
# WELCOME

www.cybercellmumbai.com

# Cyber Crime
# Do's & Don't

Presented by-

CYBER CRIME INVESTIGATION CELL, CRIME BRANCH, CID, MUMBAI.

# Do's

- Install and use a firewall, pop-up blocker and spyware detector.
- Ensure that your virus definitions are up to date and run anti-virus and spyware detectors/cleaners regularly.
- Make Backups of Important Files and Folders to protect important files and records on your computer if your computer malfunctions or is destroyed by a successful attacker?
- Use strong passwords - Easy to remember and difficult to guess type password. Use alphanumeric and special characters in your password. The length of password should be as long as possible (More than 8 characters).

# Do's continued.....

- Assignment of computer to a particular person with password protection in offices.
- Install the firewall and maintain the logs of firewall.
- Preservation of evidence (logs/received emails in question etc).
- Disconnect from internet when not in use.

# Do's continued.....

- Habitually download security protection update patches & Keep your browser and operating system up to date.
- Never share photographs in compromise positions.
- Make the wireless network invisible by disabling identifier broadcasting .
- Encrypt the network traffic.

# Do's continued……

- Change administrator's password from the default password. If the wireless network does not have a default password, create one and use it to protect the network.
- disable file sharing on computers .
- Turn off the network during extended periods of non-use, etc.

# Do's continued.....

- Avoid online banking, shopping, entering credit card details, etc if the network is not properly secured.
- Check your online account frequently and make sure all listed transactions are valid.

# Do's continued……

- Use a variety of passwords, not same for all of your account.
- Be extremely wary of spam legitimate looking  email asking for confidential information. Never ever click on the link given in the spam email.
- Always delete spam emails immediately and empty the trash box to prevent accidental clicking on the same link.

# Do's continued.....

- Be wary of websites that require your card details up front before you actually place an order .
- Not to believe everything you read online.
- Take your time - do not rush into things.

# Do’s continued……

- Avoid posting your cell phone number online.
- Never respond to text messages from someone you don't know.
- Never let someone you don't know use your cell phone.

# Do's continued……

- Open email attachment carefully
- Be careful while downloading any free software or screensaver etc.
- Not delete email in question, save the email and take out the full header of the such email and report the crime.
- Be cautious when dealing with individuals outside of your own country.
- Be cautious of unsolicited offers . Never purchase anything advertised through an unsolicited email.

# Do's continued……

- Beware of promises to make fast profits. Be cautious of exaggerated claims of possible earnings or profits.
- Beware of lotteries that charge a fee prior to delivery of your prize .
- Contact the actual business that supposedly sent the email to verify if the email is genuine
- Beware of references given by the promoter.

# Do's continued……

- Ensure you understand all terms and conditions of any agreement.
- Be leery when the job posting claims "no experience necessary".
- Always type in the website address yourself rather than clicking on a link provided.

# Don’t tell any anonymous chat friend

- Your real name, home address
- your phone number
- your friends' or family members' private information .
- your passwords

# Don’t

- Expose yourself that you are not available in town or give your details about location and itinerary when email auto responder enabled.
- Hand over your credit card to any person.

# Don’t continued…….

- Auto-connect to open Wi-Fi (wireless fidelity) networks .
- Get confused, frightened or pressured into divulging information if you receive an e-mail purporting to be from your bank or credit card provider as criminal use scare tactics .
- keep passwords stored on your computer .

# Don’t continued……

- To go online without virus protection and a firewall in place.

- Open email attachment if you are not sure about it.
- Assume a company is legitimate based on "appearance" of the website.
- Be wary of investments that offer high returns at little or no risk.
- Accept packages that you didn't order.

# Questions?