Preventing credit/debit card fraud

By taking certain precautions, a user can prevent their credit or debit card from being misused both online and offline.

1. Do not provide photocopies of both the sides of the credit card to anyone. The card verification value (CVV) which is required for online transactions is printed on the reverse of the card. Anyone can use the card for online purchases if the information is available with them.

2. Do not click on links in email seeking details of your account, they could be phishing emails from fraudsters. Most reputed companies will ask you to visit their website directly.

3. While using a credit card for making payments online, check if the website is secure The CVV will also be required.

4. Do not give any information to persons seeking credit card information over phone

5. Notify your bank / credit card issuer if you do not receive the monthly credit card statement on time. If a credit card is misplaced or lost, get it cancelled immediately.

Online Safety Tips

We all know that the Internet is a cool place to hang with friends and check out new things. But don’t forget about the Internet’s risks and dangers. If you’re going to use the Web, do it safely! Here are some suggestions on what you should and shouldn’t be doing online to help protect you against the bad stuff.
Be careful online.
Never reveal personally – identifiable information online. A lot of creeps use the Internet to take advantage of other people, especially kids and teens. Never reveal any personally-identifiable information online, whether it’s on your profile page or in a blog, chatroom, instant messenger chat or email.

- Always use a screen name instead of your real name.
- Never give out your address, telephone number, hangout spots or links to other websites or pages where this information is available.
- Be careful about sending pictures to people you do not know very well.
- Never tell people personal or private information about your friends or family.
- Never assume you’re completely anonymous online. Even if you don’t put personal information online, there are different ways that people can still figure out who you are and where you live.

Never share your password with other people (except for your parents).

Your passwords to websites, email accounts and instant messenger services should not be shared with friends or strangers. Your friends may not be as safe as you are and may unknowingly subject you to danger. You should, however, share your passwords with your parents if they ask so they can make sure you're using the Internet safely.

Never arrange meetings with strangers.

Just because you've seen a person's picture and read his or her profile, does not mean you know them. Many people online lie about who they are and what their intentions are. Just because someone seems nice online, does not mean they really are. They could be trying to hurt you. Never arrange a meeting with a stranger you've met online. Even meeting a stranger in a crowded place could be dangerous as he could follow you home. If you wish to meet an online friend in person, talk to your parents and arrange a time and place where your friend can meet your parents first, just in case. If you are worried about your parents meeting one of your online friends, you probably shouldn't be friends with them in the first place.

Don't believe everything you read or see online.

Be wary of everything you see online unless it is from a trusted source. People lie about their age, who they are, what they look like, where they live, how they know you and what their interests are. Also, a lot of websites and emails contain information that is misleading or just plain untrue. If a person or deal sounds too good to be true, it probably is. Ask your parents to help you figure out what information is really true.

Don't download files or software without your parents' permission.

There are a lot of files on the Internet that are unsafe to download to a computer. Some files will bombard you with pop-up ads all day long. Some files will actually track everything you and your family does on your computer, including your logins, passwords and credit card information, which criminals then use to steal money from you and do other harm. There is no easy way to tell which files are bad and which are ok to download. That free desktop wallpaper you want to download might also steal your parents' credit card information. Ask your parents before you download any files or software from the Internet.

Don't respond to inappropriate messages or emails.

Some people send inappropriate messages just to see if you will respond. If you do, you are simply encouraging them to send more inappropriate material to you. Don't respond to inappropriate messages. Instead, talk to your parents about how to report them to the right place.

Don't post inappropriate content.

. If you post information about tennis, you will attract people who are interested in tennis. If you post inappropriate content or pictures, you will attract people who have inappropriate interests. If you post jokes, photos or other content that contain sexual references you will probably attract people who are only interested in talking about sex. Be mindful of what you are communicating to the rest of the online world through the content you put onto the Internet.

Be leery of personal questions from strangers.

People you don't know who ask personal questions are often up to no good. Don't continue communicating with strangers who ask you personal questions. Talk to your parents about how to block them from communicating with you and report them to the right place.

Don't be bullied into fights.

People tend to say things online that they would never say in person. Some people even say rude and malicious things, sometimes just to see if you will respond. Don't respond to these people. Instead, talk to your parents about how to block them from communicating with you and report them to the right place.

Don't use adult sites.

There are some websites that kids just should not use. Don't use websites that contain adult content or that facilitate communication with older adults. No matter how much you think you know about the Internet, there are some people and places you just aren't ready to deal with. Enjoy websites that are designed for people your own age.

Understand what you put online will be there forever.

Assume that everything you put online— every email you write, every picture you post, every blog or journal entry you post— will be accessible on the Internet forever. Many search engines copy Internet pages and save them for viewing even after the pages are no longer online. Think about that before you post anything online. Do you really want pictures or blog entries to be seen 10 years from now?

Are You A Safe Cyber Surfer?

Fortunately, there are steps you can take to protect your computer, your information and your peace of mind from computer creeps who try to slow down a network operation, or worse yet, steal personal information to commit a crime. Here are some tips to help you, from the Thane Police

Make sure your passwords have both letters and numbers, and are at least eight characters long. Avoid common words: some hackers use programs that can try every word in the dictionary. Don't use your personal information, your login name or adjacent keys on the key board as passwords and don't share your passwords online or over the phone.

Protect yourself from viruses by installing anti-virus software and updating it regularly. You can download anti-virus software from the Web sites of software companies, or buy it in retail stores; the best recognize old and new viruses and update automatically.

Prevent unauthorized access to your computer through firewall software or hardware, especially if you are a high-speed user. A properly configured firewall makes it tougher for hackers to locate your computer. Firewalls are also designed to prevent hackers from getting into your programs and files. Some recently released operating system software and some hardware devices come with a built-in firewall. Some firewalls block outgoing information as well as incoming files. That stops hackers from planting programs called spyware-that cause your computer to send out your personal information without your approval.

Don’t open a file attached to an e-mail unless you are expecting it or know what it contains. If you send an attachment, type a message explaining what it is. Never forward any e-mail warning about a new virus. It may be a hoax and could be used to spread a virus.

When something bad happens-you think you’ve been hacked or infected by a virus-e-mail a report of the incident to your Internet provider and the hacker’s Internet provider, if you can tell what it is, as well as your software vendor.

Take a test before opening e-mail attachment

- Is the email from someone that you know?
- Have you received email from this sender before?
- Were you expecting email with an attachment from this sender?
- Does email from the sender with the contents as described in the Subject line and the name of the attachment(s) make sense?
- Does this email contain a virus? To determine this, you need to install and use an anti-virus program.

What is computer security and why should I care about computer security?

1. **What is computer security?**

   Computer security is the process of preventing and detecting unauthorized use of your computer. Prevention measures help you to stop unauthorized users (also known as "intruders") from accessing any part of your computer system. Detection helps you to determine whether or not someone attempted to break into your system, if they were successful, and what they may have done.

2. **Why should I care about computer security?**

   We use computers for everything from banking and investing to shopping and communicating with others through email or chat programs. Although you may not consider your communications "top secret," you probably do not want strangers reading your email, using your computer to attack other systems, sending forged email from your computer, or examining personal information stored on your computer (such as financial statements).

3. **Who would want to break into my computer at home?**

   Intruders (also referred to as hackers, attackers, or crackers) may not care about your identity. Often they want to gain control of your computer so they can use it to launch attacks on other computer systems.

   Having control of your computer gives them the ability to hide their true location as they launch attacks, often against high-profile computer systems such as government or financial systems. Even if you have a computer connected to the Internet only to play the latest games or to send email to friends and family, your computer may be a target.

   Intruders may be able to watch all your actions on the computer, or cause damage to your computer by reformatting your hard drive or changing your data.

4. **How easy is it to break into my computer?**

   Unfortunately, intruders are always discovering new vulnerabilities (informally called "holes") to exploit in computer software. The complexity of software makes it increasingly difficult to thoroughly test the security of computer systems.

   When holes are discovered, computer vendors will usually develop patches to address the problem(s). However, it is up to you, the user, to obtain and install the patches, or correctly configure the software to operate more securely.

   Also, some software applications have default settings that allow other users to access your computer unless you change the settings to be more secure. Examples include chat programs that let outsiders execute commands on your computer or web browsers that could allow someone to place harmful programs on your computer that run when you click on them.

Use Strong Password

- For each computer and service you use (e-mail, chatting, online purchasing, for example), you should have a password.
- You shouldn’t write them down nor should you share them with anyone, even your best friends.
- Computer intruders use trial-and-error, or brute-force techniques, to discover passwords.
- Use alphanumeric characters and special characters in your password.
- The length of password should be as long as possible (More than 8 characters).
- Do not write it to some place where it is visible to someone else.

Protect Your Website

1. Stay informed and be in touch with security related news.
2. Watch traffic to your site. Put host-based intrusion detection devices on your web servers and monitor activity looking for any irregularities.
3. Put in firewall.
4. Configure your firewall correctly.
5. Develop your web content off line.
6. Make sure that the web servers running your public web site are physically separate and individually protected from your internal corporate network.
7. Protect your databases. If your web site serves up dynamic content from database, consider putting that database behind a second interface on your firewall, with tighter access rules than the interface to your web server.
8. Back up your web site after every update.

Protect Your Personal Computer

1. Use the latest version of a good anti-virus software package which allows updation from the Internet.
2. Use the latest version of the operating system, web browsers and e-mail programs.
3. Don’t open e-mail attachments unless you know the source. Attachments, especially executables (those having .exe extension) can be dangerous.
4. Confirm the site you are doing business with. Secure yourself against "Web-Spoofing". Do not go to websites from email links.
5. Create passwords containing atleast 8 digits. They should not be dictionary words. They should combine upper and lower case characters.
6. Use different passwords for different websites.
7. Send credit card information only to secure sites.
8. Use a security program that gives you control over "Cookies" that send information back to websites. Letting all cookies in without monitoring them could be risky.

Tips For Children

1. Do not give out identifying information such as name, home address, school name or telephone number in a chat room.
2. Do not send your photograph to any one on the Net without initially checking with the parent or guardian.
3. Do not respond to messages or bulletin board items that are obscene, belligerent or threatening.
4. Never arrange a face to face meeting without informing your parent or guardian.
5. Remember that people online may not be who they seem to be