



# “CYBER CRIME- AN OVERVIEW...”

## ***Cyber Crimes** are broadly classified into 3 categories...*



Cyber crime against Property..  
i.e- Financial Crime, illegal fund transfer  
etc.



Cyber crime against Persons..  
i.e- On line harassment, Cyber obscenity  
etc.



Cyber Crime against Nations..  
i.e- Cyber terrorism etc.

# Different Types Of Cyber Crime ...



- Hacking (mails, System, website, database etc.)
  - Social Networking Obscenity
  - System Contamination
  - Cyber Stalking
  - Fraud and Identity Theft
  - Phishing Scams & online fund transfer.
  - Online Job Scam
  - Denial of Service
  - Online lottery Scam
  - Cyber Terrorism
  - Data Theft
- ...and *many more*



## **PROFILE OF CYBER CRIMINALS...**

- ❖ Disgruntled employees.
- ❖ Teenagers.
- ❖ Professional Hackers.
- ❖ Business Rival.
- ❖ Ex-Boy/Girl Friend.
- ❖ Hackers of enemy country.

# HACKING



Hacking in simple terms means intrusion into a computer system without the permission of the computer owner/user.

# VIRUSES



- \* A virus is a computer program that can replicate itself and spread from one computer to another.

# CYBER STALKING



- \* Stalking is a form of mental assault in which the perpetrator repeatedly, unwantedly, and disruptively breaks into the life-world of the victim. Following a victim in cyber world.

# IDENTITY THEFT



- \* Identity theft is a form of stealing someone's identity and assuming that person's identity to access resources or obtain credit and other benefits in that person's name.



# PHISHING



- \* Phishing is the act of attempting to acquire information such as internet banking usernames, passwords and credit card details (and sometimes indirectly money) by masquerading as a trustworthy entity in electronic communication medium.
- \* Link manipulation
- \* Website forgery
- \* Phone phishing

# DATA THEFT



**Data theft** is the act of stealing **computer**-based information from an unknowing victim with the intent of compromising privacy or obtaining confidential information. **Data theft** is increasingly a problem for individual **computer** users, as well as big corporate firms. There is more than one way to steal **data**.

# IMPERSONATION IN FACEBOOK




Creation of fake impersonating profile in Facebook using the photograph and personal information of the target victim. Sometimes the offender uploads morphed photograph of the victim to malign her social reputation and prestige. Also imposes the victim as “call girl” & provides contact number.

## **CHEATING BY CREATION OF FAKE/ LOOK ALIKE WEBSITE & E-MAILS**

- \* The fraudsters create fake/ look alike websites & e-mails impersonating different reputed companies, organizations, educational institutions etc. and mislead & induce the gullible public to part with huge amount of money towards achieving their eye catching offers and online job prospects like becoming e-tutor.

# Recent trend of Cyber Crime

- \* Hacking of email ID and social networking ID.
- \* Creation of fake profile.
- \* Uploading of personal info/picture/video in different websites.
- \* Data theft from computer system.
- \* Money transfer in different account by phishing/look alike mail .



**The Information Technology Act, 2000 (I.T. Act)** is the primary law in India dealing with cybercrime and electronic commerce.

# Most significant I.T. Act

- Sec-43.** Penalty for damage to computer system and unauthorized access.
- Sec-46.** Power to adjudicate.
- Sec-66B.** Punishment for dishonestly receiving stolen computer resource or communication device. (3yrs. imprisonment and/or Rs.1 lakh)
- Sec-66C.** Punishment for identity theft. (3yrs. imprisonment and/or Rs.1 lakh)
- Sec-66D.** Punishment for cheating by personation by using computer resource. (3yrs. imprisonment and/or Rs.1 lakh)
- Sec-66E.** Punishment for violation of privacy. (3yrs. imprisonment and/or Rs.2 lakh)

Continue...

# Most significant I.T. Act

- Sec-67.** Punishment for publishing or transmitting obscene material in electronic form (3yrs. imprisonment and/or Rs.5 lakh)
- Sec-67A.** Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form. (5yrs. imprisonment and/or Rs.10 lakh)
- Sec-67B.** Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form. (5yrs. imprisonment and/or Rs.10 lakh)






**Your safety....**


# SBI original log-in page...

State Bank of India

STATE BANK OF INDIA [IN]https://retail.onlinesbi.com/retail/login.htm#

**भारतीय स्टेट बैंक**  
**State Bank of India**  
The Banker to Every Indian

About OnlineSBI | Registration Forms



HomeProducts & ServicesHow Do I

**Login**Welcome to Personal Banking

To access your accounts...  
**Login to OnlineSBI**

(**CARE:** Username and password are case sensitive.)


Username \*

Password \*

☐ Enable Virtual Keyboard


[New User? Click here](#) [Login](#) [Reset](#) [Forgot Login Password](#)

For better security use the Online Virtual Keyboard to login. [More ...](#)




**NEVER** respond to any popup,email, SMS or phone call, **no matter how appealing or official looking**, seeking your personal information such as username, password(s), mobile number, ATM Card details, etc. Such communications are sent or created by fraudsters to trick you into parting with your credentials.

[Complaints](#) | [Trouble logging in](#) | [Password Management](#) | [Security Tips](#) | [FAQ](#) | [About Phishing](#) | [Report Phishing](#) | [Lock User Access](#)



This site is certified by Verisign as a secure and trusted site. All information sent or received in this site is encrypted using 256-bit encryption



- ❖ Mandatory fields are marked with an asterisk (\*)
- ❖ Do not provide your username and password anywhere other than in this page
- ❖ Your username and password are highly confidential. Never part with them. SBI will never ask for this information.

# Phishing log-in page...

Distance Education Department, Sikkin ... (Untitled) State Bank of India

About OnlineSBI | Registration Forms | Net Banking Branches

भारतीय स्टेट बैंक  
**State Bank of India**  
With you - all the way

Home Products & Services

To access your accounts...  
**Login to OnlineSBI**

User Name \*

Password \*

☐ Enable Virtual Keyboard

For better security use the Online Virtual Keyboard to login. [More...](#)

**Online Virtual Keyboard**

&	\$	+	@	)	(	-	%	^	_	*	!	#
.	8	0	4	5	6	7	9	2	1	3	=	-
e	t	r	q	w	u	i	y	p	o	}		{
a	f	s	d	g	k	h	j	\	/	[	]	
x	z	c	v	m	b	n	<	:	:	"	'	>
CAPS LOCK						CLEAR			?			.

**Important:** SBI never sends email for getting customer information except during maintainance exercises. Do not fill in your informations on any site other than this site. Beware of phishing mail. [Know more...](#)

[Trouble logging in](#) | [Password Management](#) | [Security Tips](#) | [FAQ](#) | [About Phishing](#) | [Report Phishing](#)

This site is certified by Verisign as a secure and trusted site. All information sent or received in this site is encrypted using 128-bit encryption

Mandatory fields are marked with an asterisk (\*)  
Do not provide your username and password anywhere other than in this page

## Use 2-step verification...

- \* Stronger security for your Google/Facebook Account.
- \* With 2-Step Verification, you'll protect your account with both your password and your phone.
- \* Use your Mobile as a 2<sup>nd</sup> key for your account.



## Do not respond for fake call/sms...



- \* Do not respond any call/sms seems to be from your Bank seeking information regarding bank account or card details or mobile OTP. Please keep in mind that bank do not asks any security information via call.

## WhatsApp security...



- Avoid using WhatsApp on public Wi-Fi networks (airports, cafés, etc.). You never know who may be listening.
- Use certain basic security measures with your own Wi-Fi network.
- Do not share your IMEI no.
- Be sure before joining any WhatsApp Group.
- Be sure before sending your personal information i.e. photos, videos etc.
- Keep your profile picture private.

# Online Safety Tips...



- \* What you put online will be there forever.
- \* Use a strong password (a combination of upper and lower case letters, symbols and numbers).
- \* Don't post inappropriate or illegal content anywhere on the internet.
- \* Don't open e-mail attachments or instant-message attachments unless you are completely sure they do not contain viruses.
- \* Don't click on links inside e-mails or instant messages.
- \* Never give out personal information about yourself, your family, or your friends (such as your last name, address, phone numbers, city, the name of your school, photos of yourself or your family, PIN numbers for your bank, etc.).



## Online Banking Tips...

- \* **Never use unprotected PCs at cyber cafes for internet banking.**
- \* **Never keep your pin and cards together.**
- \* **Never leave the PC unattended when using internet banking in a public place.**
- \* **Register for Mobile SMS , E-mail Transaction Alerts.**
- \* **Never reply to emails asking for your password or pin.**
- \* **Visit banks website by typing the URL in the address bar and use https.**
- \* **Log off and close your browser when you have finished using internet banking.**
- \* **Memorize your PIN. Never carry your PIN.**
- \* **Report lost or stolen card immediately.**
- \* **Use virtual cards for online shopping. For details: ([https://www.onlinesbi.com/virtual\\_card\\_faq.html](https://www.onlinesbi.com/virtual_card_faq.html))**



# Wi- Fi Security Tips...



The use of public and unsecured Wi-Fi by the use of Smart-phones, tablet and computer users are very risky. The risk is even greater when the use is for the purpose of assessing sensitive information.



- \* Change Default Administrator Passwords (and Usernames) of the Wi-Fi Router.
- \* Change Password after regular interval.
- \* Position the Router or Access Point Safely.
- \* Turn Off the Network / Wi-Fi routers if it is not in use.



Thank you  
for patience:::  
for patience:::