Do's and don'ts

Awareness

Do

1. Create and follow a security policy.
2. When in doubt, check it out! Check the leading anti-virus Web sites for security alerts and as a general reference source.

Don't

1. Assume security is someone else's job.
2. Think that you know everything there is to know about security. Technology changes quickly and new threats surface almost every day.

Telephone

Do

1. Make sure that you know who you are speaking with and suggest legitimate ways outside callers can obtain the information they seek.
2. Offer to return calls from unknown or suspicious callers after first checking to ensure the caller is legitimate. By offering to return the call, you can buy yourself time to check out the caller's authenticity.

Don't

1. Give unknown or unauthorized callers any information.
2. Be intimidated by a caller who is a "name dropper" or claims to be a VIP.

Printed material

Do

1. Pick up printouts and faxes promptly.
2. Use a cover page when sending faxes.
3. Label confidential information and handle it in a manner appropriate to its sensitivity.
4. Lock up confidential information when you leave your work area.
5. Dispose of confidential information in secure trash bins or by shredding.

Don't

1. Leave confidential information on the printer or fax machine.
2. Fax confidential information without speaking with the intended recipient first.

3. Disclose secret or sensitive Information to anyone not authorized to see it.
4. Leave confidential information out on your desk when you're gone, or in public areas at any time.
5. Throw confidential information into open trash bins, at work or at home.

Computer use

Do

1. Be aware of your surroundings and take precautions to protect confidential information.
2. Use secure e-mail for confidential information.
3. Ensure that all computers you use to access the Internet or your company's network have anti-virus software running.
4. Install security-related software patches as soon as they are available.
5. Whenever possible, encrypt sensitive or secret information that is stored on your hard drive.
6. Use cable locks to secure portable devices.
7. Keep your portable computer and PDA with you at all times.
8. Use a password-protected screen saver and logout of your company's network at the end of the day.

Don't

1. Display confidential information on your computer screen in public areas.
2. Send confidential information in ordinary e-mail.
3. Open e-mail attachments you weren't expecting, even if they're from someone you know.
4. Set up your own wireless LAN or have a modem that can accept an incoming call while your computer is connected to the Internet or your company's network.
5. Put sensitive or secret information on a portable computer or PDA in plain text.
6. Leave portable devices unsecured when you're not there.
7. Leave a computer or PDA unattended in a public place.
8. Leave your computer logged into your company's network and the display on when you're gone.

Passwords

Do

1. Use strong passwords on your computer accounts.
2. Change your password regularly.
3. Memorize your password.

4. Keep your password secret.

Don’t

1. Use your name, your family’s names, your pet’s name, or a word in a dictionary as your password.
2. Change your password in predictable ways.
3. Write it down.
4. Tell anyone your password, for any reason.