ONLINE SAFTY

MEMBERS OF ECOA ARE REQUESTED TO BE ON ALERT OF INTERNET SCAMS WHEN YOU ARE ONLINE.

They might get in touch by phone, email, postal mail, text, or social media. Fraudsters may pose as agents / representatives of companies dealing in entertainment content & give lucrative offers to buy/ sale films, TV serials, web series etc etc. Such unscrupulous elements may use fictitious websites, email address etc to show as genuine one. Though our members are smart enough to detect such fraudulent mails etc but it is always better one should be always on alert since technology is changing day by day and you never know when you are victimised by an offer.

Scams may come through phone calls from real people, robocalls, or text messages. Callers often make false promises, such as opportunities to buy/ sale products.

Scam artists defraud millions of people each year by using internet services or software. That's why it's important to protect yourself and to report internet fraud if you have been victimized.

These are the most common examples of internet fraud:

- Phishing or spoofing involves the usage of fake emails, text messages, or copycat websites to commit identity theft. Or, it can be used to steal personal information
- Data breaches occur when sensitive data (personal or financial information) is hacked into, leaked, or inadvertently posted from a secure location. This information may be used to steal identities or commit financial fraud.
- Malware is dangerous software that is designed to disable computers and computer systems.
- Internet auction fraud involves the misrepresentation of products from an internet auction site. Or, it can occur when merchandise isn't delivered to a buyer by a seller online as promised.

DO

- Learn how to spot internet fraud by knowing the warning signs of common fraud schemes. These schemes include phishing or spoofing, data breaches, and malware.
- **Know your buyer or seller. If you don't know who you're buying from or selling to online, do some research.**
- Update your anti-virus software and anti-spyware programs. Most types of anti-virus software can be set up to make automatic updates. Spyware protection is any program that protects your personal information online from malware. If your operating system does not offer free spyware protection, you can download it from the internet. Or, you can purchase it at your local computer store. But, be aware of ads on the internet offering downloadable spyware protection which could result in the theft of your information. You should only install programs from a trusted source.

DON'T

- Don't give out your personal information to anyone you don't trust. Never provide it in response to an email, a pop-up, or a website you've linked to from an email or web page.
- Don't keep your computer running all the time. Doing so will make it more prone to spyware and other attacks from hackers and identity thieves.

⇨ In the interest of members of Entertainment Content Owners
Association of India {ECOA}