Glossary

1.1 Antivirus program

Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. You can help protect your computer against viruses by using antivirus software. There is a variety of software available in the markets for free or at a cost.
Computer viruses are software programs that are deliberately designed to interfere with computer operation; record, corrupt or delete data; or spread themselves to other computers and throughout the Internet.
To help prevent the most current viruses, you must update your antivirus software regularly. You can set up most types of antivirus software to update automatically.

1.2 Cash trap

The ATM has been manipulated by criminals who have inserted a device that traps the money so that it does not come out of the ATM. When you leave, thinking that the ATM is out of order, the criminals return with a special tool and release the money from the trap. If you suspect this, you should check your account to see if the withdrawal has been registered. It is important that you call your bank if you do not get your money from the ATM.

1.3 Clickjacking

Is a vulnerability used by online criminals to collect an infected user's click. In this way the user can be forced to do all sort of things from adjusting the user's computer settings to unwittingly sending the user to websites with malicious codes.

1.4 Cookies

A cookie is a small piece of code which is stored in the browser on your pc, mobile phone or tablet when you surf on the internet. The cookie stores information about your behaviour or ensures that a web page works technically. Cookies are not harmful and when you exit Netbank by clicking on the Log out button, the cookies are deleted.

1.5 Cybercrime

Cybercrime is a term used for criminal acts involving computers, smart phones and networks. Examples of cybercrime are Internet fraud, identity theft and credit card account thefts. The illegal activities are carried out through the use of a computer and the Internet.

1.6 Encryption

Is a technical way to convert data into cipher text. Encryption is used to prevent confidential data from being accessed or used by unauthorised persons.

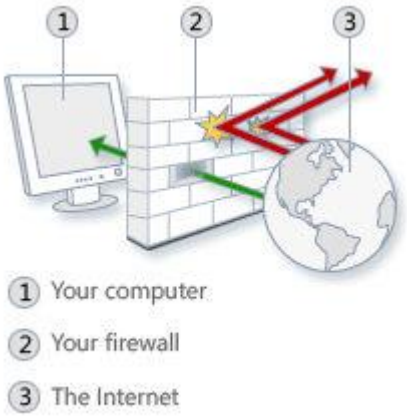
1.7 Family fraud

Someone close to you misuses your bank identity, for example account, card and/or personal information.

1.8 Firewall

A firewall is software or hardware that checks information coming from the Internet or a network and then either blocks it or allows it to pass through to your computer, depending on your firewall settings.

A firewall can help prevent hackers or malicious software (such as worms) from gaining access to your computer through a network or the Internet. A firewall can also help stop your computer from sending malicious software to other computers.
The following illustration shows how a firewall works.



A firewall isn't the same thing as an antivirus program. To help protect your computer, you need both a firewall and an antivirus and anti-malware program.

1.9 Identity theft

Identity theft (or ID jacking) is where your personal information is misused to get a bank or credit card or a loans or for gambling site accounts or purchasing goods on credit in shops.

1.10 Jailbreak

Slang term used to describe the action of gaining access to a smartphone's private file system to override some of the device's restrictions. Jailbreaking also enables a smartphone user to install third-party applications.

1.11 Keylogging

Also known as keystrokelogging. This is the practice of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that persons using their keyboards are unaware that their actions are being monitored.

1.12 Malware

Malware is short for malicious software. It is any kind of unwanted software that is installed on your devices (pc, mobile phone) without your permission or without you even knowing it. Malware is designed to damage or disrupt a system. It can also be used to give online criminals control over the device or to steal personal information.

Examples of malware: virus, worms, Trojan horses.

1.13 Money mules

A person who transfers illegally acquired money on behalf of other criminals is called a money mule.

Criminals use various ways of attracting or luring others to act as a money mule. You may be offered "a job" which involves asking you to receive money into your bank account and transfer it to another account, letting you keep some for yourself. Criminals might also ask you to open a new account for this purpose only.

The money that is transferred is stolen and the transfer is called money laundering. Anyone acting as a money mule may be liable for criminal offences whether or not there was a monetary benefit.

1.14 Pharming

The criminals trick you to go to a fake website. This method can be quite confusing and difficult to detect as the website looks very similar to the real bank or shop website.

1.15 Phishing

Phishing means the prying of personal, card or online banking data by e-mail, telephone and/or fake web sites. The aim is to scam the user into sharing private information so that it can be used for fraud such as identity theft or Netbank withdrawals.

1.16 Smishing

Short for SMS Phishing, it is a variant of phishing e-mail scams that uses the Short Message Service (SMS) systems to send phishing messages. The SMS will contain a website hyperlink. If the user clicks on the link, a Trojan horse will be downloaded to the phone and you are requested to input sensitive data on the web page.

1.17 Ransomware

Ransomware is software that denies a user access to files in a device until a sum of money has been paid (ransom) to the online criminals. A worm or Trojan horse may be the carrier of ransomware or the user has clicked on an infected e-mail attachment or visited a hacked website.

1.18 Shoulder surfing

When using your card in a shop or an ATM someone could stand close to you and see you keying in your PIN code. After this they will steal your card and use it for purchases and/or withdrawals from ATMs.

1.19 Skimming and card fraud

Skimming is where the criminals use a special card reader to copy the content of the magnetic stripe on your card. The information is copied onto another card that the criminals use and the money is drawn from your account. Skimming can be done at unattended terminals (ATMs, petrol stations), shop terminals, parking automats, restaurants and other places that use card readers.

1.20 Social engineering

Social engineering is about manipulating or tricking people into giving up confidential information. Online criminals that make use of social engineering exploit that many people want to trust others and also to be helpful. Phishing is a type of social engineering.

1.21 Spam

Spam is a term used about electronic junk mail or junk newsgroup postings – the electronic equivalent of the junk mail in the postal mail. The most common types of spam are: prescription drugs, herbal remedies, get-rich quick schemes, financial services, online gambling and pirated software. Spammers often disguise their e-mails in order to evade anti-spam software. Most often spam will do no harm but it can be very annoying and take up a lot of space in your mailbox. You should never answer spam e-mails or click on any link in a spam e-mail. Use a spam filter to block out unwanted e-mails.

1.22 Spyware

Spyware is software that enables hackers to gather and steal information without your permission. Information could include credit card numbers and passwords etc.

1.23 Trojans

Trojans (or trojan horses) are programs that pretend to be legitimate software, but they actually carry out hidden, harmful functions such as stealing personal information from the device. Some Trojans allow online criminals to take control of another user’s device via the internet without the user’s knowledge.

1.24 Virus

Viruses are computer programs that can spread by making copies of themselves. They spread from one computer to another and from one network to another usually without you knowing about it. Viruses can be harmful and display irritating messages, steal information, jam or crash the device, or even give other users control over your device.

1.25 Worm

A worm is a program that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down.