



# Cyber awareness for students

Internet has become one of the integral part of our daily life. It has transformed the way we communicate, make friends, share updates, play games, and shop. They are impacting most aspects of our day-to-day life. Cyberspace connects us virtually with crores of online users across the globe. With increasing use of cyberspace, cybercrimes especially against women and children such as cyber stalking, cyber bullying, cyber harassment, child pornography, rape content, etc. are also increasing rapidly. To stay safe in the online world, it is important to follow some cyber safe practices which may help in making our online experience and productive.

To know more, [Click here.](#)



## Business Email Compromise (BEC)

**BEC is when a fraudster hacks into an e-mail account and impersonates the real owner to defraud the company, its customers, partners, and/or employees. This may be used to send sensitive data, forged payment invoices or malicious documents**

### Safety Tips

Enable multi-factor authentication for all email accounts

Flag differences in “reply” and “from” email addresses

Enable security features that block malicious emails

Do not share personal information

**Be Vigilant, Be Cyber Safe**







## Business Email Compromise (BEC)

BEC is a tried-and-tested cyberattack method that costs consumers and businesses billions every year. So what makes BEC such a prevalent cybercrime technique? Simply put: cybercriminals use BEC as a way to make social engineering attacks more effective. A social engineering attack is any form of cybercrime involving impersonation. The attacker pretends to be a trusted person so that the target does what they're told. According to Verizon's 2021 Data Breach Investigation Report (DBIR), BEC is the second-most common type of social engineering attack. In a BEC or other social engineering attack, the threat actor pretends to be a trusted person so that the target does what they're told. To know more, [Click here](#).



## How to prevent **ONLINE FINANCIAL FRAUDS**

Follow these tips and stay cyber secure!

-  Never disclose your net banking password, One-Time Password (OTP), ATM or phone banking PIN, CVV number, expiry date to anyone
-  Do not make financial transactions over shared public computers or while using public Wi-Fi networks
-  Use strong passwords for your online banking accounts and change them periodically
-  Always use virtual keyboards while logging into online banking services
-  Always delete the browsing data of your web browser after completing your online banking activity
-  Always review transaction alerts received on your registered mobile number and reconcile them with the amount of your purchase

## Financial Fraud

With the growth of information and communication technology, the structure and nature of financial services delivery has also changed. Online banking or internet banking has emerged as a new and convenient way for using financial services like funds transfer, viewing account statement, bill payment, use of e-wallets etc. An upsurge in the use of devices connected with the internet and the

convenience of online financial services has increased the risk of our hard-earned money being duped by cybercriminals of our hard-earned money.

To know more, [Click here.](#)



# AVNL

## Steps to be taken if Identity theft had taken place

If you feel an identity theft had taken place, then what are the possible steps to be taken to mitigate the situation

### STEP 1

Ascertain the type of identity theft that has taken place on your identity.

### STEP 2

File a complaint in a written document showing the details of theft happened on your identity

### STEP 3

Report your identity theft to the police station concerned and register a complaint and also submit a copy to the concern banks/ financial institutions.

It is always advisable to keep a copy of all the document pertaining to your identity at a safe place. File complaint based on the copies of the identity cards safely preserved.

If necessary, the following documents are to be submitted in the local police station

- A copy of your identity theft report
- A government issued ID with a photo
- Proof of your address
- Any other proof of your identity theft
- After reporting make sure you take a copy of the police report

What are the further steps that can be taken?

- Once we identify ourselves as a victim of identity theft, it is better to intimate the bank to close any of the new accounts that are opened on your identity without your knowledge. Also intimate the bank to remove the bogus charges from your account which are being charged on you for the actions of the identity thief.
- Make sure that your credit/debit account reports are corrected by intimating the bank.

Other possible steps that can be taken?

- Immediately report to the authority concerned on misuse of any identity card.
- Stop debit collectors from trying to collect debits you don't own.
- Apply for re issue of Identity card to the authority concerned.
- Take efforts to clear your identity from the criminal charges that are occurred by seeking the help of Law




**Be Cyber Smart, Be Cyber Safe**

## Identity Theft

Identity theft is the act of wrongfully obtaining someone's personal information (that defines one's identity) without their permission. The personal information may include their name, phone number, address, bank account number, Aadhaar number or credit/debit card number etc. Identity theft can have many adverse effects. Let us look at some examples of identity theft. Hacking or gaining access to Social Media Accounts Misuse of photo copies of identity proofs Credit/Debit Card Skimming.

To know more, [Click here](#).

## Learn More

-  Citizen Manual Report CPRGR complaints
-  Citizen Manual Report Other Cyber Crime
-  Citizen Manual Financial Cyber Frauds Reporting and Management System

## Report Cybercrime at

 Helpline Number - **155260**  **@CySecKCoE**

 **@cyberdosti4c**  **@cyberdosti4c**  **@cyberdosti4c**