powered by

SAFER INTERNET INDIA

Mission GraHAQ Handbook

Your Guide to Safe Online Shopping

sponsored by

amazon

Mission GraHAQ handbook

Your Guide to Safe Online Shopping

JULY 2026

The Safer Internet India coalition is dedicated to enhancing user welfare, trust, and safety within India's digital economy, thereby fostering innovation-driven growth.

Acknowledgement
This report was supported by Amazon, a member of the Safer Internet India coalition.

www.saferinternetindia.com
secretariatsaferinternetindia.com

Contents

What's Inside this Handbook?

Online shopping has transformed the way millions of Indians discover, compare, and buy products every day. It is one of the more quietly remarkable shifts in how people live, and for most, it works exactly as it should.

This handbook is built around that reality. It is a resource for anyone who wants to shop with greater awareness, exercise their rights with ease, and handle the occasional hiccup without losing time or money.

This handbook introduces you to some of the most common scams circulating today, helping you recognise the warning signs before they impact you.

Then, we turn awareness into action, helping you evaluate your own shopping habits and learn what protections are already available to you. Finally, the handbook covers your legal rights as a consumer and what steps you can take if things go wrong.

By the end, the aim is for you to be a ***Viksit GraHAQ***: a consumer who is not just informed, but alert enough to apply that knowledge and act on it.

Section I

Understanding the Online Shopping Landscape

The Rise of e-commerce Platforms in India

India's e-commerce sector has emerged as one of the fastest-growing segments of the digital economy, driven by increasing smartphone adoption, expanding internet connectivity, and widespread use of digital payment systems.

This growth has significantly enhanced consumer access to goods and services, fostered innovation, and enabled businesses of all sizes to reach customers across geographies.

Why is Online Shopping so Popular?

Online shopping offers unmatched convenience and variety. You can explore numerous products and brands at once, compare prices instantly, find great deals, and enjoy doorstep delivery.

As e-commerce continues to expand and play a larger role in India's digital economy, ensuring a safe, trustworthy, and transparent online shopping environment has become increasingly important.

India's e-commerce market continues to be one of the world's fastest-growing digital consumer ecosystems, driven by rising internet penetration, expanding digital payments, quick commerce, and increasing adoption beyond metropolitan cities.

Valued at approximately US$90 billion in 2025, the market is projected to nearly triple to US $250 billion by 2030, underscoring its scale and strategic importance for businesses and policymakers alike.

Recognising Common Scams

In this section, we highlight common types of e-commerce scams and how a Viksit GraHAQ can protect themselves against such scams.

Who is a Viksit GraHAQ?

Mission GraHAQ is a consumer awareness initiative to educate and empower online shoppers with safe, informed purchasing habits. It aims to ensure that every consumer is a 'Viksit GraHAQ' who is well-informed and aware of their rights.

The journey of becoming a Viksit GraHAQ begins with a Shikshit GraHAQ, an informed and educated consumer who understands products, services, and associated rights and risks. This awareness evolves into a Satark GraHAQ, who consciously applies this knowledge by exercising caution, verifying information, and avoiding impulsive decisions. The final step involves becoming a Sashakt GraHAQ—an empowered consumer who consistently demonstrates safe online practices, makes informed choices, and actively safeguards personal and financial interests.

We will illustrate how a Shikshit GraHAQ can identify common online frauds before they occur by recognising their key warning signs. This section will then demonstrate how a Satark GraHAQ translates this knowledge into safe online shopping behaviour. This aims to nurture a Sashakt GraHAQ who adopts safe practices and is well-versed in their rights.

01 FAKE WEBSITES & PHISHING LINKS

Bad actors may create websites that closely resemble well-known brands or send phishing messages and emails claiming unpaid deliveries, account issues, or other urgent matters. These often direct you to fake webpages designed to collect sensitive information such as UPI IDs, OTPs, or credit/debit card details.

Shikshit GraHAQ

Even small differences in a website address, such as a spelling variation or an unsecured webpage, can indicate that a site is not genuine. These subtle changes are commonly used to collect sensitive credentials without attracting attention. Forexample, a link like xyzzzzzz.in may redirect you to a fake website.

Satark GraHAQ

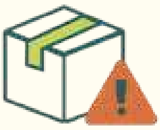
A quick verification of the website address or mobile application can go a long way in confirming that you are accessing the official domain or an authorised app before entering any personal or financial information.

Sashakt GraHAQ

Once you've confirmed that the source is genuine, you can proceed with greater confidence. If there is any uncertainty, it's worth independently verifying the source before sharing personal or financial information.

Read Section 2 of this Handbook to learn more about how you can avoid fake shopping websites and keep your personal and financial information safe.

The “#ScamSmartIndia” campaign by Amazon India with Indian Cybercrime Coordination Centre (I4C) designed to safeguard consumers from the growing threat of online scams and fraud warns of phishing, fake alerts, weak security, and impersonation during festive deals. Many fake emails/texts claim a problem with your “order” or “account” to push you to click.



02 FAKE DELIVERY SCAM

Scammers send unsolicited cash on delivery (CoD) packages to random addresses. These deliveries may contain empty boxes or low-value items, relying on confusion or urgency to persuade recipients to make a payment.

Shikshit GraHAQ

Unexpected deliveries can catch anyone off guard, especially if there is a possibility that someone else in the household placed the order. A quick check with family members before accepting or paying for a package can help avoid unnecessary payments.

Satark GraHAQ

These scams often rely on pressure, confusion, or the assumption that someone else ordered the item. Recognising these tactics can make it easier to pause and verify the order before making a payment.

Sashakt GraHAQ

Sharing this awareness with family members can help everyone respond confidently to unexpected deliveries. If suspicious or repeated incidents occur, it’s worth reporting them to the police or the relevant authorities.

03
“TOO GOOD TO BE TRUE” DEALS

Scammers often set up websites offering deep discounts or “too good to be true” deals. They also run ads on social media to lure consumers. Often, fake sites vanish after payment, or scammers send a poor-quality knockoff. There’s no customer support, and victims have little recourse since the platform itself was bogus.

Shikshit GraHAQ

A quick review of the websit’s URL, independent customer feedback, contact details, and return policy can provide useful signals about its credibility, rather than relying solely on advertisements or promotional posts on social media.

Satark GraHAQ

Some websites and social media accounts use unusually attractive offers to encourage quick purchasing decisions. Recognising these tactics can help you take a moment to verify the seller before proceeding.

Sashakt GraHAQ

Putting these checks into practice can make online shopping more secure. Choosing trusted websites, avoiding impulse purchases driven by steep discounts, and using secure payment methods that offer buyer protection can all help reduce the risk of problems after purchase.

04
EMPTY BOX SCAM

In this scam, customers receive empty boxes or worthless items after placing orders from fraudulent sellers or websites.

Shikshit GraHAQ

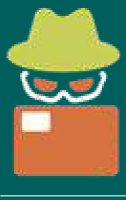
Choosing verified sellers is one of the most reliable ways to reduce the risk of this scam, as it is more commonly associated with unreliable sellers and websites.

Satark GraHAQ

Seller ratings, recent reviews, and product listings can provide useful signals about credibility. Inconsistent product descriptions, limited seller history, or unusually low prices are all worth examining more closely before placing an order.

Sashakt GraHAQ

If something goes wrong, raising a complaint within the timelines prescribed under the website's policies, along with supporting evidence, can help strengthen your case.



05 PAYMENT SCAM

In this fraud, scammers ask customers to pay outside the e-commerce website or mobile application (e.g., via a third-party site). The customer loses money and does not receive the product.

Shikshit GraHAQ

Requests to make payments through external links, QR codes, or third-party websites often bypass the safeguards available on the original website or app. Even if the offer appears genuine, it is worth completing the transaction only through the official payment process. For example, a seller may claim there is a "technical issue" and ask you to complete the payment through an SMS link to receive a steep discount. Verifying the request through the official checkout process can help avoid this type of scam.

Satark GraHAQ

Using only the website's or app's communication and payment systems helps preserve important safeguards such as order tracking, dispute resolution, and buyer protection. If a seller encourages an off-website or off-app transaction, it is worth reporting the account.

Sashakt GraHAQ

Understanding why these requests are made can make them easier to identify. Payments requested outside the website or app are often intended to bypass the protections available to buyers.

06
FAKE URGENCY SCAM

Scammers send customers messages saying, "Pay within the next 10 minutes or your order will be cancelled" or "This discount is only valid if you click on this link." The urgency is fake; it is designed to pressure you into paying quickly or sharing sensitive information without thinking.

Shikshit GraHAQ

Messages that create a sense of urgency are often intended to discourage careful verification. Taking a moment to review the message and checking the order or offer directly through the official website or application can help you make an informed decision.

Satark GraHAQ

If a message appears suspicious or creates unnecessary pressure, marking it as spam or reporting it can help reduce the chances of similar attempts in the future.

Sashakt GraHAQ

Recognising artificial urgency as a common scam technique makes it easier to pause, verify the information independently, and avoid rushed decisions involving payments or personal information.

07
DELIVERY BOX SCAM

In this increasingly common scam, scammers procure delivery boxes discarded by customers and use the information on those boxes to contact them. The scammers then ask the customer to click on a link to “give feedback” or share information by promising an extra discount on their next purchase. Clicking on these links or sharing information can result in financial losses.

Shikshit GraHAQ

Feedback or reward links received through unsolicited calls, messages, or emails are worth verifying before you interact with them. Sharing personal or payment information only through the official website or app can help reduce unnecessary risks.

Satark GraHAQ

Delivery labels can contain personal information that may be misused if they are discarded without being obscured or removed.

Sashakt GraHAQ

Destroying or covering personal details on delivery boxes before disposal is a simple precaution that can reduce misuse. If you receive suspicious communications, reporting them to the relevant e-commerce entity and the relevant authorities can also help.

08
FAKE CUSTOMER SUPPORT ACCOUNTS

Scammers monitor customer complaints on social media and reply using fake customer support accounts. These profiles usually use generic names such as “Help Desk”, “Support Team” or “Customer Service” They try to move the conversation to private messages, share suspicious links, or request personal information under the guise of troubleshooting or resolving issues.

Shikshit GraHAQ

Social media comments are public, making them an easy place for fake customer support accounts to approach customers. Using the verified customer support channels available on the official website or app, and avoiding the sharing of personal or account details on social media, can help keep your information secure.

Satark GraHAQ

Genuine customer support teams generally do not request sensitive information through social media comments or unsolicited direct messages. Keeping this in mind can make suspicious accounts easier to identify.

Sashakt GraHAQ

If you accidentally interact with a suspicious link or account, contacting the official customer support team, securing your account, and reporting the fake profile to the e-commerce entity are useful next steps.

09 MEMBERSHIP RENEWAL SCAM

In this scam, scammers impersonate legitimate subscriptions or membership services and send messages claiming that your membership is about to expire. These messages include links that direct you to fake payment pages or ask you to provide your card details urgently. Their communication often uses threatening or time-sensitive language to create panic and push victims into making quick payments.

Shikshit GraHAQ

Renewal reminders received through unsolicited messages are worth verifying independently. Renewing memberships through the organisation's official website or app, and checking your subscription status there, can help ensure that the request is genuine.

Satark GraHAQ

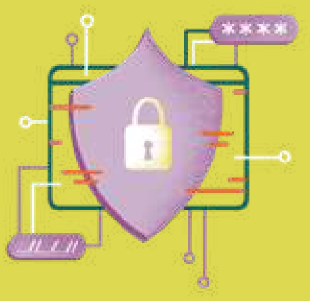
Links in unsolicited emails or text messages should be treated with caution. Taking a moment to verify the website before entering any details can help avoid fake payment pages.

Sashakt GraHAQ

Genuine organisations generally do not pressure customers into immediate renewals through unsolicited messages or rely on threatening language to obtain payments. Recognising these tactics can make suspicious renewal requests easier to identify.

Section II

Your Safety Checklist



Inbuilt Protections in Platforms to Protect Against Scams

Online shopping sites use built-in tools and systems designed to stop scams and protect shoppers from fraud.

Encryption, OTPs, and secure payment gateways:
When you shop or pay online, organisations use certain tools to keep your money and data safe.

Encryption
Scrambles your payment data so hackers can't read it while it travels online.

One Time Password (OTP)
A short code sent via SMS or app to confirm it's really you or to confirm that you have actually received the products.

Safe Payment Gateways
Trusted intermediaries that safely transfer your payment details between the site and your bank.

Habits that help you shop safely

The website address should start with https:// (not just http). The "s" stands for secure, indicating that the connection between your device and the website is encrypted and better protected.

Verify order details directly in the shopping app or website; if the order is not visible there, treat the message with caution.

Scammers often register website addresses that closely mimic legitimate ones - a misplaced letter or an extra word is usually the giveaway. It' s worth a quick look before you proceed.

Urgency is a common pressure tactic — messages claiming your account will be blocked or that you must act immediately are often designed to make you skip the checks you'd otherwise do. Be cautious of such messages.

A "Not Secure"warning or an invalid certificate alert from your browser is a signal that the site may not be safe to use - it's best to close it and navigate away.

Never share your password, OTP, CVV, card details, or banking credentials over calls, messages, or chats.

Do not download apps that are not available on the Google Play Store/iOS App Store.

Do not click on links received through SMS, WhatsApp, or email that ask you to log in, make a payment, or verify account details.

Links to APK files or software shared over social media or messaging apps are a common way to deliver malware — downloading directly from official app stores is the safer route.

Check the sender's details and any links carefully, as scammers often use website names that closely resemble legitimate ones.

If you click a malicious link (posing as a bank or courier) and enter your details or OTP, all the tech safeguards become moot. Checking sender authenticity, verifying links, and keeping personal and financial information private go a long way. Scammers do evolve their methods, but these habits help keep you secure while you shop.

Website/App-level Protections: Buyer Guarantees, Return Policies

Online shopping sites/apps in India are mandated by law to provide adequate grievance redressal mechanisms for users. Most have also developed their own policies and programs to protect their users and resolve complaints. These also include policies for processing refunds or returns where a product is wrongly delivered, defective, or materially different from what was advertised.

To make use of these protections, you will generally need to follow the site's grievance and return process, raise your claim within the stipulated time period, and return the product in its original, undamaged condition where a return is sought.

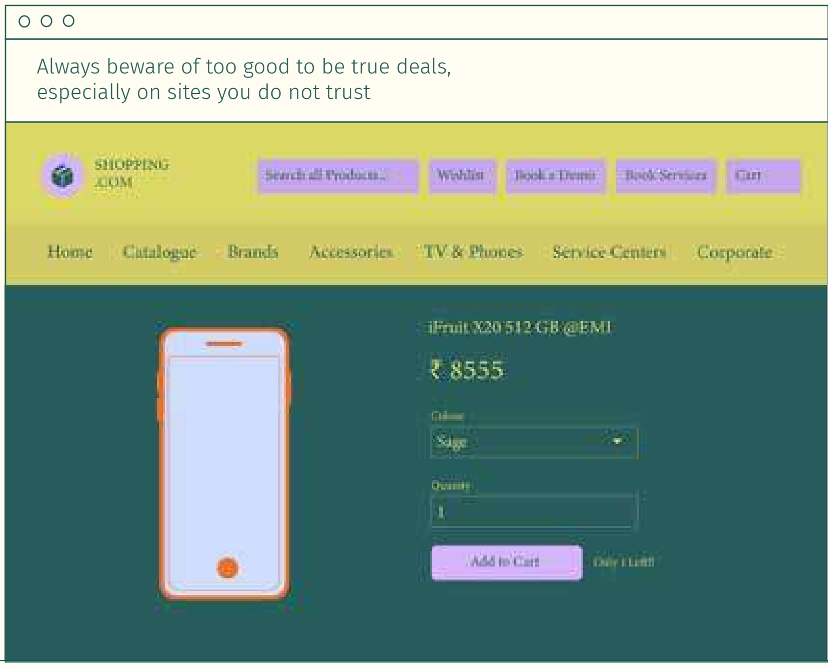
Shopping safely:
Practices worth keeping in your toolkit

The previous chapters covered the kinds of scams you may encounter while shopping online, from fake websites to elaborate delivery scams. We also looked at the built-in protections that shopping sites offer against these threats. That said, some of the most effective protection comes from your own safety habits.

The following practices can go a long way in keeping your personal and financial information safe. Some may already be part of how you shop and others might be worth adding to your routine.

01 Checking that a site or app is legitimate before you shop

Shopping from websites and apps you know are legitimate is one of the most reliable ways to protect yourself. If you shop from a scam website, your personal information, including financial details, can be stolen and misused. Sometimes, you may never receive the product you ordered, or you may receive a counterfeit item, which could pose a risk to your safety or health.



How to check if a shopping website is legitimate

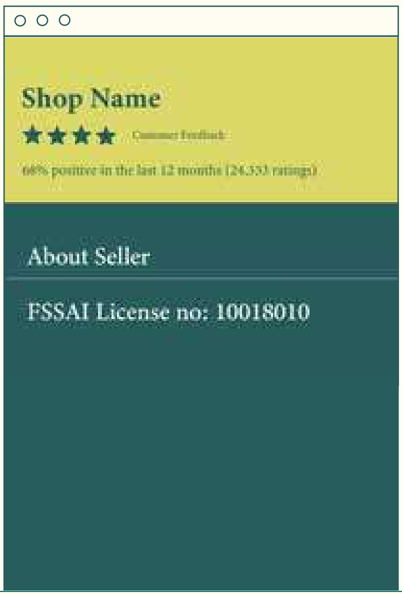
	Contact & Support Information	A legitimate site or app will usually include details of the organisation, such as contact information, an address, or a way to submit questions or complaints.
	Returns & Exchange Policy	A reliable website or app will include details about the returns and exchange policy on products. If a site offers no way to return a product for valid reasons, it's worth treating with caution.
	Too-Good-To-Be-True Discounts	If you notice products being offered at unbelievable discounts, always check other websites to verify the correct pricing.
	Check Online Presence & Reviews	A quick search and a look at the seller's social media pages can tell you a lot - whether they're active, how they respond to customers, and whether others have flagged any concerns.

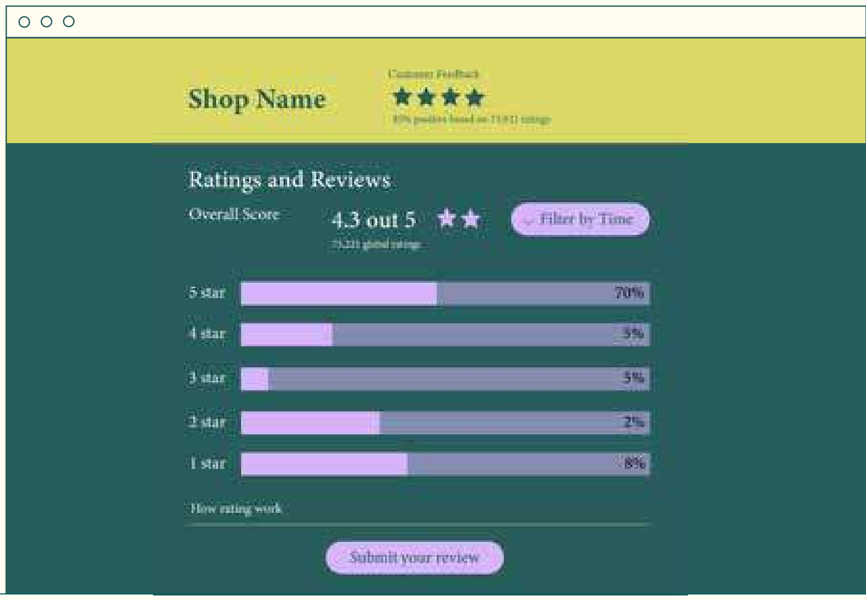
02 Checking that your seller is reliable

On sites that host multiple sellers, the seller you buy from matters as much as the site itself, not all sellers on a legitimate site are equally reliable.

How to check if the seller is legitimate:

Seller reviews and ratings are a useful starting point to check their authenticity. A pattern of mixed reviews around product quality or authenticity is a reasonable signal to look for another seller.





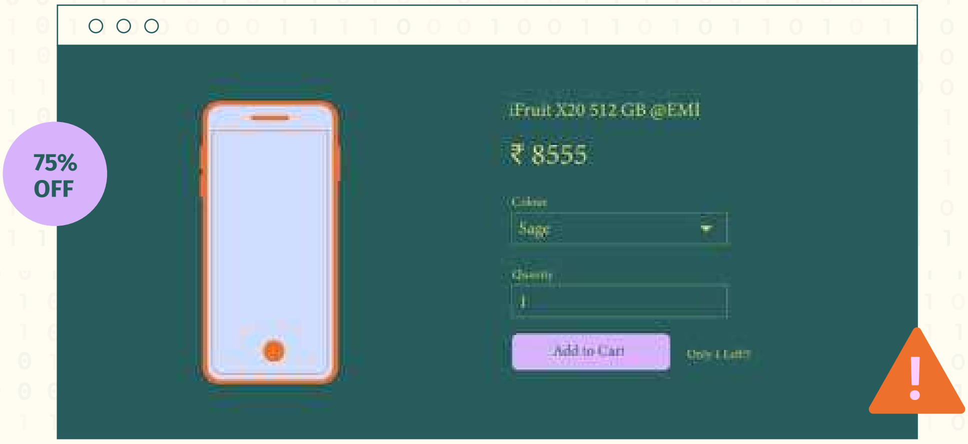
Verified sellers on reputable sites will often display government marks such as FSSAI numbers. If you're buying food, health, or regulated products, checking the seller's page for these details is worth the extra moment.

How long a seller has been active is another useful signal. A seller with an established presence and consistently good ratings gives you a reasonable basis for confidence in your purchase.

03 Recognising and responding to misleading ads

Advertisements, especially on social media, have become a very popular way to discover new products and services. However, the same accessibility that makes online advertising useful also means that scammers can use it to promote fake products, direct you to fraudulent sites, or harvest your information.

Scammers often replicate brand visuals and logos to make ads look legitimate. If an ad is promoting a well-known brand, going directly to the brand's official website or app is the most reliable way to confirm whether the offer is real.



Ads offering unusually large discounts or free gifts, particularly those pushing you to act immediately, are a common pressure tactic designed to skip the checks you'd otherwise make. Don't buy directly through the links in ads. Instead, visit the brand's verified website or app to make your purchase.

Comments and engagement on social media ads can be informative. Real users often flag suspicious promotions in the comments section. Reporting misleading or fake ads helps prevent others from being targeted - most sites have a straightforward option to flag suspicious content.

04 Using product descriptions to judge what you're buying

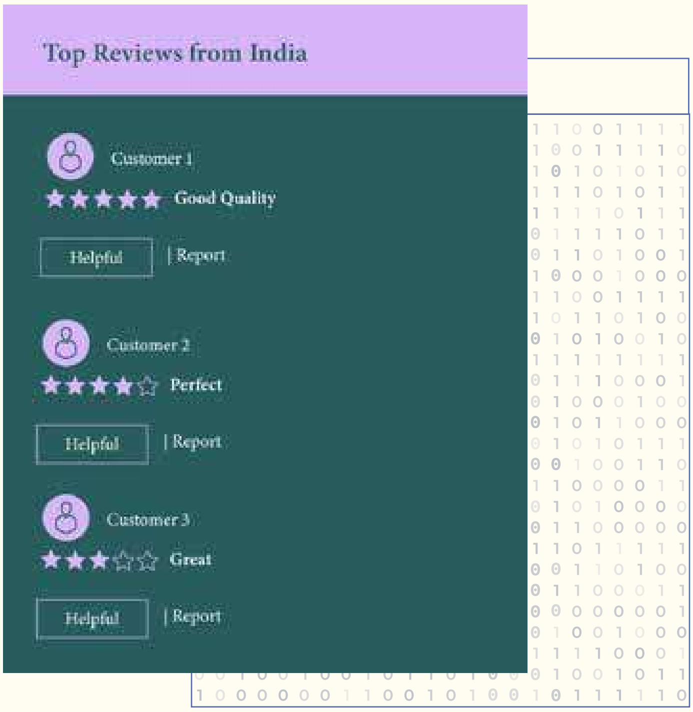
Legitimate products come with clear specifications such as storage capacity, materials, dimensions, warranty terms. When those details are missing or vague, it's worth pausing before you buy.

Look for a clear specification of size, material, and warranty (as relevant to the product you are purchasing).
It's also worth checking whether the specifications on the product page match what users describe in reviews or what appears on the actual packaging. Inconsistencies between these are a useful signal. Vague descriptors like 'quality fabric' or 'original,' especially when unaccompanied by detailed specifications or photos, are often a sign that a listing isn't what it claims to be.

05 Using reviews and ratings to make a more informed call

Individual opinions on a product will naturally vary, but patterns tend to emerge. If something is consistently flagged across reviews, that's worth paying attention to. User-uploaded photos and videos are extremely helpful for seeing how the product might look in real life, which is particularly beneficial for personal-use items such as clothing, accessories, and home goods.

For higher-value purchases, comparing ratings across trusted and secure platforms can give you a more complete picture before you commit.



06 Tracking your order and handling delivery safely

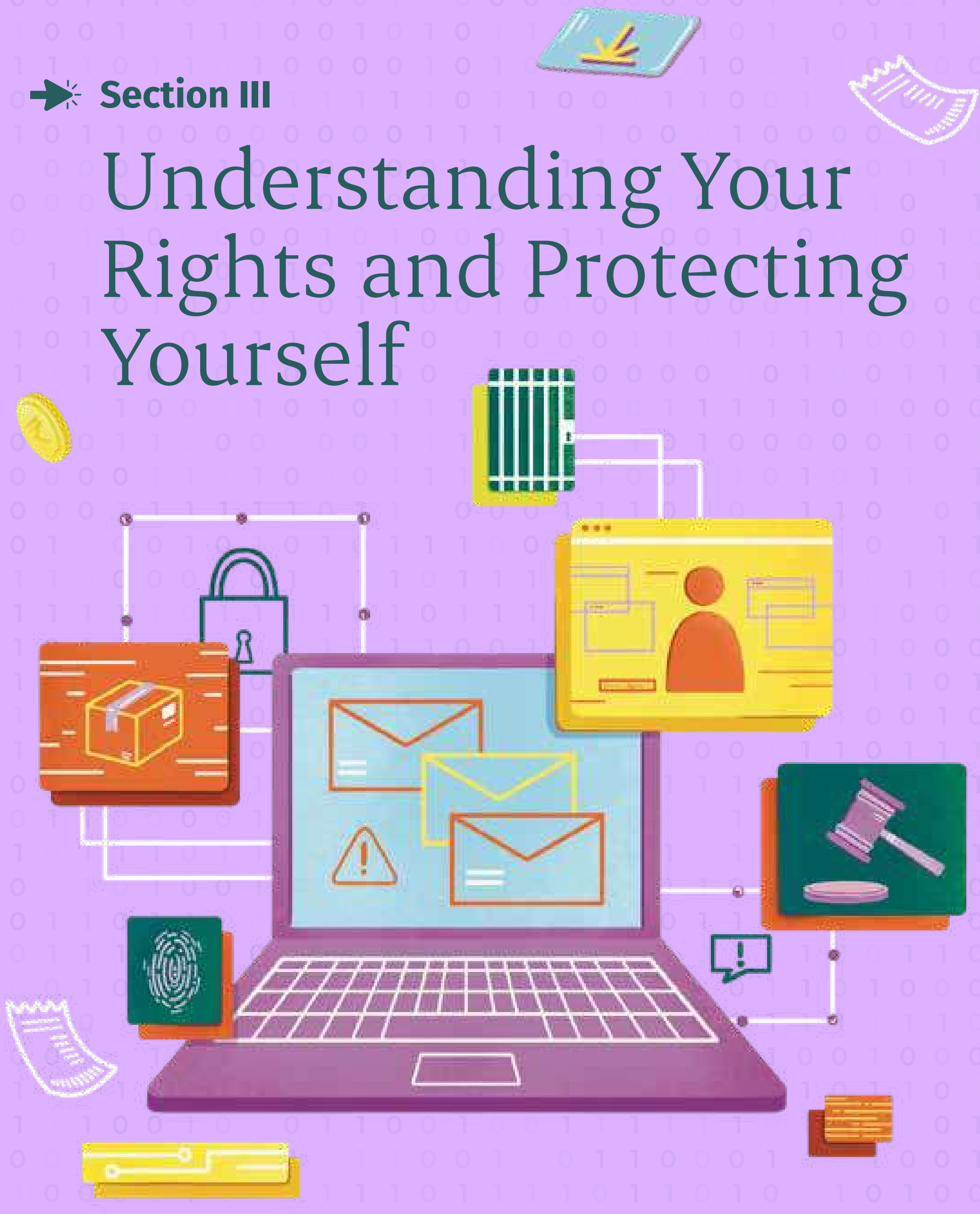
Always track your order using official tracking links or the order -feature on your shopping app.

Legitimate delivery services generally accept payments only through the shopping app before delivery or through verified payment methods at the time of delivery. If you receive a call or message claiming to be from the delivery partner asking for advance payment or personal details, do not share them.

When receiving an expensive order, open the package in front of the delivery agent (if possible) to ensure you received the correct item. Report any issues immediately through the website or app's support section.

Section III

Understanding Your Rights and Protecting Yourself



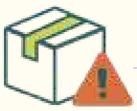
What the Law Says You Can Expect

In this section, we will identify the relevant laws that aim to protect the consumer from scams and fraud.

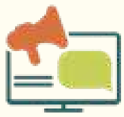
Rights of Consumers

The Consumer Protection Act, 2019 ("CP Act, 2019") was enacted to protect consumers' interests.

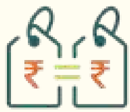
It recognises the following consumer rights:



Right to be protected against hazardous goods.

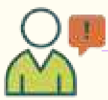


Right to be informed about the products.

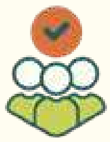


Right to be assured about access to a variety of goods at competitive prices.

Right to be heard and receive consideration about consumer interests.



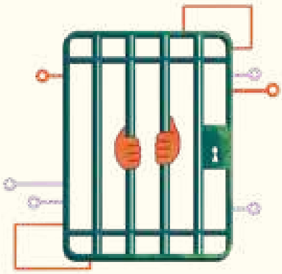
Right to grievance redressal.



Right to consumer awareness.

Protecting You From Unfair Trade Practices

The CP Act, 2019, defines unfair trade practices as, among other things, making false or misleading representations about a product, selling spurious products and refusing to process returns or refunds. These practices are prohibited under the CP Act, 2019.



Criminal Liability of Fraudsters

Fraudsters engaging in scams on e-commerce platforms or impersonating legitimate sellers, marketplaces, or service providers can be prosecuted under Indian criminal law, including the Bharatiya Nyaya Sanhita, 2023 (“BNS, 2023”) and the Information Technology Act, 2000 (“IT Act, 2000”).

Such conduct may amount to cheating under Section 318 of the BNS, 2023, punishable with imprisonment up to three years, or fine, or both.

Phishing is an online scam where cyber criminals pretend to be a trusted person or organisation to trick people into sharing sensitive information, such as passwords, bank details, or OTPs. Phishing can constitute the offence of cheating by personation under Section 319 of the BNS, 2023 and is punishable with imprisonment for 5 years, or with a fine, or with both.

Phishing is also punishable as cheating by personation under Section 66D of the IT Act, 2000, which can lead to imprisonment for up to 3 years and a fine of up to Rs. 1 lakh. Additionally, it can attract punishment under Section 66C of the IT Act, 2000, for identity theft. This also entails a jail term of up to 3 years and a fine of up to Rs. 1 lakh.

The next chapter will explain how you can seek help in case you become a victim of a scam.

When things go wrong

What are your options when you realise you have been scammed?

Always remember:

NEVER PANIC

Help is always a click or call away.

DOCUMENT

Take photos and videos of the damaged items, collect your bills and invoices and any other important documents.

ACT QUICKLY

Do not hesitate to raise an issue or file a complaint. Check the website or seller's page to find out the period within which you can either exchange/return the item.

The following options can be considered as your next steps after you have been scammed.

Contacting the seller or the shopping website

Sometimes, the item delivered to you might not be what you ordered, or it could be damaged and unusable. It is a frustrating situation, but you should reach out to the seller or e-commerce website immediately.

Most sellers will have their contact email on their app or website; if not, they will provide a customer care helpline where you can raise your issue.

If you are shopping on e-commerce marketplaces, you can submit your complaints directly through the tools provided on their websites or apps.

Filing a complaint under India's consumer redressal forums

If you are unable to get a satisfactory response from the e-commerce platform, you can approach consumer redressal forums or use the online consumer helpline portal. You can file your complaint online by contacting 1915 or the National Consumer Helpline (NCH) website at consumerhelpline.gov.in.

Tip: It is always advisable to first directly contact the seller or platform regarding your complaint. You can also file complaints offline at the appropriate consumer courts.

In case of fraud and scams that have criminal penalties

Certain types of fraud and scams, such as phishing and the sale of counterfeit products, are punishable under Indian criminal laws, as mentioned in the previous chapter.

For such frauds, you can file a complaint through the National Cyber Crime Portal or by calling the National Cyber Crime Helpline at 1930. Remember to retain all proof of purchase and communications with the seller.

Terms Used in this Handbook

Cash on Delivery

It is a payment method where customers pay for goods in cash or digitally at the time of delivery.

E-Commerce

E-commerce is the buying selling of goods or services through electronic networks, involving digital exchange of information and payments.

Seller

A seller is a person or business that sells goods or services to customers through an online marketplace platform.

Open-Box Delivery

A delivery method where the package is opened in the presence of the delivery agent to inspect damages in the product or verify the contents before acceptance.

UPI

UPI (Unified Payments Interface) is a real-time digital payment system that enables instant money transfers between bank accounts using a mobile app.

OTP

OTP (One-Time Password) is a temporary, single-use code used to verify a user's identity during secure transactions or logins.

Spam

Spam refers to unwanted or junk communication, typically transmitted through phone calls, email, text messages, or social media. It's often used to advertise things, but sometimes it's a part of an attempt to steal your information or money.

Scam

An online scam is when someone tricks you on the internet to steal your money, personal information, or sensitive data. Scammers often pretend to be trustworthy, offering fake deals, posing as officials, or sending messages that look real to deceive you. An online scam is a type of online fraud, but not all frauds are scams. A scam often involves convincing people to voluntarily give money or information (e.g. fake prizes or job offers). Online fraud, on the other hand, can involve actions like identity theft or hacking, where the victim might not even realise they've been targeted right away. In short, scams rely on tricking people, while fraud includes broader methods such as stealing or misusing information. This is why users must be vigilant, not only when interacting with people online, but also when visiting websites or downloading apps.

Fraud

Online fraud is when someone uses lies or deception to illegally take money or sensitive information through the internet. This includes things like hacking accounts, stealing payment details, or creating fake websites to trick people.

Grievance Redressal Mechanism

A formal process provided by e-commerce platforms or under law through which consumers can raise complaints and seek resolution.

Impersonation

A fraudulent practice where scammers pretend to be a trusted entity, such as a platform, seller, delivery partner, or customer support representative.

Encryption

A security technique that converts payment or personal data into coded form to prevent unauthorised access during online transmission.

Phishing

Phishing is a trick used by scammers to steal your personal information, such as passwords, bank details, or credit card numbers. They usually pretend to be someone you trust, like your bank, a company, or a government agency, to make you click on fake links or share sensitive information. Phishing attacks can occur through multiple channels. Attacks carried out through SMS/messaging apps are called smishing attacks, whereas those carried out over phone calls are called vishing (voice-phishing) attacks.

APK

APK stands for Android Package Kit, and it's the format used by Android to distribute and install apps. Every time you download an app—whether from the Play Store or an external site—you're actually installing an APK in the background.

www.saferinternetindia.com
secretariat@saferinternetindia.com
Safer Internet India
@SaferInternetIndia
@SaferInternetIN