SECURITY TIPS TO CUSTOMERS

Online Fraud

Online frauds happen when someone poses as a legitimate entity and illegally conducts transactions on your existing accounts. This is commonly known as 'phishing' or 'spoofing'. Most contemporary modes of online frauds are generally through fake emails, Websites, pop-up windows or any combination of such methods.

Whatever may be the mode, the main objective of both offline as well as online frauds is to steal your 'identity' and the whole process is commonly termed as "identity theft". Identity theft happens when someone illegally obtains your personal information like credit card number, bank account number, internet banking user id and passwords or other sensitive identification information etc. and uses it to initiate transactions in your name.

It is to be remembered that Identity theft can happen even to those who do not shop, communicate or transact online as a majority of identity thefts occur offline. Stealing wallets and purses, intercepting or rerouting your mail and rummaging through your trash / waste are some of the common tactics that fraudsters generally resort to obtain personal information. The more you are aware about identity theft, the better you would be prepared.

Phishing Emails

All Internet users should be aware about one of the most common attempts of fraud through means like 'phishing' or 'spoofing'. 'Phishing' is an attempt by fraudsters to 'fish' for your banking details. 'Phishing' attempts usually emanate in the form of an email appearing to be from your bank or an authority like a regulator etc. Within the email you are then usually prompted to click on a hyperlink to a fraudulent website designed to capture your details. Email addresses are obtained from publicly available sources or through randomly generated lists. Therefore, if you receive a fake email that appears to be from your bank,, this does not mean that your email address, name, or any other information has been taken from the banks systems.

Although they can be slightly difficult to spot for a unsuspecting customer, 'phishing' emails generally ask you to click on a link which takes you back to a spoofed website which would look similar to your Bank's website, wherein you are asked to provide, update or confirm sensitive personal information. To prompt you into action, such emails may signify a sense of urgency or emergency condition concerning your account such as 'there has been a problem in your account', 'in order to enable you to access your account smoothly and faster' or something like that.

The most commonly sought after information through such means would be:

- Your PIN numbers
- Your Internet Banking Passwords
- Your Bank Account/ Credit Card/ Debit Card number
- Card expiry date
- Other verification parameters, like; your date of birth, mother's maiden name etc.

Some fake emails could also contain a malware known as a 'Trojan horse' capable of carrying out many malicious activities such as recording your keystrokes, triggering background installations of key logging software or installing viruses onto your computer. The virus could be present in an attachment or be accessed via a link in the email. In computer parlance, a **Trojan horse** is a

program that contains or installs a malicious program usually called the 'payload' or 'Trojan' meaning under the guise of being something else.

The need of the hours is, therefore, to not to respond to such emails, open attachments, or click on links from suspicious or unknown senders.

If you receive an email from Dhanlaxmi bank and you're not sure if an email sent by us is legitimate, please contact customercare@dhanbank.co.in , without replying to the email.

Please remember Dhanlaxmi bank will never ask any of your personal sensitive information over email

Counterfeit web sites

It is probable that, often, online fraudsters would direct you to fraudulent websites via email or pop-up windows etc. and try to collect your personal information. The best possible way to detect a rogue website is to consider how you arrived there. Generally, you may have been directed by clicking a link in a fake email requesting your account information. However, when you type or cut and paste, the URL into a new web browser window and it does not take you to a legitimate Web site, or you get an error message, it was probably just a fake website.

For your security you should always type www.dhanbank.com in your browser instead of trying to visit it from any link in emails.

Identify & protect yourself from fraud

How to identify a fake email/website?

Fake emails/ websites are not always easy to identify, however the following indicators could enable you to safeguard against such emails or websites, should you ever come across one of these:

Ask you for sensitive information: Fake emails claim that your information has been compromised due to which your account has been de-activated/suspended, and hence ask you to confirm the authenticity of your information/ transactions.

Appear to be from a legitimate source: While some emails are easy to identify as fraudulent, others may appear to be from a legitimate source. However, you should not rely on the name or address in the 'From' field alone, as this can be easily duplicated.

Contain spelling mistakes: Very often, such 'phishing' mails could contain several spelling mistakes and even the links to the counterfeit websites may contain a url with spelling mistakes in order to take you to a website which looks like that of your Bank but actually is not. Whenever you use a link to access a website, be sure to check for the url of the website and compare it with the original. It is recommended that you type the url yourself whenever you access the Bank's website or you may bookmark/store the same in your 'List of Favorites' so that it can be invoked whenever you want to log-in.

Contain prizes or other offers: Some fake emails promise a prize or gift certificate in exchange for completing a survey or answering a few questions. In order to collect the alleged prize, you may be asked to provide your personal information.

Advertise fraudulent job offers: Some fake emails appear to be sent by companies to offer you a job. These are often work-at-home positions which are actually schemes that victimize both the

job applicant and other customers. Be sure to confirm that the job offer is from a genuine and reputed company.

Link to counterfeit Web sites: Fake emails may direct you to counterfeit websites carefully designed to look real. Hence such websites may look very similar and familiar to you, but are actually used to collect personal information for illegal use.

Look like a genuine Web site: Spoof websites can be more difficult to detect, because even the address bar and padlock symbol that appear in your browser window can be faked. To make sure you are really on the Bank's site, type in Bank's website name and find out if you get to the same place.

Below are some tips for recognizing whether you have possibly been a victim of fraud:

- If you do not receive an expected bill or statement by mail
- If unexpected charges occur on your account
- If there are charges on your account from unrecognized vendors
- If the cheque leaves in your cheque book appear out of sequence
- If you get collection calls regarding merchandise or services that you did not buy

Use Internet Banking to minimize the risk of Fraud

- Monitor your account activity regularly by checking your balances and statements online through the Bank's website. This helps you to promptly detect any fraudulent transactions. The earlier a fraud is detected, the smaller will be its financial impact.
- Also, limit the use of cheques, transfer funds online between your Dhanlaxmi Bank accounts, or send money to other Dhanlaxmi Bank and Non-Dhanlaxmi Bank customers through the Bank's website.
- Make it a practice to receive SMS alerts upon transactions in your account.

Protect yourself against Offline fraud

- Make photocopies of all the information you carry daily like credit cards, debit cards etc. and store them in a secure location like a safe deposit locker.
- Shred financial or personal documents before discarding. Most fraud and identity theft incidences happen as a result of mail thefts.
- Whenever you or your family are away from home, get the incoming post collected by a trusted acquaintance and if you are going to be away for a longer period, arrange to get your mails diverted to an alternate address. Do not leave your incoming post lying around in your absence.

Protect yourself against online fraud

With a few simple steps, you can help protect your account and personal information from fake emails and websites:

- Please delete suspicious emails without opening them. If you happened to open a suspicious email, do not respond to online solicitations for personal information. Also do not open any attachments or click on any links it may contain.
- Never provide any sensitive account or personal information in response to an email. If you have entered / parted personal information, report it to the Bank immediately by calling our Call Centre or sending a mail to customercare@dhanbank.co.in.

Cyber Cafe Security

If you are accessing any website including the Bank's website from a cyber cafe, or from any shared computer or from a computer other than that of your own, you are requested to change your passwords after any such use immediately thereafter, from your own PC at your workplace or at home. It is very important to do so especially when you have entered your transaction password from such shared computer or cyber cafe computer, as the sensitive details including user-ids and passwords could have been tracked by key loggers both hardware or software based meant for the purpose in such systems. Please note to change these passwords from your own PC at your workplace or at the house.

Password Related Tips

Always choose unique passwords that include a mix of letters, numbers and characters wherever permitted. Make it a point to use longer passwords as allowed by your application using a mix of letters, numbers and special characters as they are much more difficult to figure out than shorter, more straightforward passwords. Please avoid choosing passwords that are obvious, easily guessable, such as names of family members or pets, nicknames, birthdays and telephone numbers that might be easy for others to figure out.

Please remember that Dhanlaxmi Bank is NOT liable for any loss arising from your sharing / compromise of your sensitive account related information such as User Ids, passwords, cards, card numbers or PINs with anyone, NOR from their consequent unauthorized use. You are required to understand the importance of keeping such details confidential as well be aware of the consequences of their misuse.

Please destroy the PIN mailer after memorizing the PIN / Password and/or change the PIN after the first usage.

Change your Internet Banking Password (both meant for Login and Transaction authorisation) after your first login and thereafter regularly (at least once in a month).

Create and maintain different passwords for Login and for Transaction authorisation. This provides additional security for financial transactions through Internet Banking.

Avoid using the same password for multiple applications or Internet services. Make it a practice to use a unique password for each website and purpose. In case you have more than one Internet Banking User-ID, use a different password for each of your Internet Banking User-IDs.

Your password should be complex and difficult for others to guess. Use letters, numbers and special characters [such as !, @, #, $, %, ^, &,* (,)] in your passwords. These increase the security of the passwords.

Avoid using passwords that are obvious, like your name/ nickname, names of family members, your address, phone number or any other information that a fraudster might find in your purse or wallet.

Do not use a password that contains part of your User ID or account number.

Try to avoid passwords that are real [as in dictionary] words and always use cryptic words as passwords.

Avoid using the same password as the one which you use to login to your PC or access your email account to the online transaction accounts.

If your login IDs or passwords automatically appear in the sign-in page of a secure Web site, the auto complete function should be disabled to increase the security of your information.

If you are accessing any website including the Bank's website from cyber cafe, any shared computer or from a computer other than that of your own, change your passwords after such use from your own PC at workplace or at house. It is very important to do so especially when you have entered your transaction password from such shared computer or cyber cafe computer. Change these Passwords from your own PC at your workplace or residence.

Never share your passwords with others, including family members. Do not disclose your Internet Banking password to anybody, not even to a Dhanlaxmi Bank employee.

Using Internet Banking

Always type the address of the website in the address bar of your browser or access it from your stored list of favorites.

Do not share your Passwords with anyone - Dhanlaxmi Bank officials will never ask you for your Internet Banking Passwords.

Change your Passwords frequently - Use the best practices for creating passwords based tips on creating passwords in the respective sections.

Use Virtual Keyboard - Using the virtual keyboard wherever available would help prevent key logger compromises as in such cases the keyboard is not being used for the input.

Check for your Last Login Time - Login to the Bank's internet banking website to view the date and time of your last login.

Limit the use of physical statements - Online statements easier to manage than paper statements and instantly retrievable. The fewer personal documents are sent through the post, the less the chance for a possible fraud.

Review your account statements carefully - Make a habit of reviewing your account statements regularly. The Mini Statement and Detailed Statement options available on the internet banking site shall help you to review your bank account statements thoroughly.

Sign Up for SMS Alerts - Register for Mobile Banking and receive alerts upon all transactions in your account.

Be Vigilant - Never fill in any form that you have accessed via a link with sensitive data such as User-ID, Password, PINs, and other account related information.

Login Frequently - Logging into the internet banking website not only helps you keep track of your accounts online but also enables you to notice and stop any fraudulent activity quickly.

Be Cautious - Do not leave your internet banking session unattended. Always ensure sign off after use from your online banking session.

Shopping Online

Be very sure of the website address:

The website address is reflected on the address bar of your Internet Browser. This check is recommended every time you access any website from a link given elsewhere. Always type the website address yourself or bookmark the websites that you use frequently.

Never enter, confirm or update your account-related details on a pop-up window.

Enjoy added security when using your Credit card online:

If you tend to use your Credit Cards frequently for online shopping, make sure that you sign up for the websites displaying **Verified by Visa** and/or **Master Card Secure Code** program(s).

Confirm that website is a secure one:

Make sure any Internet purchase activity you engage in is secured with encryption to protect your account information. Look for "secure transaction" symbols.

Shop Online only from reputed websites

Beware of online offers that require you to provide your account details for ' verification'

Privacy Commitment

In the course of using this website or availing the products and services vide the online application forms and questionnaires, Dhanlaxmi Bank and its Affiliates may become privy to the personal information of its customers, including information that is of a confidential nature.

Dhanlaxmi Bank is strongly committed to protecting the privacy of its customers and has taken all necessary and reasonable measures to protect the confidentiality of the customer information and its transmission through the world wide web and it shall not be held liable for disclosure of the confidential information when in accordance with this Privacy Commitment or in terms of the agreements, if any, with the Customers.

Dhanlaxmi Bank Endeavour's to safeguard and ensure the security of the information provided by the Customer and uses 128-bit encryption, for the transmission of the information, which is currently the permitted level of encryption in India. When the information provided by the Customers is not transmitted through this encryption, the Customers' system (if configured accordingly) will display an appropriate message ensuring the best level of secrecy for the Customers' information.

The Customer would be required to cooperate with Dhanlaxmi Bank in order to ensure the security of the information, and it is recommended that the Customers necessarily choose their passwords carefully such that no unauthorised access is made by a third party. To make the password complex and difficult for others to guess, the Customers should use combination of alphabets, numbers and special characters (like !, @, #, $ etc.). The Customers shall undertake not to disclose their password to anyone or keep any written or other record of the password such that a third party could access it.

Dhanlaxmi Bank undertakes not to disclose the information provided by the Customers to any person, unless such action is necessary to:

- Conform to legal requirements or comply with legal process;
- Protect and defend the Bank's or its Affiliates' rights, interests or property;
- Enforce the terms and conditions of the products or services; or
- Act to protect the interests of the Bank, its Affiliates, or its members, constituents or of other persons.

The Customers shall not disclose to any other person, in any manner whatsoever, any information relating to Dhanlaxmi Bank or its Affiliates of a confidential nature obtained in the course of availing the services through the website. Failure to comply with this obligation shall be deemed a serious breach of the terms herein and shall entitle Dhanlaxmi Bank or its Affiliates to terminate the services, without prejudice to any damages, to which the customer may be entitled otherwise.

Dhanlaxmi Bank will limit the collection and use of customer information only on a need-to-know basis and would deliver better service to the customers. Dhanlaxmi Bank may use and share the information provided by the Customers with its Affiliates and third parties for providing services and any service-related activities such as collecting subscription fees for such services, and notifying or contacting the Customers regarding any problem with, or the expiration of, such services. In this regard, it may be necessary to disclose the customer information to one or more agents and contractors of Dhanlaxmi Bank and their sub-contractors, but such agents, contractors, and sub-contractors will be required to agree to use the information obtained from Dhanlaxmi Bank only for these purposes.

The Customer authorises Dhanlaxmi Bank to exchange, share, part with all information related to the details and transaction history of the Customers to its Affiliates / banks / financial institutions / credit bureaus / agencies/participation in any telecommunication or electronic clearing network as may be required by law, customary practice, credit reporting, statistical analysis and credit scoring, verification or risk management and shall not hold Dhanlaxmi Bank liable for use or disclosure of this information.

IMPORTANT SECURITY CONCERNS IN ONLINE BANKING

Viruses

Virus (***acronym for Vital Information Resources Under Siege***) in computer parlance, is applied to a variety of malicious computer programs that send out requests to the operating system of the host computer system to append such programs to other host programs. The computer viruses, therefore, are self propagating to other programs. Viruses are one of the several types of ***malicious software*** or ***malware*** developed for the purpose of harming computer systems. In common parlance, the term ***virus*** is often extended to refer to worms, trojan horses and other sorts of malware.

Many variants of computer viruses are generally categorized based on the way they affect the computer system. Some viruses are relatively benign or merely annoying while others are intentionally destructive and malicious, capable of deleting files, corrupting programs or causing denial of service etc. Some viruses have a delayed payload or course of action which is sometimes called a ***bomb***. For example, a virus might display a message on a specific day or wait until it has infected a certain number of hosts. The ***time bomb*** category triggers on a particular date or time and a ***logic bomb*** wrecks havoc when the user of a computer initiates an action that triggers the bomb.

A category of viruses frequently encountered is the ***'Worm'.*** Unlike a virus, worm does not physically attach itself to another program but to get propagated to the host systems, characteristically exploits the security weakness in the configuration of the operating system of the host computer. Consequently, the worms strike especially in client–server environments and have assumed critical importance with the widespread usage of the Internet.

Trojan horses are destructive programs that masquerade as benign applications. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horses is a program that claims to get rid of computer viruses but instead introduces viruses to the computer. Spyware which gather sensitive and critical user / system related information and pass them on to the sponsored sites have gained in popularity with the increasing acceptance of the Internet as a popular media for information transfer and sharing.

Viruses generally target four components of a computer system viz. data files, boot and system areas that are required to start a computer, executable program files and file directory system that tracks location of all computer files. It is to be remembered that the visible effect of virus on a computer system is only consequential in nature and is directly attributable to the way the virus is programmed to affect the computer system. Some of the apparent symptoms of virus attacks are as under:

a. Unusual error messages getting displayed
b. The file size is seen reduced
c. Missing files or even increase in file size
d. Sudden lack of disk space
e. Access to hard disk files being denied/delayed
f. Reduction in memory size
g. Display of communication between two user IDs/systems in the network on the computer screen
h. Change in the file date or time stamp
i. Longer time to load a program
j. Unusual screen activities
k. Data file getting corrupted
l. Antivirus Software itself getting corrupted

Notwithstanding the fact that the latest version of virus scan software and updates thereof are being run, the users shall exercise sufficient caution when any of the above symptoms are observed.

Trojans

In computer parlance, a **Trojan horse** is a program that contains or installs a malicious program usually called the 'payload' or 'trojan' meaning under the guise of being something else.

Trojan horses could appear to be useful, interesting or harmless programs to an unsuspecting user but they tend to be extremely harmful when executed. Often the term 'Trojan Horse' is abridged in usage as **Trojan**.

There are two common types of Trojan horses. One category is that of any useful software which has been subsequently corrupted by a hacker by inserting some malicious code which executes when the said software program is used. The other category is that of standalone programs which will masquerade as something else viz. like a game or image file, in order to force the user into

doing something which is needed to trigger / carry out the program's objectives. It is to be remembered that Trojan horse programs cannot operate autonomously in contrast to some other types of malware. Needless to iterate, if Trojans are to replicate and even distribute themselves, each new victim must run the program that will trigger the Trojan.

Trojan horse payloads are generally designed to do various harmful things but some Trojans could be relatively harmless. Their classification is based on how they breach the victim's systems and the damage they cause. A simple example of a trojan horse would be a program named "waterfalls.scr" claiming to be a free waterfall screensaver which when run would allow remote access to the user's computer.

The nine main types of Trojan horse payloads are those that facilitate:

1. Remote Access
2. Sending of Email
3. Destruction of data
4. Download of data
5. Disguising others as the infected computer - Proxy Trojan
6. Adding or copying data from the infected computer - FTP Trojan
7. Disabling of security software
8. Denial-of-service attack (DoS)
9. Directing the infected computer to only connect to the internet via an expensive dial-up connection - URL trojan

The common manifestations of Trojan Horse attacks are erasing or overwriting data on a computer, encrypting files, corrupting files, uploading and downloading files, allowing remote access to the victim's computer, setting up networks of zombie computers in order to launch Denial of Service attacks or send spam, spying / covert reporting of data, making screenshots, logging keystrokes to steal information, phishing for bank or other account details, installing a backdoor on a computer system, opening and closing CD-ROM tray, harvesting e-mail addresses and using them for spam, restarting the computer whenever the infected program is started, deactivating / interfering with anti-virus / firewall programs, deactivating / interfering with other competing forms of malware etc. The list is endless.

Time bombs and **logic bombs** which activate on particular dates and/or times and on activation of certain conditions being met by the computer respectively are treated under the Trojan Horses category. Then there are the **Droppers** performing a legitimate task as well as an illegitimate task at a time.

Spyware / Malware / Adware

Spyware is a comprehensive term for computer software that is designed to collect personal information about users without their tacit consent. The term Spyware is often used interchangeably with two other terms, adware and malware. In all these cases, the spyware

consumes the computer resources under siege to a certain extent without permission. In the present day computerised environment, personal information is secretly captured / recorded using a variety of techniques including logging the keystrokes, recording the Internet web browsing history etc. The purpose ranges from overtly criminal like theft of passwords and financial details to the merely annoying categories like those recording Internet search history for targeted advertising.

Spyware may collect different types of information. Some variants called **Adware** attempt to track the websites a user visits and then send this information to an advertising agency. Adware also frequently refers to any software which displays advertisements whether or not a user has given his consent. There are much more malicious variants of software designed for infiltrating and damaging / harming a computer system called **Malware** which include computer viruses, worms, trojans etc. Some of these variants attempt to intercept passwords, PINs, credit card numbers as a user enters them into a web based form or in other applications.

Spyware does not directly spread in the manner of a computer virus or worm. Instead, spyware gets on to a system through deception of the user or through exploitation of software vulnerabilities. Most spyware is installed without the users being aware of the fact. Since they tend not to install the software if they know that it will disrupt their working environment and compromise their privacy, spyware deceives users, either by piggybacking on any desirable software downloaded or tricking the users into installing it. In some cases even some deceitful anti-spyware program itself will even masquerade as security software.

The distributor of spyware usually presents the program as a useful utility. In some cases they are pushed in as a "Web accelerator" or as a helpful software agent. Users download and install the software without ever suspecting that it could cause harm. Spyware also come bundled with shareware or other `downloadable software as well as music CDs. When the user downloads a program and installs it, the installer additionally installs the spyware in the computer. Although the desirable software itself may do no harm, the bundled spyware is bound to carry out the specific purpose it was indented for. A third way of distributing spyware involves tricking users by manipulating the security features designed to prevent unwanted installations. Some spyware authors infect a system through security holes in the Web browser or in other software wherein when the user navigates to a Web page controlled by the spyware author, the page containing the code will attack the browser and force the download / installation of the spyware. In some cases computer worms or viruses are observed to deliver spyware payloads.

Spyware programs are rarely alone on a computer as the affected machine can rapidly be infected by many other components. One of the most conspicuous symptoms of spyware infection is performance degradation and abnormal system behavior. A spyware infestation can create significant unwanted CPU activity, disk usage and network traffic all of which are bound to slow the computer. System crashes are also common. Spyware which interferes with networking software commonly causes hitches in getting connected to the Internet.

Phishing

Phishing is a form of cyber attack in which the fraudsters induce Internet users to divulge sensitive, confidential information relating to bank accounts. The technique uses email to 'fish' the Internet hoping to 'hook' users into supplying with the login-IDs, passwords, PINs, credit card information etc.

In a typical phishing attack, a user receives an e-mail purported to be sent by a financial institution. The e-mail will carry the spoofed [Spoofing : creating a look alike/shadow/mirror copy] image or logo of the financial institution and will attempt to convince the user to provide / part with personal, account details by directing him to visit a web link (hyperlink) given in the e-mail

message. When the user clicks the hyperlink, he will be led to a fictitious web page, which will be a look alike/ exact replica of the website of the financial institution but hosted by the fraudsters. An unsuspecting user, unaware of such a malicious activity will be requested to provide his personal / account details in the fraudulent website in the pretext of some exigencies like updating Bank's database, for cross-verification etc. The fraudsters then use the information for fraudulent transactions causing huge financial losses to the individuals and financial institutions.

Phishing attacks involve thousands of users. In a single phishing attack, a fraudulent e-mail message is sent to thousands of users with the hope that at least a small percentage of users will respond. The trends show that on an average, 5 -10 % users respond to such e-Mails.

Successful phishing countermeasures involve educating the users to be careful while handling emails even though they appear to be emanating from legitimate sources. What needs to be remembered is that Banks will not request customers for such sensitive information in the first instance; leave alone through relatively unreliable modes like Internet / email etc... This necessitates an user to pay close attention to the contents of any email that seek any personal information.

Key Loggers

The expectations from computerized processes, applications and delivery channels are constantly on the rise these days. This necessitates a situation where in the computerised environments need to be totally secure, always available and be reliable to the core so that the growing expectations are fully met. However, many new technologies do surface which constantly pose a threat of one sort or the other. One such emerging technology which has great ramifications on the information security front is the usage of 'Key Stroke Loggers'.

Keystroke logging (often called **keylogging**) is a diagnostic tool / device to capture the user's keystrokes. On the positive side, it can be beneficial to determine the causes of errors in computer systems, measure employee productivity, support law enforcement and espionage [for instance to obtain passwords or encryption keys for law enforcement and other purposes]. However, the flip side is that the keyloggers widely available on the Internet can be used to spy on the computer usage of others.

Keylogging can be achieved by both hardware and software means. **Hardware key loggers** could be devices attached to keyboard cable or devices installed inside the keyboards. The former has the advantage of easy installion and they may go undetected for quite some time. The keylogger inside the keyboard (the keyboard of the target system) is the toughest to install and also is virtually undetectable unless specifically looked for.

Software key loggers are software applications specifically designed for the purpose and like any other computer program are distributed as a trojan horse or as part of a virus. An attacker connecting to a host machine to download logged keystrokes risks being traced. The most difficult task, therefore, for a keystroke logger is to escape being traced while downloading data that has been logged. A trojan that sends keylogged data to a fixed e-mail address or IP address also risks exposing the attacker.

Currently there is no easy way to prevent keylogging. However, users should constantly observe the programs which are installed on their systems. Anti-spyware applications are able to detect many keyloggers and cleanse them. Enabling a firewall does not stop keyloggers per se, but can possibly prevent transmission of the logged material over the net. Network monitors (also known as reverse-firewalls) are useful to alert users whenever an application attempts to make a network connection.

Keylogger detection software is also available. Some of this type of software use "signatures" from a list of all known keyloggers. One drawback of this approach is that it only protects from keyloggers on the signature-based list, while the system remains vulnerable to other keyloggers. Other type of detection software analyzes the working methods of many modules in the computer system blocking many different types of keyloggers. One drawback of this approach is that even legitimate, non-keylogging software is also blocked in this respect.

Using the virtual keyboard wherever available would help prevent key logger compromises as in such cases the keyboard is not being used for the input.