSN required? Are you sure?
- What data is critical to this task?
- Who do I need to share this with?
- Why am I sharing this?
- How should I get this data to someone?
- Will anyone else see this information?
- How safe is this information in someone else's hands?

- Is computing equipment where anyone can get to it?
- Is the main office locked? When? Who has keys?
- Are locked cabinets in use? Shredders? Desks clean?

- Is there a startup password on computing devices?
- Are screensavers activated and password protected?
- Do PC hard drives prevent file storage on them?
- Are USB's allowed to be shared/taken off site?
- Are passwords strong and changed frequently?
- Is network equipment in a secure area?
- Can users log in remotely? Is agreement signed?
- Are computing resources protected with anti-virus and firewall programs that are up to date?
- Do you password protect or encrypt confidential files?
- Do you know how to send/receive secure emails?
- Are files containing confidential data secured in a restricted directory/file share on network?
- If you use portable media, is it stored securely
  Are the business web based applications secured ? through software controls and id/s and passwords?
- Are the vendors you work with clear on their role and responsibilities when it comes to data security?

Business & organizational improvements

- Do you understand what data is "private", needs to be "secured" and where it lives in your business environment?
- Are information technology policies and procedures in place?
- Are you aware of the current policies and procedures?
- Have you signed off on receiving, reviewing and acknowledging those policies?
- Are you trained on how to put those policies and procedures into practice?
- Do you know the steps to take if there is a breach of data considered to be confidential/ private?
- Do you understand social engineering practices?
- Are there plans to review and revise business security practices and make improvements?

All levels of the organization need to take responsibility.

Remember to manage the exposure risk.

awareness, training and professionalism on all levels is necessary for success.